

How to drive adoption of safer, more secure sign-in options for VA services

Tuesday, December 6, 2022



U.S. Department
of Veterans Affairs



What we know

Users are **frustrated** and **confused** because they must go to multiple websites to access VA services and there are a variety of ways to sign in via credentials that have known usability, security, and compliance issues.



Sign in

 [LOGIN.GOV](#)

 [ID.me](#)

 [DS Logon](#)

 [My HealtheVet](#)

Or create an account

 [Create an account with Login.gov](#)

 [Create an account with ID.me](#)

Having trouble signing in?

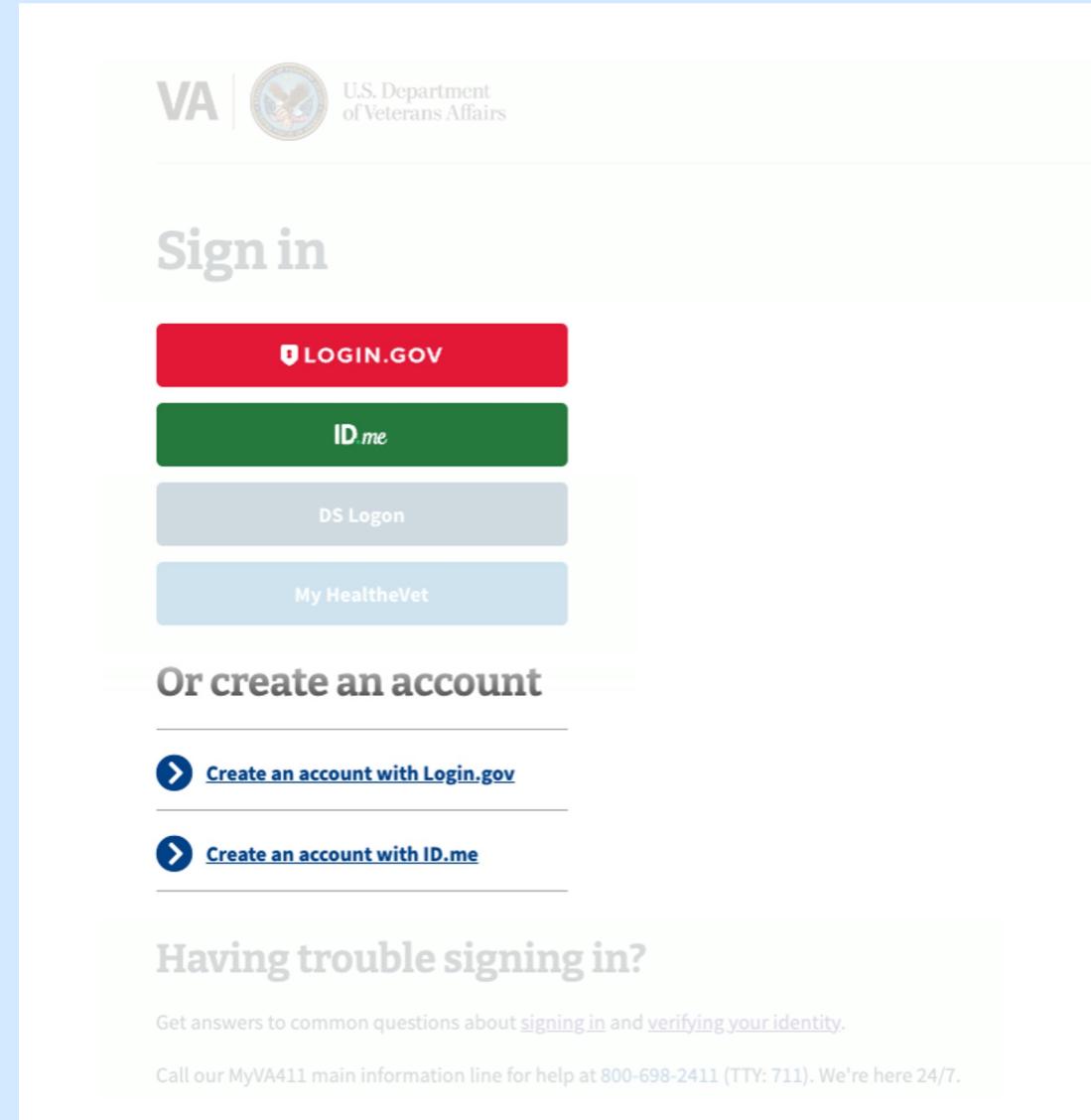
Get answers to common questions about [signing in](#) and [verifying your identity](#).

Call our MyVA411 main information line for help at **800-698-2411** (TTY: 711). We're here 24/7.

The product vision

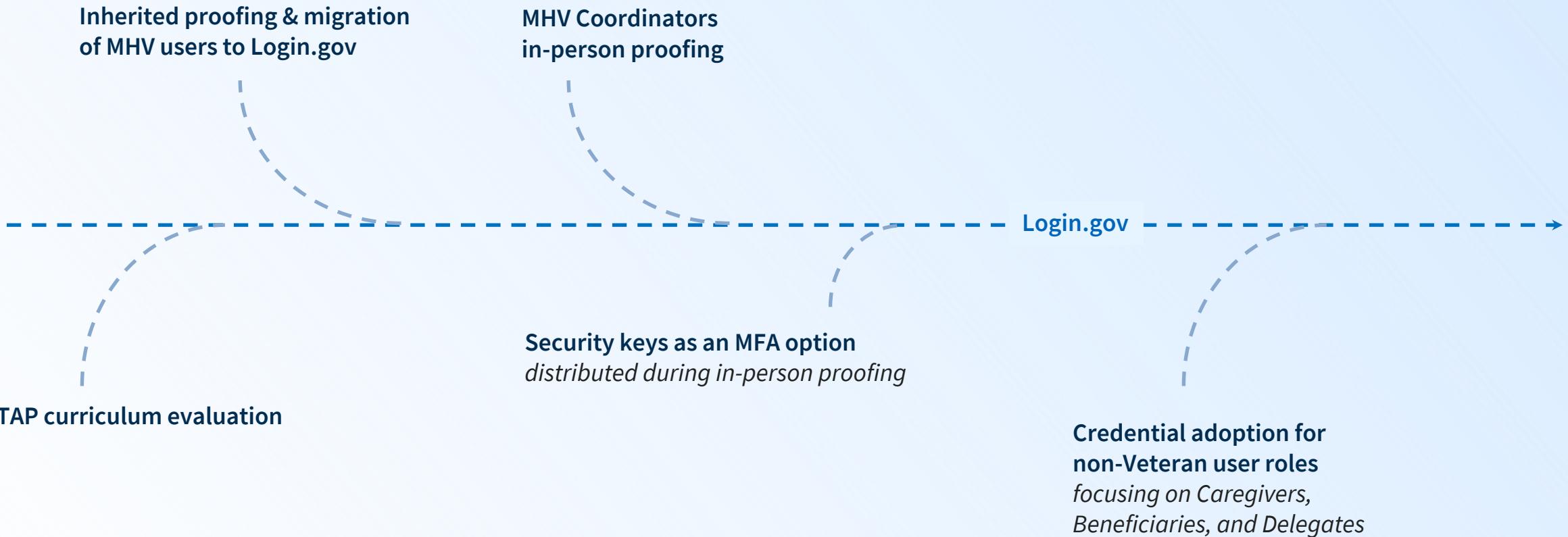
One sign-on to access all products and services, with a choice between a public or private credential option.

- **Adherence to standards:** Robust, compliant credential solutions (NIST 800-63A)
- **Veteran-centered experience:** Design approach based on Veteran input to discover and validate solutions

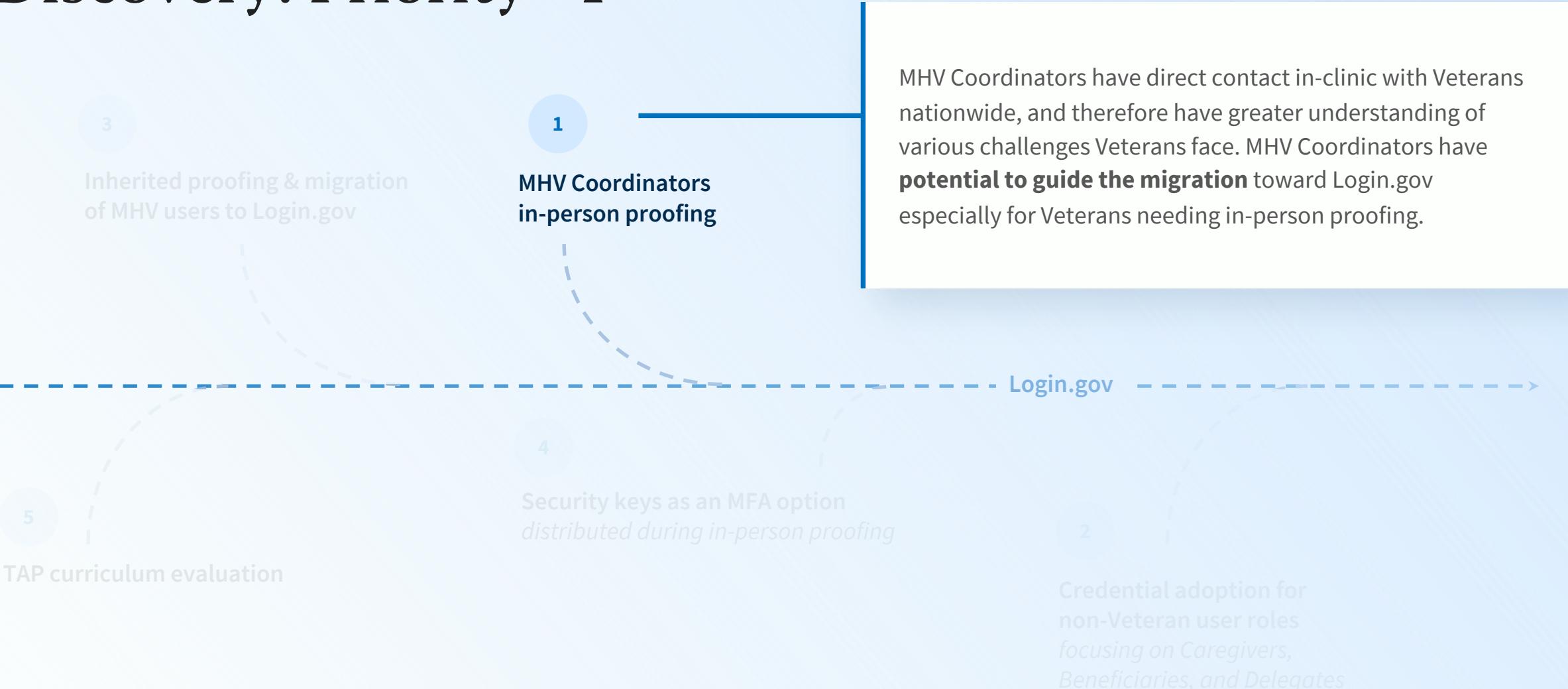


The image shows the 'Sign in' page of the U.S. Department of Veterans Affairs website. At the top right is the VA logo and the text 'U.S. Department of Veterans Affairs'. Below this, the word 'Sign in' is displayed in a large, light gray font. There are four horizontal buttons for signing in: a red button labeled 'LOGIN.GOV', a green button labeled 'ID.me', a light gray button labeled 'DS Logon', and a light blue button labeled 'My HealtheVet'. Below these buttons, the text 'Or create an account' is centered. Underneath this, there are two blue links with right-pointing arrows: 'Create an account with Login.gov' and 'Create an account with ID.me'. At the bottom, the text 'Having trouble signing in?' is followed by a link to 'Get answers to common questions about signing in and verifying your identity.' and a phone number 'Call our MyVA411 main information line for help at 800-698-2411 (TTY: 711). We're here 24/7.'

Our Discovery encompassed five areas of focus



Discovery: Priority #1



Discovery: Priority #2



Discovery: Priority #3

3

Inherited proofing & migration
of MHV users to Login.gov

1

MHV Coordinators
in-person proofing

5

TAP curriculum evaluation

4

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

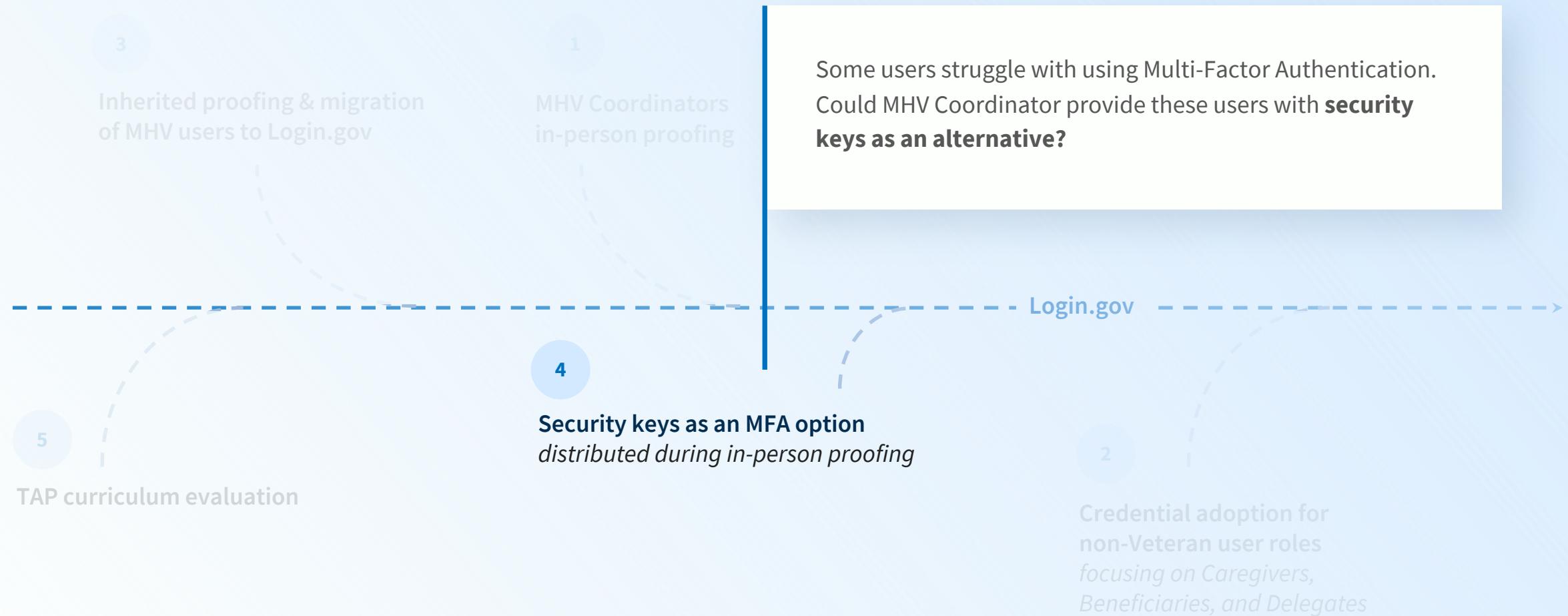
2

Credential adoption for
non-Veteran user roles
*focusing on Caregivers,
Beneficiaries, and Delegates*

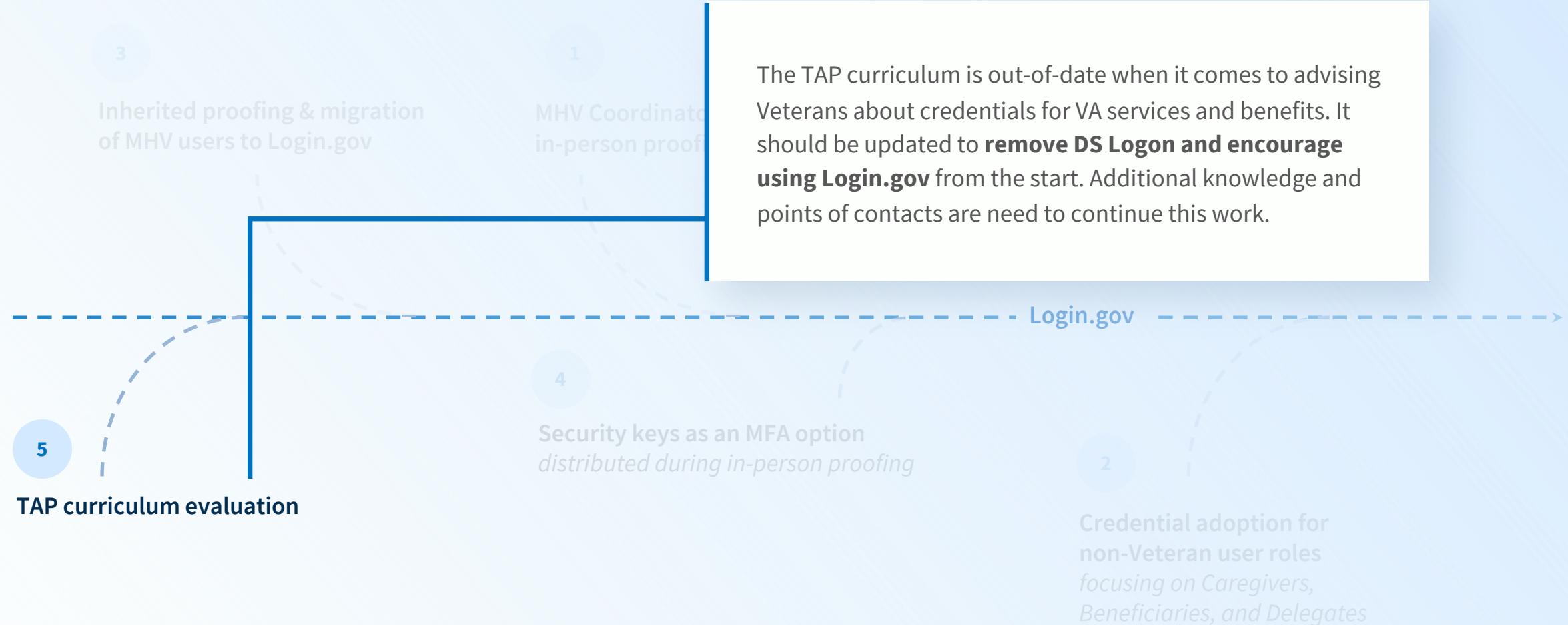
There is an opportunity to **leverage previous identity proofing** to streamline the transition to Login.gov for existing users. By understand the differing security standards of legacy credentials, we can identify users who may be eligible **for a simplified transition process**, and support users who will need to repeat ID proofing to meet Login.gov standards.

Login.gov

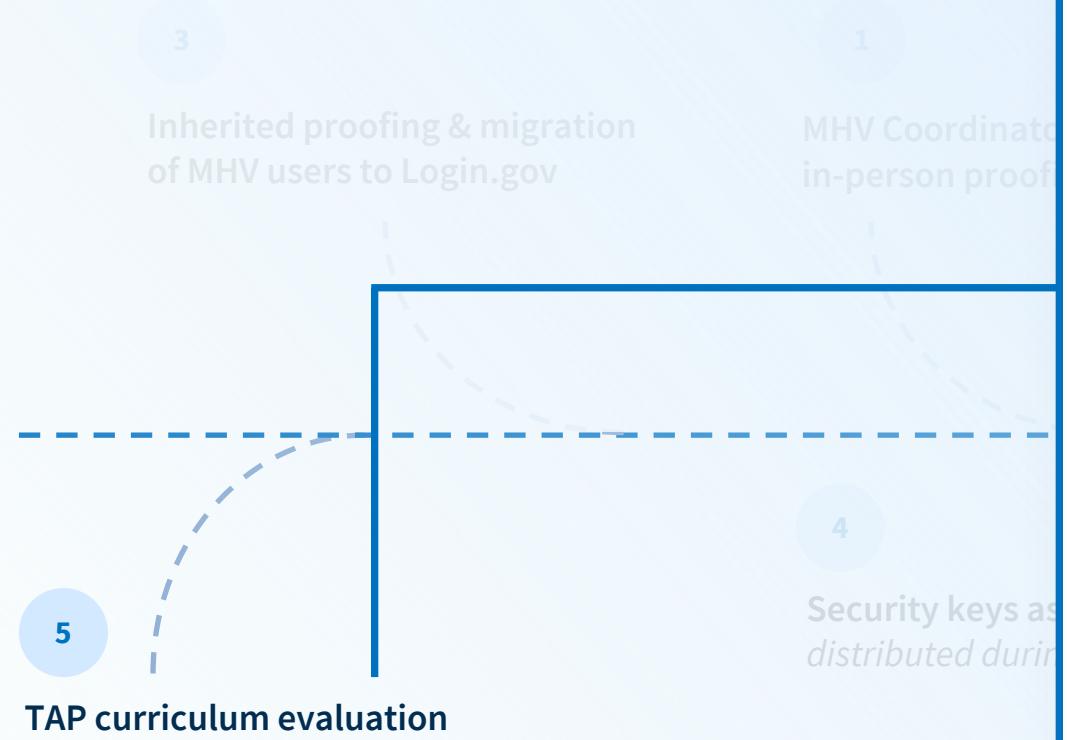
Discovery: Priority #4



Discovery: Priority #5



A status update



Updated TAP curriculum that removes mention of DS Logon and replaces it with Login.gov will be released in **January 2023**.

At this phase, the discovery team has audited the existing curriculum and tracked recommendations in the roadmap for further research and comparative auditing against the newer curriculum.

Recommendation include:

- Conduct **further research with TAP instructors** to better understand the day-of training when Login.gov is introduced
- Promote Login.gov pre-TAP
- Provide clear instructions for a path to help; Extend/promote **in-person assistance** as an option during or following TAP session
- Include visual step-by-step guides for Login.gov; Add specific examples (images of acceptable IDs)
- Have **physical examples** when appropriate (e.g., **security keys**) / offer them to those at the time of the class, to bring home

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

Today, we'll share findings and recommendations, informed by VA staff and Veteran input, across these areas of focus

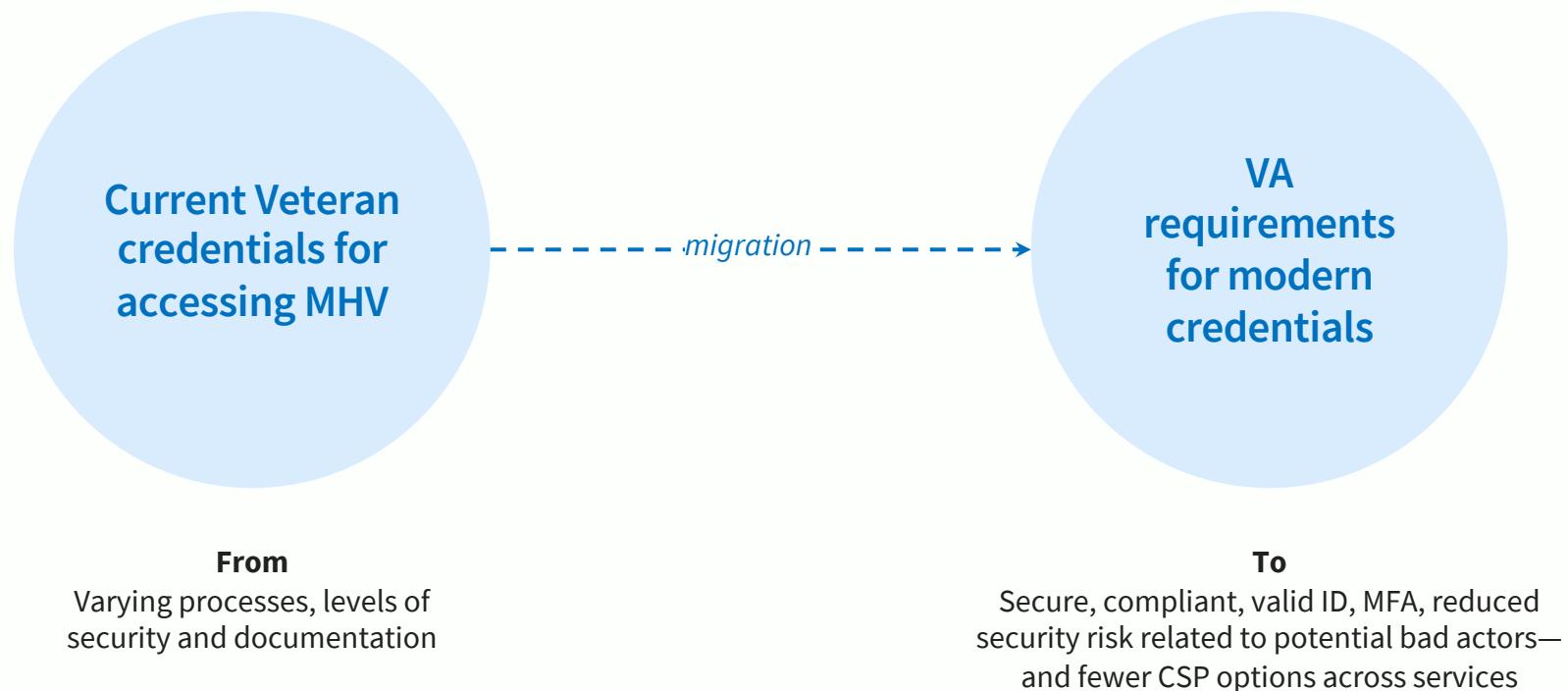
Agenda

Understanding the constraints	13
Shaping our research	30
What we learned	43
The big picture	64
Access and use cases for non-Veteran users	83
From vision to implementation	111
Questions	120

Understanding the constraints

Consolidating the available data that will determine who needs to migrate to Login.gov and what paths will be open them.

To understand possible paths for migration we need to understand where Veterans are coming from and what's required for new credentials



What determines if current credentials meet new ID verification requirements?



NIST 800-63A & IAL2

Current security & compliance standards

There is a degree of interpretation needed when assessing compliance.



VHA POLICY

VA requirements for My HealtheVet proofing



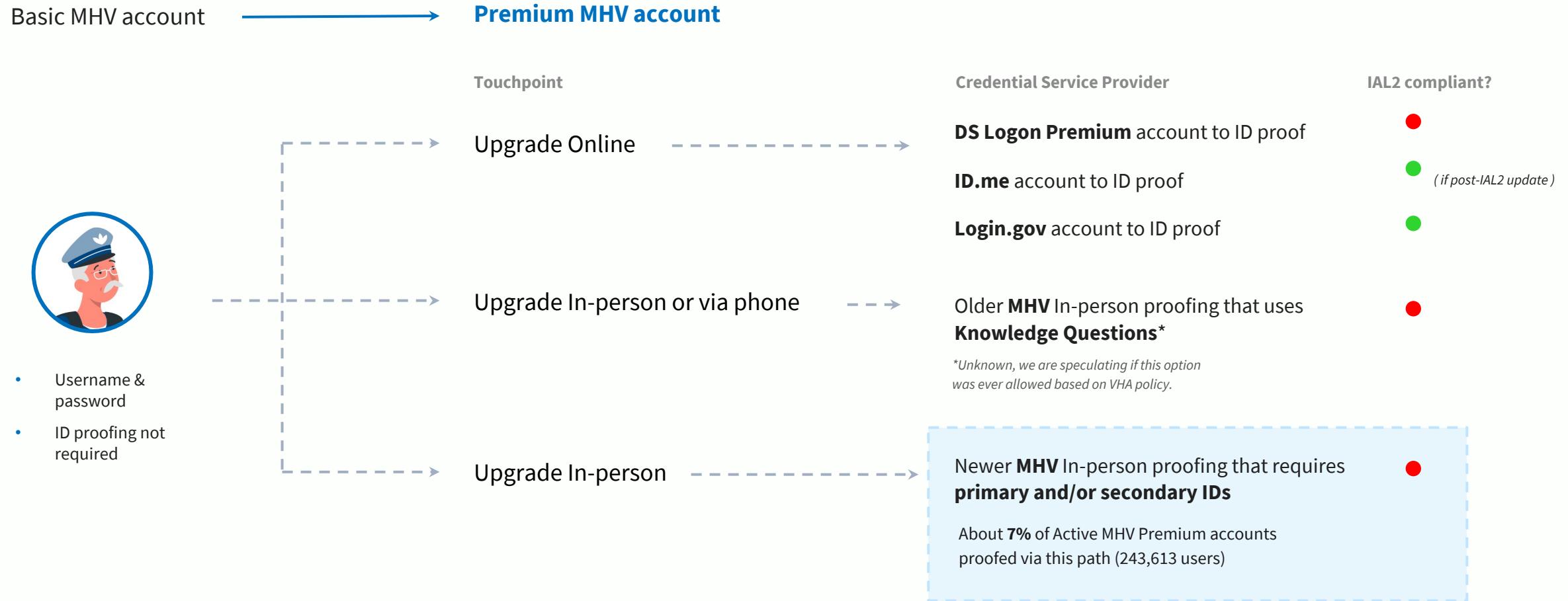
FORM OF ID + PROCESS

The method in which users proofed (form of ID and associated touchpoint, in-person or online)

Training & policies may differ from what, in reality, is being implemented.

Not all credentials for MHV premium accounts are created equal

How Veterans “upgrade” to MHV Premium



Why MHV Premium accounts that proofed in-person are *not* compliant

VHA policy allows the following:

Drivers License is STRONG evidence strength and has been allowed as a **single primary evidence**.

Note: REAL ID cards are STRONG+ and are IAL2 compliant as a single ID evidence

LOWER RISK

VIC cards are FAIR evidence strength yet **allowed as a single primary evidence**.

STRONG+ or SUPERIOR evidence are the only IAL2 compliant options for a single ID evidence

HIGH RISK

In cases where there is a **mismatch** with the VA record and the **primary ID** evidence, a **single form of FAIR evidence**.

For IAL2 compliance, two forms of FAIR evidence are required in addition to the STRONG primary

HIGH RISK

If primary and secondary forms of evidence aren't available, **knowledge-based questions** are allowable.

HIGHER RISK

Also, **ID cards** are not vetted with the issuing source.

MHV must confirm address (phone, postal or email) to be IAL2 compliant; currently no process exists for this, the MHV in-person proofing has no process for this.

ID used for MHV Premium in-person proofing:

- State Issued ID: **96,554**
- Govt Issued ID: **16,719**
- Passport: **836**
- Veteran ID: **129,504**

Potential paths for migrating to Login.gov credential

1

REPROOFING

No information is carried over from previous credentials and Veterans set up Login.gov, an IAL2-compliant credential, that **requires enabling MFA and identity proofing**

2

INHERITED PROOFING

Identity proofing from previous credentials is accepted in place of Login.gov specific identity proofing. **Veterans set up new password and MFA, but are not required to do any additional proofing to have a fully functional Login.gov account.**

3

WAIVED PROOFING, LIMITED ACCESS (GRANDFATHERING)

If this is allowed, Veterans would set up a new password and enable MFA but would skip identity proofing and **receive a reduced-access (IAL1) credential**. Reproofing for full access would be possible at a later date.

Burden on Veterans

Higher

Lower

Evaluating the risks associated with each path

1



REPROOFING

- Login.gov controls the ID proofing process, so no additional risk

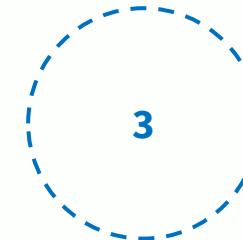
2



INHERITED PROOFING

- For IAL2 compliant proofing, little to no additional risk
- Some non-compliant accounts may be deemed an acceptable risk; Currently considering MHV accounts with in-person proofing

3



WAIVED PROOFING, LIMITED ACCESS (GRANDFATHERING)

- TBD

Burden on Veterans

Higher ←

→ Lower

The risk of *not* complying with IAL2:

Non-IAL2 compliant ID at time of proofing
and/or **not having MFA enabled**

This could allow an entry point for bad actors and a **larger attack vector across government agencies** accepting Login.gov, e.g. IRS.

Even without a security compromise, Login.gov could **risk reputation** for certifying accounts if they claim IAL2, despite not following IAL2 proofing processes.

To further understand risk and which accounts might qualify for inherited proofing, we've requested additional data via IAM

- Do those who proofed in-person **also have** an ID.me, DS Logon, or Login.gov account? What CSP do they use?
- Of the 93% of MHV **users who upgraded online** via DS Logon, ID.me, or Login.gov what **primary forms of ID** used were used?
- How many of MHV Premium users **also have a VHIC**?

For Veterans who don't qualify for
inherited proofing, how can we reduce
the burden of migration?

Consideration: Grandfathering non-eligible MHV Premium accounts to Login.gov as IAL1

Proofing would be deferred until needed (or within a predetermined timeline). Login.gov IAL1 accounts would be reusable across government agencies, although limited access until upgraded.

Benefit to Veteran

Veterans are empowered with a migration alternative if the **burden of reproofing** is too great—or not convenient / too hard without in-person assistance.

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

Benefit to VA

Potentially **expedites migration** of MHV premium accounts, which otherwise cannot migrate via inherited proofing.

Benefit to Login.gov

Reduces risk of inheriting accounts that are not IAL2 compliant.

Additionally, there are a few ways to streamline data input users

We can pull data necessary to generate a Login.gov account from a MHV account **except for:**

- ID proofing evidence (images are not stored)
- Address (not collected), verification if the phone number verification fails

MHV Premium: In-Person proofing	Login.gov, connect to MHV Premium
Name	Name
SSN	SSN
DOB	DOB
Sex	
Email	Email
Phone	Phone
User ID	
Password	Password
Security Questions (2)	

MHV approved IDs	Login.gov 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 Identification Verification (PIV) card	
Common Access Card (CAC)	

The struggle is real: Despite solutions to avoid or simplify ID proofing, account migration poses a major technical challenge for many Veterans

MHV Coordinator key takeaways:

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

-Phillip Walton Jr.

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

-Melissa A. Beals & Renee S. Vharen Ruggles

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

-Ramona J. Dewitt-Morris

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.

-Ramona J. Dewitt-Morris

“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 Coordinator

Experts across the VA warn—mandatory, unsupported migration will leave Veterans behind

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.

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.

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**.

To shape the path forward

It's imperative to understand what paths to Login.gov adoption resonate with Veterans and how we can help them avoid the challenges

A photograph showing a woman with long dark hair in a wheelchair, facing a man who is seated and wearing a patterned shirt. They are in an office setting with a computer monitor on a desk between them. The monitor displays a webpage with the text "LOVE WHAT YOU DO".

VA IDENTITY PRODUCT • Discovery Readout

How we shaped our research

Veteran needs we are aware of when it comes to credentials

Simplicity

Veterans need a simple way to access all VA sites—multiple options create confusion

Guidance

Veterans need efficient customer service and intuitive troubleshooting when they encounter barriers

Trust

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

Friction with purpose

Veterans need ease of use balanced with security requirements to feel like their data is secure

Proprietary government tool

Veterans distrust commercial CSPs to protect their government related data because there is an inherent conflict of interest

Control of data

Veterans take responsibility for their own internet security because they believe they cannot rely solely on the government or a company to fully protect their data

To gain a more in depth understanding of the challenges with CSPs and proofing across VA services, we spoke with the experts:

- 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
- 11. Laurie Baker: VBA, VACO
- 12. Danny Reed: VHIC subject matter expert
- 13. Stephania Griffin: Director, Information Access and Privacy, Privacy Officer VHA

Our research goals

1

Understand how we can **intervene** to ensure that new generations of Veterans use Login.gov or ID.me to access My HealtheVet from the start.

2

Understand what **in-person support** will enable Veterans to create and use a Login.gov account to access My HealtheVet.

3

Understand how the greatest number of Veterans can use **multi-factor authentication**, exploring **security keys** as an option.

4

Understand how setting up and maintaining **shared access** to Veteran information might work for Veterans and non-Veterans.

1

Understand how we can **intervene** to ensure that new generations of Veterans use Login.gov or ID.me to access My HealtheVet from the start.

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.

-MHV Coordinators

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.

-Melissa Rebstock

The lack of coordination between DOD TAP training and VA **TAP training creates redundancy** and confusion, especially around login options.

-Dr. Carla Hill

What we wanted to learn:

- When should proactive intervention encourage the creation of a Login.gov account?
- How do we communicate the value of Login.gov?
- How do we support Veterans and non-Veterans after they set up Login.gov?

2

Understand what **in-person support** will enable Veterans to create and use a Login.gov account to access My HealtheVet.

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.

-Sonja Skinner, MHV Coordinator

VHIC in-person proofing process could be used to initiate a preliminary Login.gov account creation process with inherited proofing. This could eliminate redundant proofing.

-Danny Reed

What we wanted to learn:

- How do we communicate the need to migrate to Login.gov to access MHV?
- When people in-person proof and migrate their account, what issues arise for them?
- What content, resources or workflows can help with challenges during in-person proofing and migration?

3

Understand how the greatest number of Veterans can use **multi-factor authentication**, exploring security keys as an option.

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.**

-MHV Coordinators

[For] Veterans experiencing homelessness (lowest common denominator)... 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.

-Matt Baum

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.

-Login.gov team

What we wanted to learn:

- How do we communicate the value and process of MFA?
- Which MFA options would allow more Veterans to migrate to Login.gov?
- How can MFA support caretakers who need access to certain portions of a Veterans' information?
- If Veterans could opt out of using MFA, would they?

3

Understand how the greatest number of Veterans can use multi-factor authentication, exploring **security keys** as an option.

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

Who most uses VA services:

- Ages 25-34 & 65+ most likely to use VA benefits
- Roughly 1 in 3.5 Veterans have a caregiver
- > 70% urban regardless of age (no major difference in age composition between rural and urban)

Access to technology:

- 47-76% of Veterans own smartphones (lowest ownership & connectivity/financial barriers were rural & older)
- In 2020, 21 of every 10,000 Veterans in the US were experiencing homelessness (<1% of entire Veteran population)

Trust:

- General trend of increasing trust in VA (79%)
- War has led to an erosion in trust for some (i.e., Vietnam Veterans)

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.

3

Understand how the greatest number of Veterans can use multi-factor authentication, exploring **security keys** as an option.

Hypothesized use case for security keys

- Veterans who want an MFA option that does not require accessing other websites/accounts and/or has fewer **fewer steps**
- Those who need an MFA option that **does not require refined movements**—currently all MFA options offered require a typing or time-sensitive element in comparison to a simple button press
- Those who want further **anonymity**: Reduce feeling that govt is tracking user through a network of devices/accounts: a strategy to engage them while maintaining their need to feel safe/independent
- Veterans who want to **share access** to their information (e.g., with a Caregiver), but also know *when* that access is occurring (i.e., sharing a key instead of a pw)

Known 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

4

Understand how setting up and maintaining shared access to Veteran information might work for Veterans and non-Veterans.

When logging in anywhere, it's always assumed that you're a Veteran. **Role-based content strategy** (and access) will lessen the burden on non-Veteran support resources—which are already difficult for these roles to access.

-Laurie Baker

In terms of organizing roles related to delegated access and sharing access to Veteran information, **[organize] roles based on how they are authorized.**

-Stephania Griffin

What we wanted to learn:

- Which non-Veteran users would Veterans choose to set up access for, when and why?
- How do non-Veterans imagine shared access to work for themselves and non-Veterans?



We took these goals into the field for a week of research with Veterans

Quick Guide

VA IDENTITY PRODUCT • Discovery Readout

This Quick Guide is designed to help you Create and Navigate your My healthevet account.

What we learned: Insights and opportunity areas

Our field research was conducted at the Tampa VAMC

Scheduled interviews were held at the Primary Care Annex (PCA). We ran intercepts at the PCA and the Main Facility, in or near Eligibility and Enrollment offices.



We spoke to 37 Veterans who had a range of experiences using My HealtheVet and Login.gov

10 scheduled interviews

90-120 min each

With Veterans who actively use MHV Premium, without a Login.gov account:

- **5** migration & re-proofing scenario
- **5** migration & delayed proofing scenario

24 intercepts interviews

6-20 min each

- **14** with Veterans who actively use MHV with or without Login.gov, focused on migration to Login.gov
- **10** with Veterans who don't use MHV or Login.gov, intercepted during VHIC or other eligibility appointment, focused on proactive adoption of Login.gov

Note: We intercepted 3 additional Veterans who were not migration or proactive, but with relevant experience that could provide insight.

Out of the insights
and patterns in the data,
six opportunity areas
emerged

1. Don't sell me, just tell me
2. Humanized, contextualized, and dedicated help
3. Interactions with the VA are emotionally charged
4. Daily hassle trumps theoretical risk
5. Meet Veterans where they are
6. Trust and life events guide access decisions

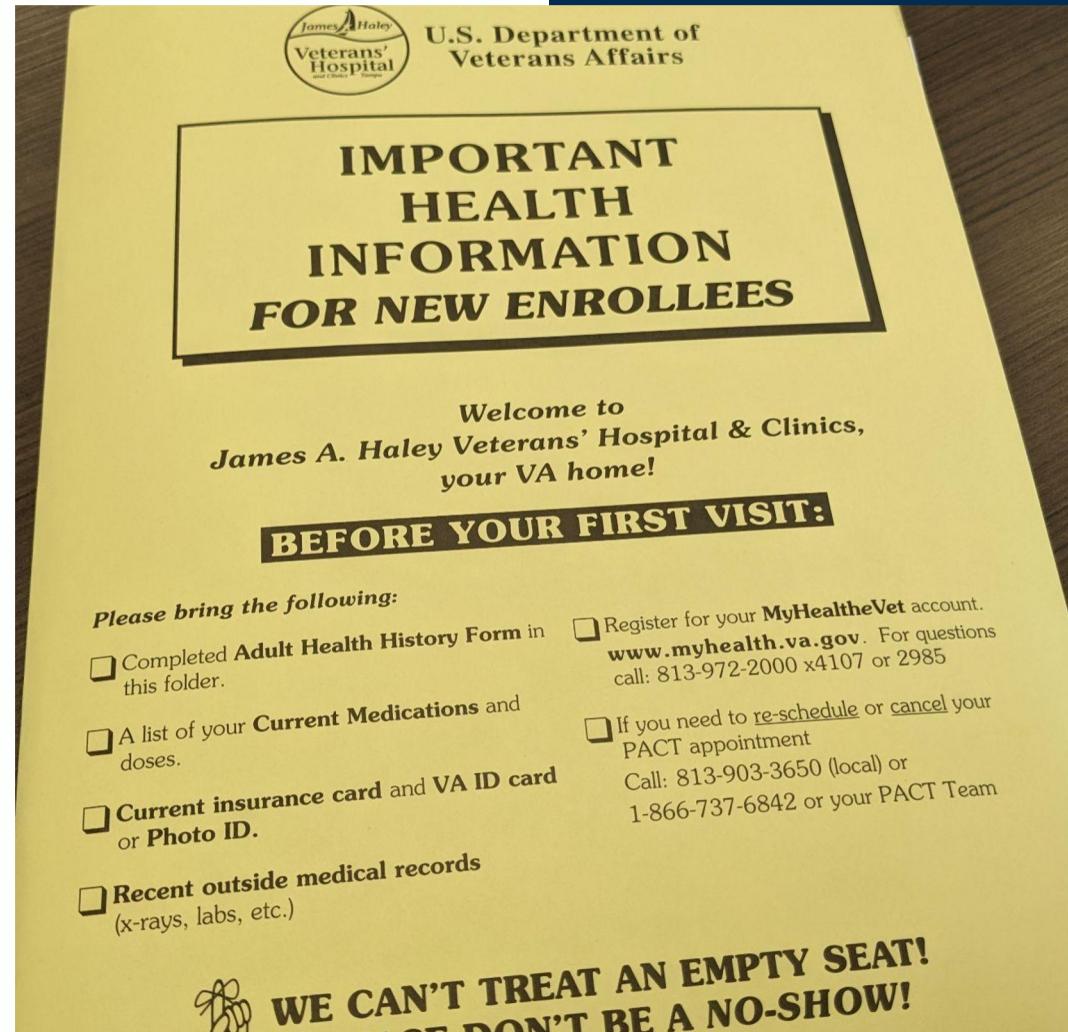
1. Don't sell me, just tell me

“If Login.gov is the preferred method,
the VA has to say that and stop
providing options.”

Participant 9, Veteran Interview

Don't sell me, just tell me

For Veterans, credential service providers (CSP) are a necessary evil. Provide clarity by telling them what is required and then let them be pleasantly surprised by a painless migration and additional benefits, rather than trying to sell them on something that isn't really a choice.



Opportunity area 1

Don't sell me, just tell me

Veteran insights:

- Messaging that suggests setting up a new credential is optional, when it is in fact required is frustrating for Veterans—they want clear instructions about what is expected of them.
- Veterans will choose whichever login credential is most familiar, or appears to be the most direct route to completing a task.
- If Login.gov is the only option available for accessing valued services, Veterans will use it, but they'd like to know the reason for the changing requirements.

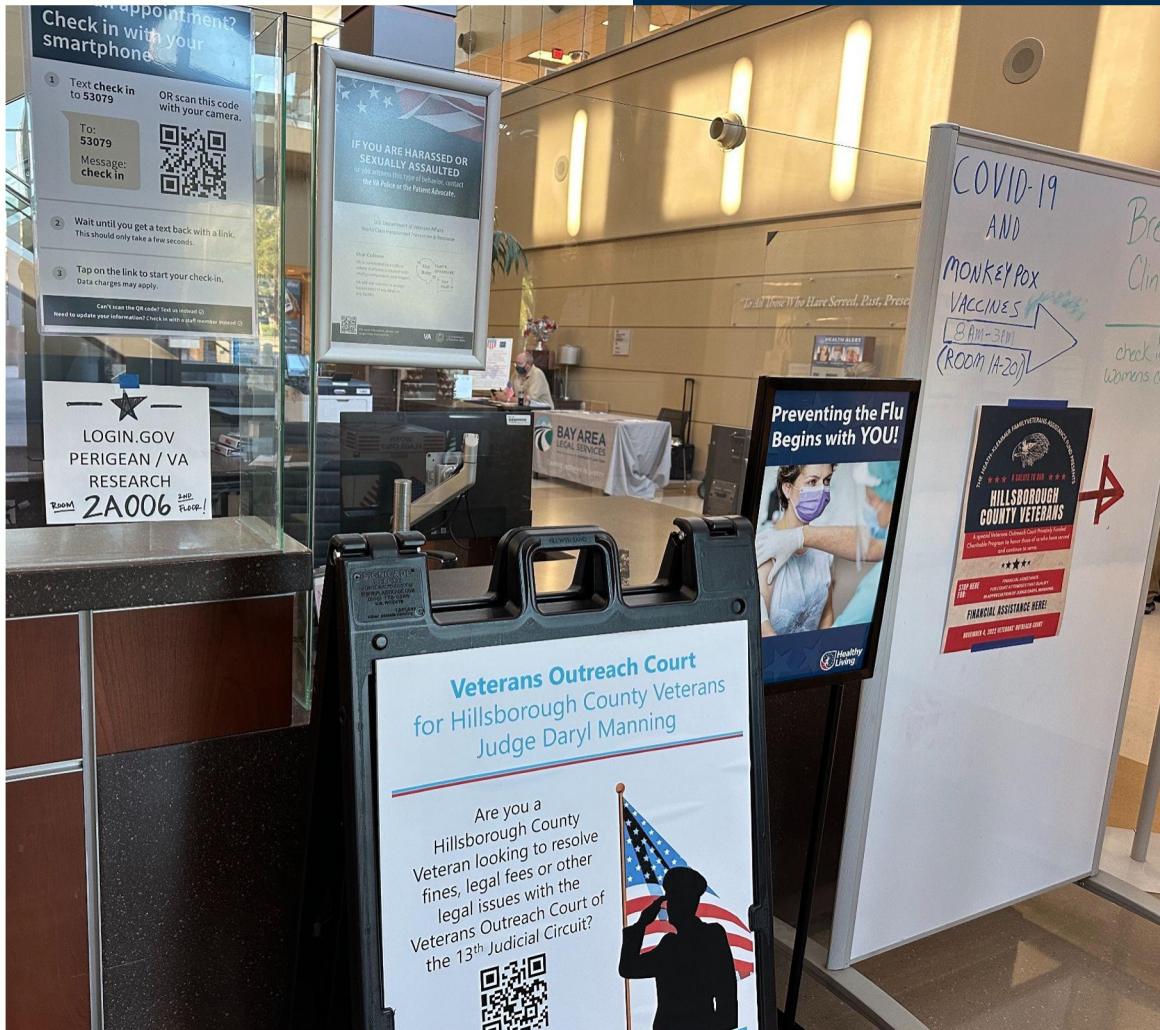
2. Humanized, contextualized, and dedicated support

“I would walk away at this point unless someone is on the phone helping me [with my password].”

Participant 7, Veteran Interview

Humanized, contextualized, & dedicated support

Respect Veteran independence by allowing them to navigate Login.gov set up on their own terms, but provide flexible and dedicated help so they can succeed before giving up entirely. Once they reach the point of frustration, they are lost for good.



Humanized, contextualized, and dedicated support

Veteran insights:

- Knowing that quality, dedicated help is available makes Veterans more willing to try to set up and continue to use a new credential.
- Many older Veterans are highly competent and familiar account creation and MFA. They want to be empowered to do things online themselves, but may have limited troubleshooting skills.
- Building on familiar paradigms and offering proactive support to make the Veteran feel smarter than the system will lower frustration and result in high successful account set up and adoption.
- Rather than requiring Veterans to be able to diagnosis their problem to find a solution, Veterans want a person or artifact, that will speak their language and can guide them through the steps in a way that makes sense to them.
- Even technologically challenged Veterans see benefits in My HealtheVet services, they just need a trusted intermediary who can assist them to set up and learn how to use it.

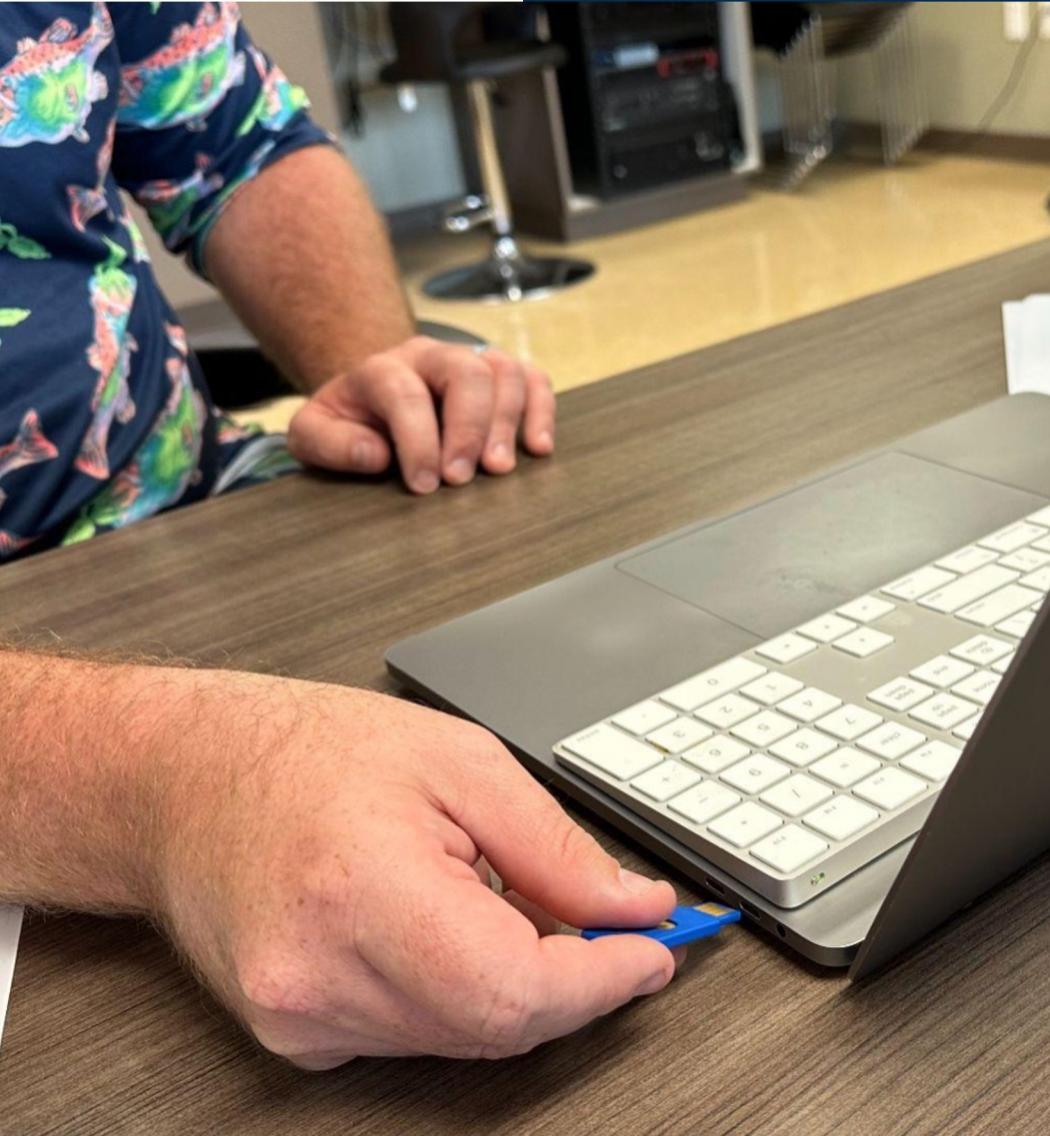
3. Interactions with the VA are emotionally charged

“We’ve all experienced the ‘oh, my God, where’s my rifle!?’ Veterans aren’t going to want to be accountable for [a security key] since there’s too much ingrained trauma there.”

Participant 7, Veteran Interview

Interactions with the VA are emotionally charged

There is a complex mix of trust, skepticism and responsibility that informs Veteran interactions with the VA and each other. Veteran expectations are shaped by military processes, previous experiences with the VA, and loyalty to other Veterans.



Interactions with the VA are emotionally charged

Veteran insights:

- While Veterans might distrust the government, they tend to overestimate its online security and feel it's the responsibility of the VA to make sure things are secure, not theirs.
- Ingrained responsibility for government-issued property undermines the perception that a security key from the VA would be an easy and low-stress MFA option.
- Veterans are eager to share information that will benefit other Veterans, so their experiences can have a ripple effect and impact adoption, good or bad.
- Veterans fear being jerked around and seeing need resources wasted. Transparency around VA decisions and spending serves more than satisfying a curiosity, it instills trust and encourages Veterans to embrace change.

4. Daily hassle trumps theoretical risk

“I understand that they are trying to be secure, but I also know that when it comes to the internet, nothing is under lock.”

Participant 4, Veteran Interview

Daily hassle trumps theoretical risk

Despite a reputation for distrust of systems, and professed skepticism that anything is truly secure online, security was not a major motivator for Veteran choices. They worry about personal privacy but do not really understand the risk or risk factors. When pressed, ease of use wins out over security.



Daily hassle trumps theoretical risk

Veteran insights:

- Many Veterans perceive little risk around their medical information being hacked, but are deeply worried about not being able to access their doctors and prescriptions through My HealtheVet.
- Perceived ease of use drives Veterans' MFA choices—they may want high-security in theory, but choose what they see as an easier option in practice.
- Remembering multiple passwords is a major source of hassle for Veterans. Those who have the most success using new logins long-term, are those who expect to forget passwords, and find workarounds that don't rely on memory.
- Biometrics can at first feel like a violation, but through repeated exposure, it is increasingly embraced as an easy option requiring no memory. When choosing an MFA option, Veterans weigh intrusiveness against ease of setup and continued use.

5. Meet Veterans where they are

“Yes, I would set up Login.gov at the end of my doctor’s appointment, while I’m here. I’d rather get more done in a single period, than do it later.”

Participant 26, Veteran Intercept

Meet Veterans where they are

Build on existing points of interaction and familiar experience to make login.gov set up as convenient as possible for Veterans.



Meet Veterans where they are

Veteran insights:

- Setting up Login.gov alongside another VA appointment is a welcome convenience for Veterans, as long as it represents a definitive start or end to the process—don't create another ongoing process to manage.
- While Veterans appreciate bundling tasks with appointments, bundling communications causes confusion and fear around doing something wrong.
- Moving between online and offline touchpoints can create confusion – but clarity on what to bring, why you're identity proofing and how it won't affect your existing appointments or accounts, helps put Veterans at ease.

6. Trust and life events guide access decisions

“It depends on my trust in the person who I give access, what I would give them access to. My husband could have full access, but my children, would be able to see my medications only.”

Veteran Intercept

Trust and life events guide access decisions

Use smart defaults and simple customizations to make managing shared access so simple that Veterans put it in place before they need it.



Trust and life events guide access decisions

Veteran insights:

- Veterans don't think to set up shared access until life-altering events make it necessary for others to have access to their information.
- Shared access asks Veterans to consider who they trust and who will take care of them in the future, which can evolve or change over time.
- With more complex care situations, caretakers recognize the need for nuanced permissions when accessing a Veterans' information.
- Veterans and their support systems find it important that a Veteran is able to grant and revoke shared access and see exactly what has been accessed by others.

And by consolidating into a set of 7 insights, this research can be useful beyond this program and across the VA

1. Setting up a new credential is frustrating for Veterans if it's made to seem like a choice or the need is unclear.
1. Veterans see security as the VA's responsibility, but they're motivated to be more careful if they feel they're at risk of not being able to access their benefits, or they understand how their actions affect fellow Veterans.
1. Bundling identity proofing with other appointments, and moving it to the beginning or end of the account set up process, makes it more convenient for Veterans.
1. Veterans will choose whichever login credential is most familiar, or appears to be the most direct route to completing a task.
1. Perceived ease of use and paradoxical views about security inform Veterans' multi-factor authentication choices.
1. Veterans don't think to set up shared access until life altering events make it necessary for others to have access to their information.
1. Having humanized, contextualized and dedicated support available motivates Veterans to set up and continue to use a credential.

The big picture, an end-to-end view

Service blueprint and moments that matter

1ST FLOOR

CLINIC ADMINISTRATION

EDUCATION & TRAINING

HPACT

LAP & RADIODIAG

PRESSCRIPTION RECEIVING

P / PR / ST / TICS

VOLUNTEER

WOMEN'S CENTER

VA POLICE

2ND FLOOR

DENTAL SERVICE

ALPHA CLINIC

BRAVO CLINIC

PODIATRY

SITEHEALTH

CHARLIE CLINIC

DELTA CLINIC

PATIENT ADVOCATE

2B101A

2B601A

2B701A

2A201A

2A101A

2A007

The Service Blueprint explores how we can connect *in-person services* and *digital modifications* to improve the experience of migrating to Login.gov.

We highlight three Veteran journeys with a focus on re-proofing with in-person support

Veteran journeys | The major phases the Veteran experiences are shown sequentially, including the detailed steps and where the experience may shift from online to in-person.



Re-proofing

Create a Login.gov account online and ID-proof online or in person



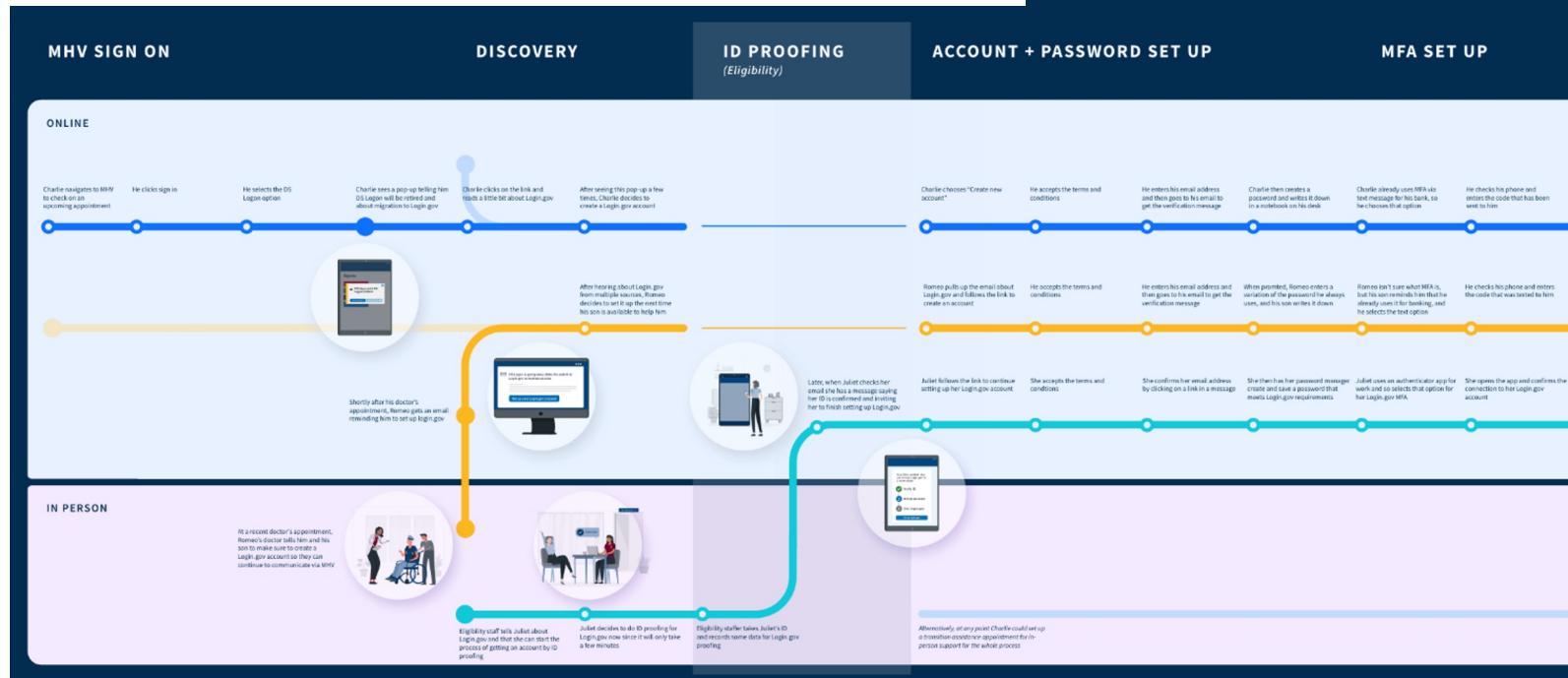
Inherited proofing

An existing account is migrated to Login.gov without ID-proofing



Proactive proofing

Create a Login.gov account during Eligibility and ID-proof first, in person



The blueprint demonstrates how people, processes, and technical capabilities interact to deliver a valuable experience.

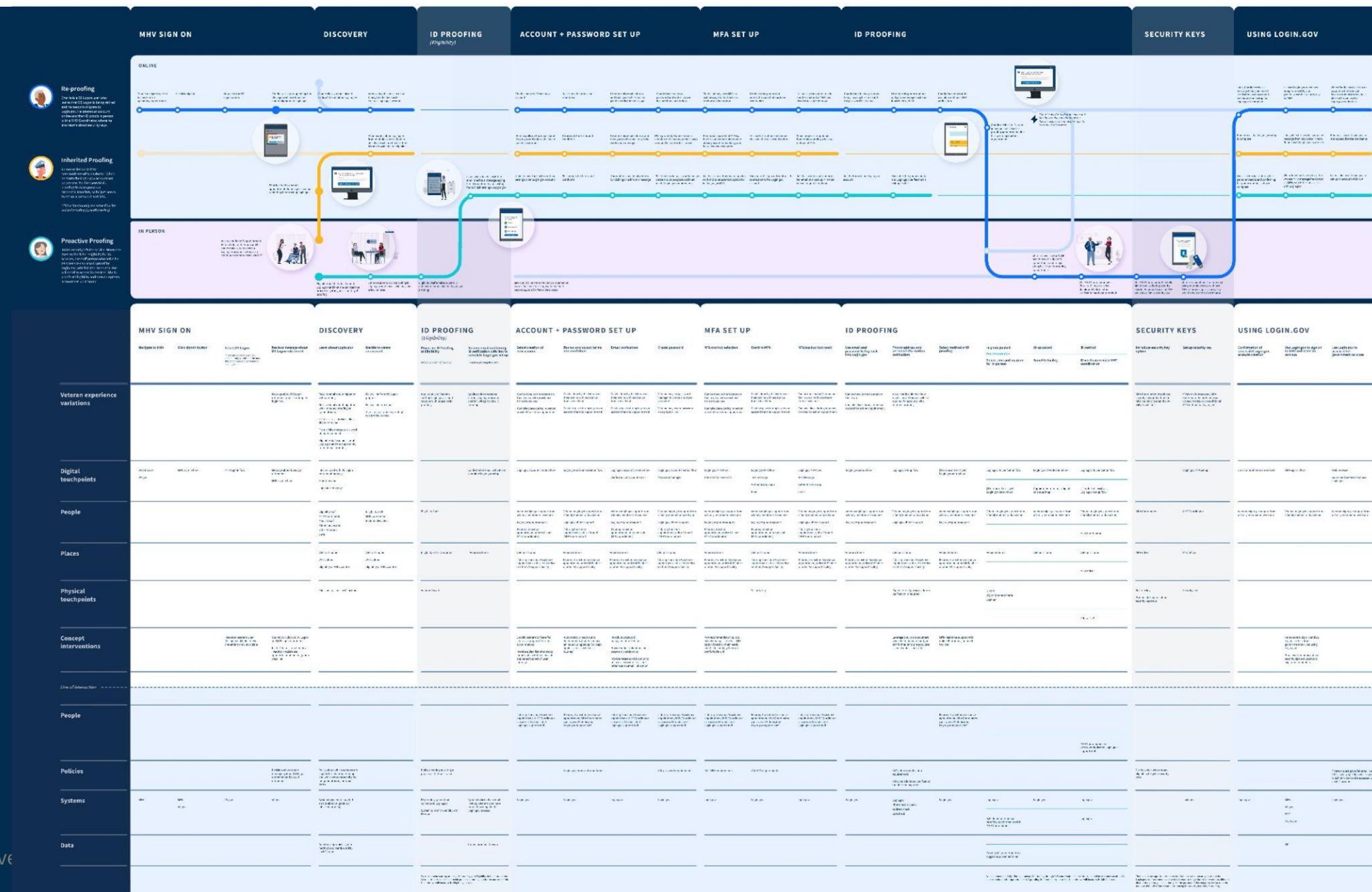
People & places | Identifies what employees & partners (Login.gov) are doing to support the customer experience. Includes systems interaction, ongoing processes, hand-offs, and direct Veteran contact.

Touchpoints & interventions | Identifies what partners are doing, in context, via which touchpoint and for what purpose. Includes in-context description of systems and interactions within the organization.

Policies & systems | Identifies the behind-the-scenes applications and software necessary to support Veteran and employee experiences.



Let's take a look...



Moments that matter

There are many paths to migrate to Login.gov, and many ways to start the process

Key considerations

Communication:

- Tailor communication for particular migration path, provide only details relevant to that path

Experience:

- Intercept users when it is contextually relevant but don't ruin the flow of their other activity
- Allow Veterans time to adapt to the upcoming change

Service:

- Insure support is in place before starting Veterans down any of these paths



Veterans follow varied paths to Login.gov. Migration from an existing credential may require re-ID proofing, or they may be able to skip ID proofing if they have inherited proofing or are being grandfathered in. With each of these variations a Veteran may be inspired to start the process by an email communication, pop-up or conversation with a VA services provider.

Consistent, contextual reminders, will be key to insuring DS Logon users migrate

Communication:

- Be consistent in messaging about date DS Logon retires and what is required

Experience:

- Allow user multiple exposures to prepare for change
- Don't prevent users from completing intended task
- Give user necessary information to pick a convenient time for account creation

Service:

- Identify DS Logon users and intercept

An official website of the United States government. [Here's how you know](#).

Talk to the Veterans Crisis Line

Search Contact Us

U.S. Department of Veterans Affairs

Benefits and Health Care About VA Find a VA Location

Sign in

me > Sign in

sign in

LOGIN

ID.me

DS Logon

My HealtheVet

Set up Login.gov Continue to DS Logon

⚠ 127 days until DS Logon retires

DS Logon will no longer be available to access services like MyHealtheVet starting Sept. 1, 2023.

Please create a Login.gov account now to ensure continued access to all your VA information.

or create an account

Create an account with Login.gov

Create an account with ID.me

Learn more about choosing an account

When a Veteran signs into MHV with DS Logon they encounter a modal with a countdown of how long until DS Logon retires and what is required of them. They have the option to set up Login.gov now or continue with DS Logon for the time being.

Reach out to Veterans who are struggling and offer support on their terms

Communication:

- Connect communication to the Veteran's attempt to set up Login.gov
- Be transparent about source of information

Experience:

- Follow up quickly while process is still fresh in the Veteran's mind
- Be proactive about offering help so Veteran does not become completely frustrated and disengaged
- Make it easy for the Veteran to pick up where they left off

Service:

- Empower support staff with all the context needed to help Veteran



Setup for your Login.gov account is incomplete

Dear Veteran,

Access to your VA services and benefits through DS Logon will end on August 29, 2023 and we noticed that you have not yet completed setup for your account on Login.gov. To see where you left off and complete setup for your account, visit www.login.gov.

If you are having trouble and need assistance, the following options are available:

- 1 Visit [\[insert url here\]](#) to learn more about a representative who can help answer questions.
- 2 Call the [\[insert name of office\]](#) at (x) to speak with someone over the phone who can help complete, step-by-step.
- 3 Schedule an in-person transition appointment by visiting: [\[insert url here\]](#)

We want to make sure you keep uninterrupted access to MyHealtheVet and VA.gov, so reach out if you need help.

When a Veteran abandons the account creation flow for Login.gov, they receive a follow-up email giving them the option to resume the process on their own or to get support across a variety of channels. It also reiterates the need to migrate to Login.gov before other options are retired.

Time remaining to complete setup

29 days, 8 hours, 37min

Online async processes and in-person support with clear transitions between them are necessary for migrating Veterans to Login.gov

Communication:

- Clearly communicate what has happened in past phase of process, whether in person or online, and how that connects to what will happen next

Experience:

- Schedule in-person support before or after existing VA appointments whenever possible

Service:

- Empower support staff with all the context needed to help Veteran

Your identity has been verified. Here are your next steps

[First Name],

Thanks for completing the identity verification process. Now that we have verified your identity, the next step is for you to create an account on Login.gov so that you can access all of your VA benefits and services online.

1 Verify identity
Verify identity in-person or online
Completed Today, 11/23/2022

2 Create your account on Login.gov
Complete the following steps to create Login.gov account

- Visit www.login.gov, click on “create an account” to get started. You will be asked for basic information such as a username and password
- Set up Multi-Factor Authentication for your account. If you’re not familiar with this, watch this short video explaining it

3 Sign-in with Login.gov
Sign-in to your new Login.gov account to access all of your services

[Set up your Login.gov Account](#)

VA - Appointment with Dr. Arva
3:00 PM - 4:00 PM

VA - ID Proofing for Login.gov

MHV coordinators are used to ID proofing and helping Veterans navigate account setup. Let's build on this trusted relationship.

Communication:

- When asking for information Veterans have already provided, acknowledge it and explain why

Experience:

- Allow Veterans to choose to get in-person support without having to fail online first
- Allow Veterans to use VHIC for ID proofing

Service:

- Empower MHV coordinators with responsive Login.gov support so they can get necessary information to help Veteran
- Create dedicated interface for VA staff to do ID proofing



Veterans can bring their identification to MHV coordinators, who they already trust, to complete the required ID proofing for Login.gov. Additionally, MHV coordinators have access to the necessary information and support from Login.gov to help Veterans determine the status of the account creation and troubleshoot any problems.

Tailored Communications about migration to Login.gov based on VA standards

VA COMMUNICATION GUIDANCE

Consistent. We use words consistently to inspire trust and confidence in our customers.

Conversational. We use everyday human words and plain language whenever possible. We talk like a human, not like Government.

Clear and helpful. We break down complex information into simple, snackable chunks, and provide it progressively, when and where they need it, so it's easy to find, easy to understand, and not overwhelming.

Empathetic. We talk person-to-person with our customers, and use language that puts the person first, not the disability, condition, age, gender, or race.

Align on consistent language to talk about “required” CSPs, and CSPs that will be “retired”. Remind users every time they login. Set a date and stick to it.

Tailored Communications about migration to Login.gov based on VA standards

VA COMMUNICATION GUIDANCE

Consistent. We use words consistently to inspire trust and confidence in our customers.

Conversational. We use everyday human words and plain language whenever possible. We talk like a human, not like Government.

Clear and helpful. We break down complex information into simple, snackable chunks, and provide it progressively, when and where they need it, so it's easy to find, easy to understand, and not overwhelming.

Empathetic. We talk person-to-person with our customers, and use language that puts the person first, not the disability, condition, age, gender, or race.



Shoot straight with Veterans. Tell them that they have to transition to either Login.gov or ID.me.

Tailored Communications about migration to Login.gov based on VA standards

VA COMMUNICATION GUIDANCE

Consistent. We use words consistently to inspire trust and confidence in our customers.

Conversational. We use everyday human words and plain language whenever possible. We talk like a human, not like Government.

Clear and helpful. We break down complex information into simple, snackable chunks, and provide it progressively, when and where they need it, so it's easy to find, easy to understand, and not overwhelming.

Empathetic. We talk person-to-person with our customers, and use language that puts the person first, not the disability, condition, age, gender, or race.

Tell Veterans what is required. List steps, the expected time to complete them, and any required documentation.

Tailored Communications about migration to Login.gov based on VA standards

VA COMMUNICATION GUIDANCE

Consistent. We use words consistently to inspire trust and confidence in our customers.

Conversational. We use everyday human words and plain language whenever possible. We talk like a human, not like Government.

Clear and helpful. We break down complex information into simple, snackable chunks, and provide it progressively, when and where they need it, so it's easy to find, easy to understand, and not overwhelming.

Empathetic. We talk person-to-person with our customers, and use language that puts the person first, not the disability, condition, age, gender, or race.

Understand that this can be daunting for Veterans. Assure them of available help but don't belittle them or make assumptions about what they can and can't do.

Migration to Login.gov specific communication considerations

Awareness-focused

Provide context and rationale for the change like the changing security landscape and the security requirements from the federal government.

Action-focused

Provide basic overview information about the activity such as how long it will take and what steps are involved and detailed information about the immediate next step

Solely Login.gov-focused

Users only reason for engaging is their interest in Login.gov so it's important to connect to what motivates them. Their focus is undivided, so it's a good opportunity to communicate nuanced information.

Part of larger communication or experience

User's attention is split and they may not expect to consider Login.gov so it is important to focus on the convenience or other benefit of acting on Login.gov now (like as part of another appointment). Avoid information overload.

Geared to a general audience

Focus on what is relevant across all Veterans, like reason for migration to Login.gov. Avoid creating confusion by providing details for a use case that's not their own (e.g., if I have inherited proofing, I don't need details of the in-person proofing option).

Tailored for a specific Veteran or group

Build on the information that the Veteran has already shared and be transparent about where information is coming from.

Key internal and external communication touchpoints

Veteran facing:

- TAP Curriculum
- Websites (banners, pop-ups, etc.) VA.gov / eBen / MHV
- MHV Appointments
- VHIC Appointments
- Stand-Down
- Email
- Newsletter
- VSO
- VA Notify (Text Alerts)
- VA YouTube Channel

Internal facing:

- Internal Memo
- Identity Working Group Session
- (regular team meeting)
- Monthly SSOe partner meeting
- Digital modernization council

Key partner:

Veteran Experience Office, especially communication department

10 minute break

Access needs for non-Veteran user roles

Caregivers, Delegates, and Beneficiaries

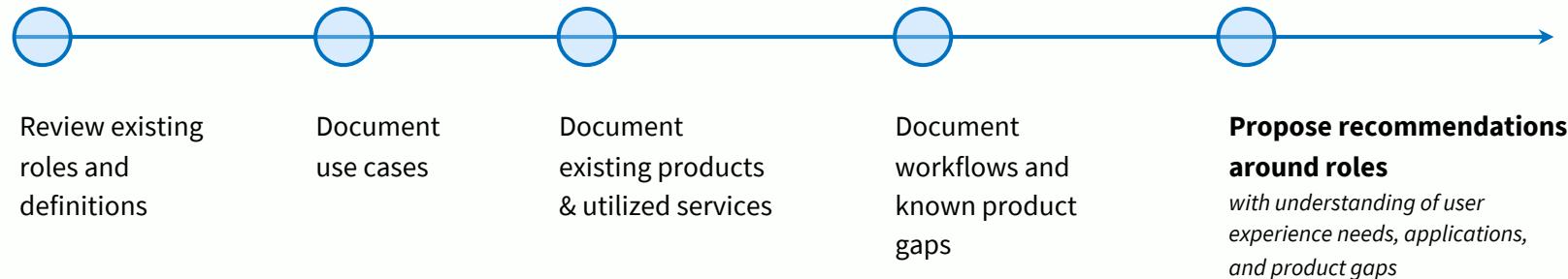
Discovery: Priority #2



Discovering Non-Veteran User Roles (*i.e. the NVUR-ending story*)

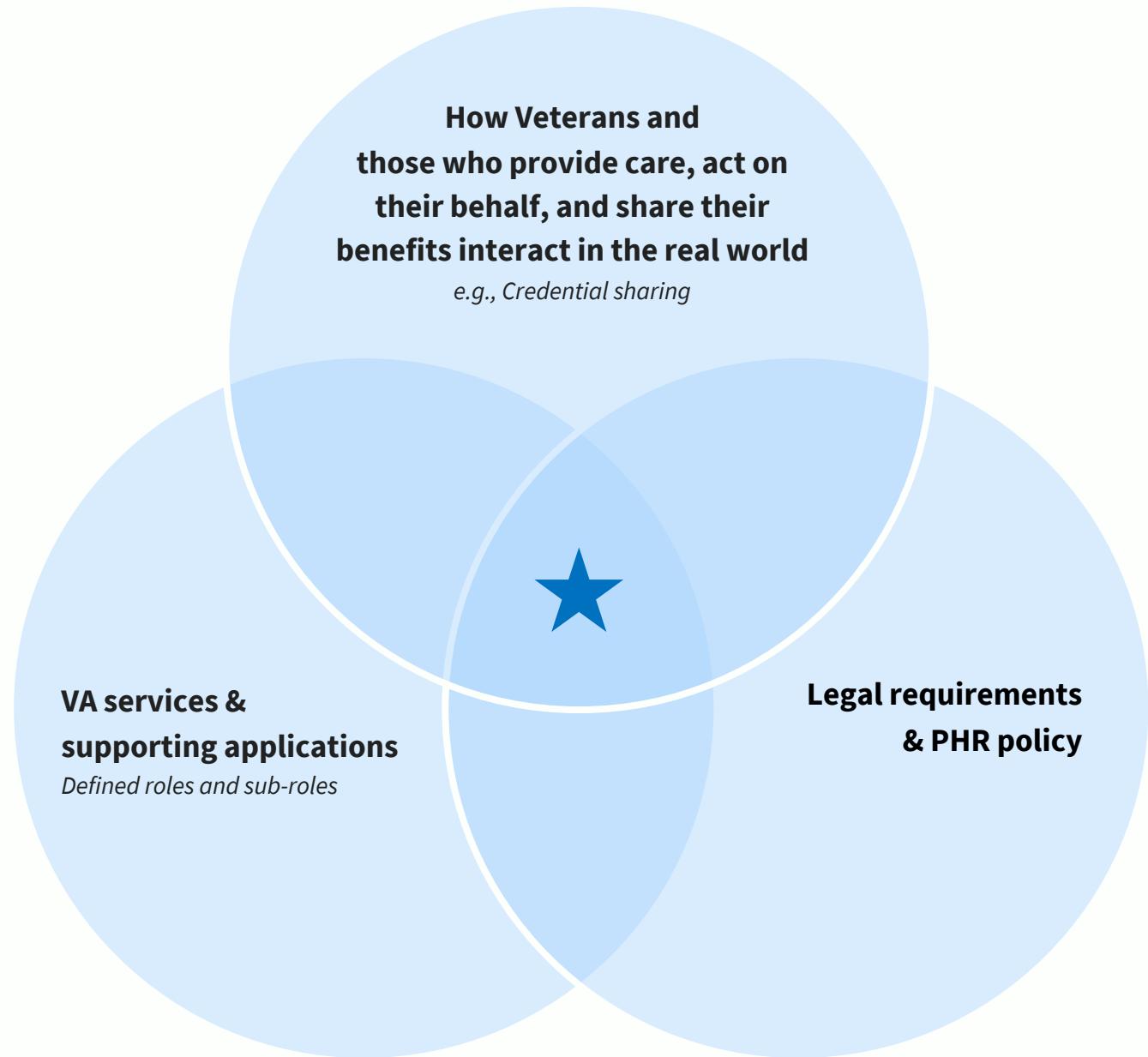
In order to understand potential credential adoption for non-Veteran user roles, focusing on Caregivers, Beneficiaries, and Delegates, we explored **high-level interactions and uses cases around non-Veteran user roles**, their corresponding applications, and access points as they pertained to VA Services.

Our activities:



What did we find?

- A complex interaction between Policy, Services and the lived experiences of Veterans and their loved ones
- A lack of consistency in how terms are used and what features are available between departments and services
- Opportunities to evolve service and products to better serve Veterans and those who support them
- Our initial findings focus primarily on delegates and proxies, addition exploration on the needs of beneficiaries and caregivers is recommended



“So from the VA clinician side, there, [for] non-Veteran roles, [it’s] not the role, but the relationship. Like, what is your relationship? How do you know this Veteran? ... This is my friend, ... or this is the person who drives me. That's coming from the doctors.”

Carnetta Scruggs

Understanding the difference: Role & Relationship

Role:

The responsibilities, benefits, and permissions assigned to an individual as defined by VA policies based on that individual's relationship to the Veteran and the VA. Attributes of a role tend to be clearly defined.

Roles include:

- Power of Attorney
- Surviving Spouse
- Emergency Contact
- Caregiver [Beneficiary]

Relationship:

The connection and way of interacting between a Veteran and another individual based on personal, familial, and/or professional connections. Attributes of relationship tend to exist on a continuum.

Relationships include:

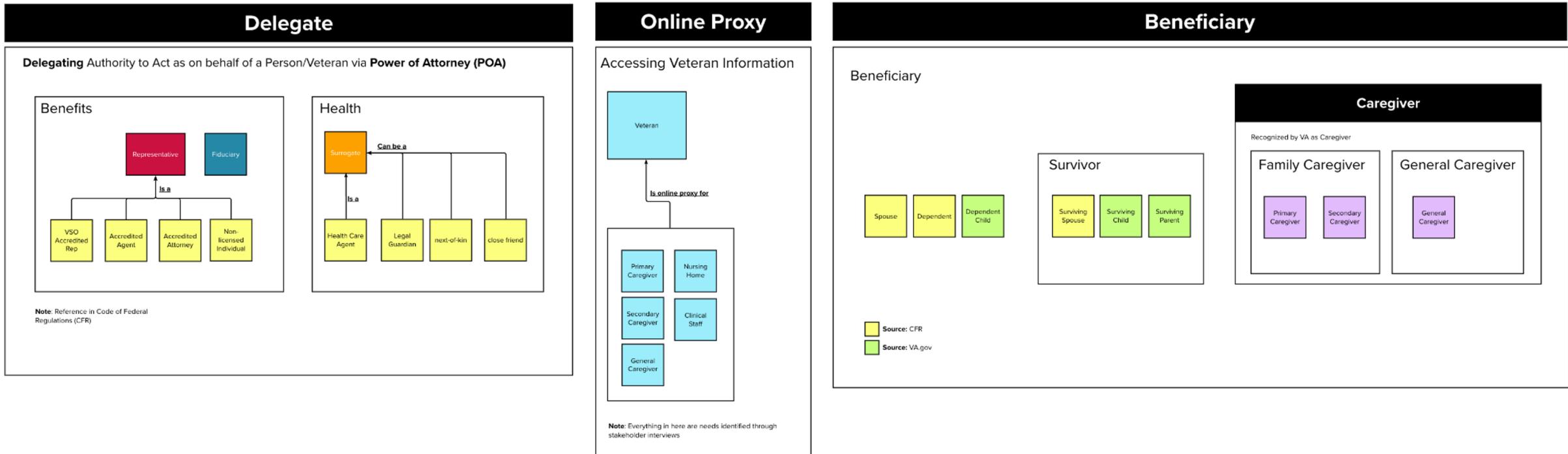
- Partner
- Child
- Neighbor
- Friend
- Caregiver

Understanding the difference: Role & Relationship

Recommendation: Although there is obviously some overlap, being explicit about the difference between roles and relationships, and understanding the limits of the VA's ability to define or understand relationships, will support VA-wide alignment on definitions.

Understanding the Roles

We were initially charged with focusing on the roles of **Delegate**, **Beneficiary** and **Caregiver**. We added **Online Proxy** to the this list.



Caregiver confusion: Defined role vs. range of relationships

Caregiver only exists as an official **role** relative to the VA in terms of the support and benefits provided for the caregiver through two programs:

- Program of Comprehensive Assistance for Family Caregivers (PCAFC)
- Program of General Caregiver Support Services (PGCSS)

There is nothing about the definition of this role that implies anything about access to Veteran information.

Caregiver is used constantly in a colloquial manner to refer to a range of **relationships** with Veterans that run the gamut from a partner in an interdependent relationship who picks up a Veteran after a medical procedure all the way to a loved one or professional upon whose care the Veteran is completely dependent.

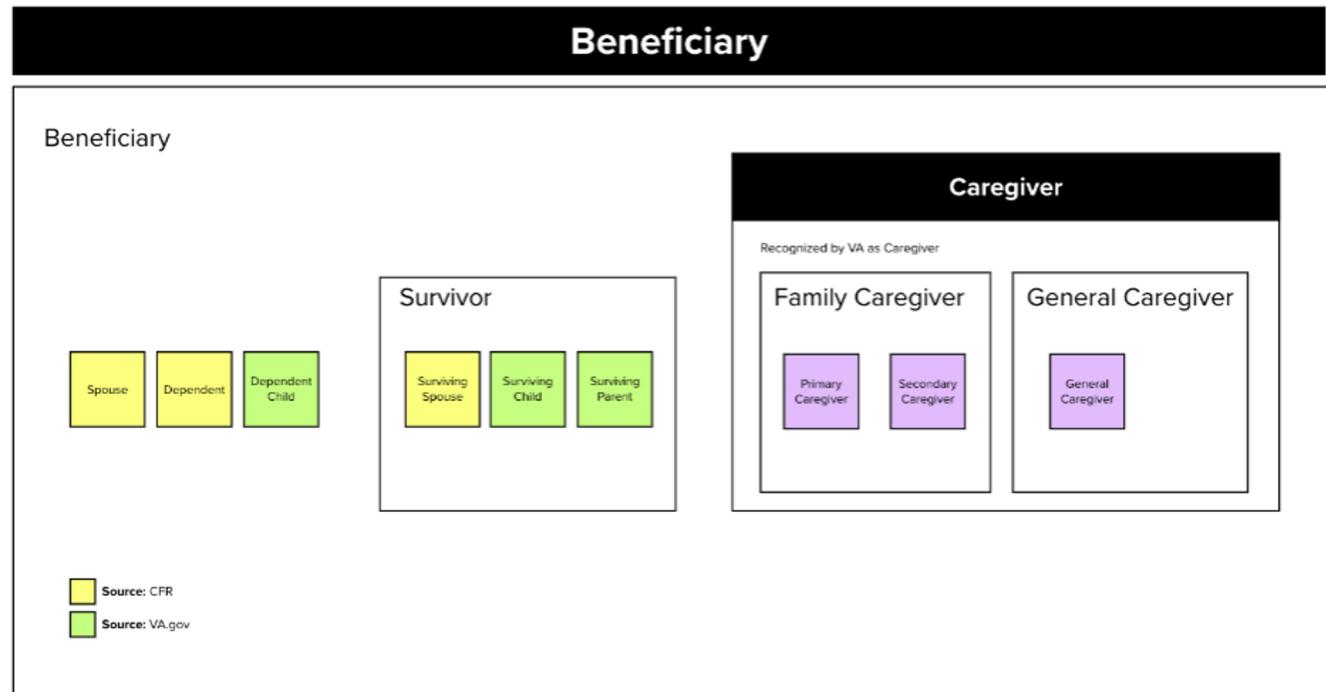
Thus a caregiver could have no access to Veteran information, could have partial or total proxy access, or could have been delegated complete authority to manage Veteran healthcare and benefits.

Caregiver confusion: Defined role vs. range of relationships

Recommendation: Although it is not realistic to stop using caregiver colloquially, we recommend avoiding this language when talking about access to Veteran information, and instead focus on delegated authority or granted proxy access.

The Caregiver Role

The **Caregiver** role is under the umbrella of **Beneficiary**. Caregivers that are recognized by the VA, whether they are family or general, will receive benefits and as such are deemed as beneficiaries. The difference between family and general caregiver is driven by the type of benefits they have access to. There are some varying experiences for caregivers between VHA and VBA related to what they are authorized to do and how it is enforced



Delegate: Legal transfer of Authority

Delegate: Individuals who have been legally delegated the authority to act on behalf of a Veteran for specific authorized actions, which may include logging into the veteran's accounts to view and update their information.

For the VA, that delegation of authority is based in some legal premise, statute or otherwise, e.g. 38 CFR § 17.32 and 38 CFR § 14.629.

Common types of delegates:

- Surrogate: Durable Power of Attorney to make healthcare decisions
- Fiduciary: Durable Power of Attorney for financial decisions
- Accredited representative: Limited Power of Attorney for Claims

Delegate: Legal transfer of Authority

Recommendation: The concept of delegation is a legal term that exists outside of VA policy and so internal VA usage should align to that definition. Currently, VA employees use ‘delegate’ to mean someone who the Veterans has voluntarily granted access to their information, we recommend aligning on another term to distinguish this meaning. Currently proxy is used by some parts of the VA.

“You gotta get [them]... 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 [...] path.”

Carnetta Scruggs

Veterans need the ability to voluntarily grant access

Proxy access:

Veterans who are not incapacitated want to be able to give their loved ones and care providers partial or total access their VA benefits and healthcare information for a variety of reason from being temporarily out of the country to having increasing trouble navigating technology because of age or disability.

Dimensions of Proxy access to consider

- Read vs. edit access
- By type of service and type of information

A source of confusion:

Currently much of the work that has been done to support this use case is called the “**Delegation Toolkit**” which creates confusion because this is not technically delegation by the legal definition, but voluntarily granting access.

Veterans need the ability to voluntarily grant access

Current work around:

Veterans frequently choose to share their credentials with loved ones and care providers as the easiest, and in some cases only, way to share access to their VA information.

Unless they have had a bad experience, many Veterans do not see the need for creating a separate account to share access to information.

Communicating to Veterans, and those would share with, the benefits of separate accounts will be an important part of implementing shared access.

What's the problem:

- No ability to control level of access
- Many MFA solutions require having access to the Veteran's devices or other accounts
- Changing relationships can mean the information is no longer safe with another person
- Changing circumstances can mean the Veteran no longer needs for someone else to have access

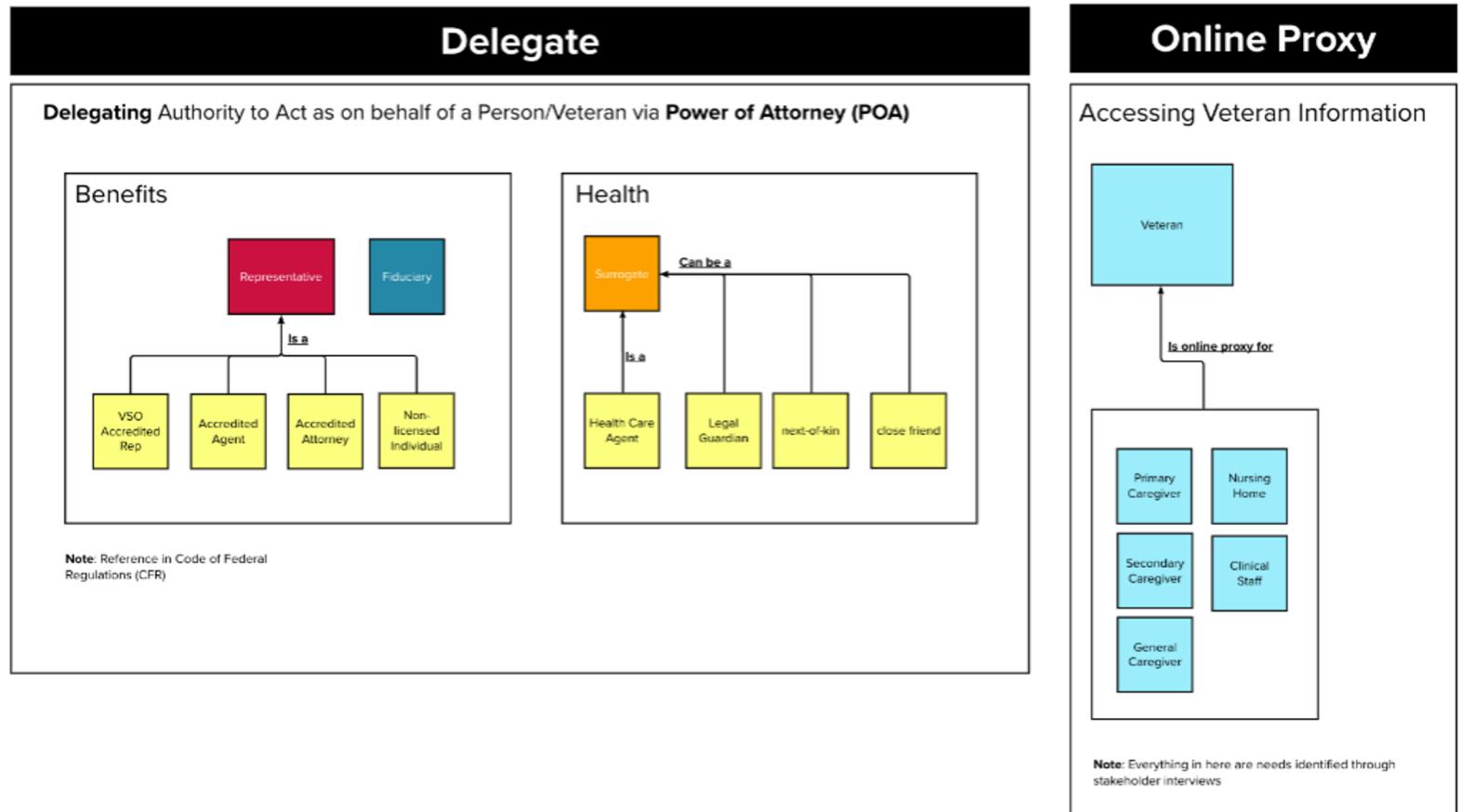
Veterans need the ability to voluntarily grant access

Recommendation: Align on the need for proxy access that can be granted and revoked by the Veteran and align on name for this voluntary granting of access (could be proxy or another term).
Rename the “Delegation toolkit” to the “Proxy toolkit” or similar.

The Delegate vs. Online Proxy

The Delegate and Online Proxy roles can be functionally similar and can be supported by overlapping tools. However, the location of authority is the key difference between them.

Also, whereas delegates always have read and edit access, proxy access should allow for either read only or read and edit access.



While hugely important, healthcare is not the only place non-Veterans need access

Access to healthcare information:

Healthcare has been a primary focus for research on non-Veteran user roles (delegates and proxies) and without question the ability to complete health tasks on behalf of the Veteran is the primary need.

Health Tasks:

- Ordering prescription medication
- Communicating with doctors
- Viewing appointment information

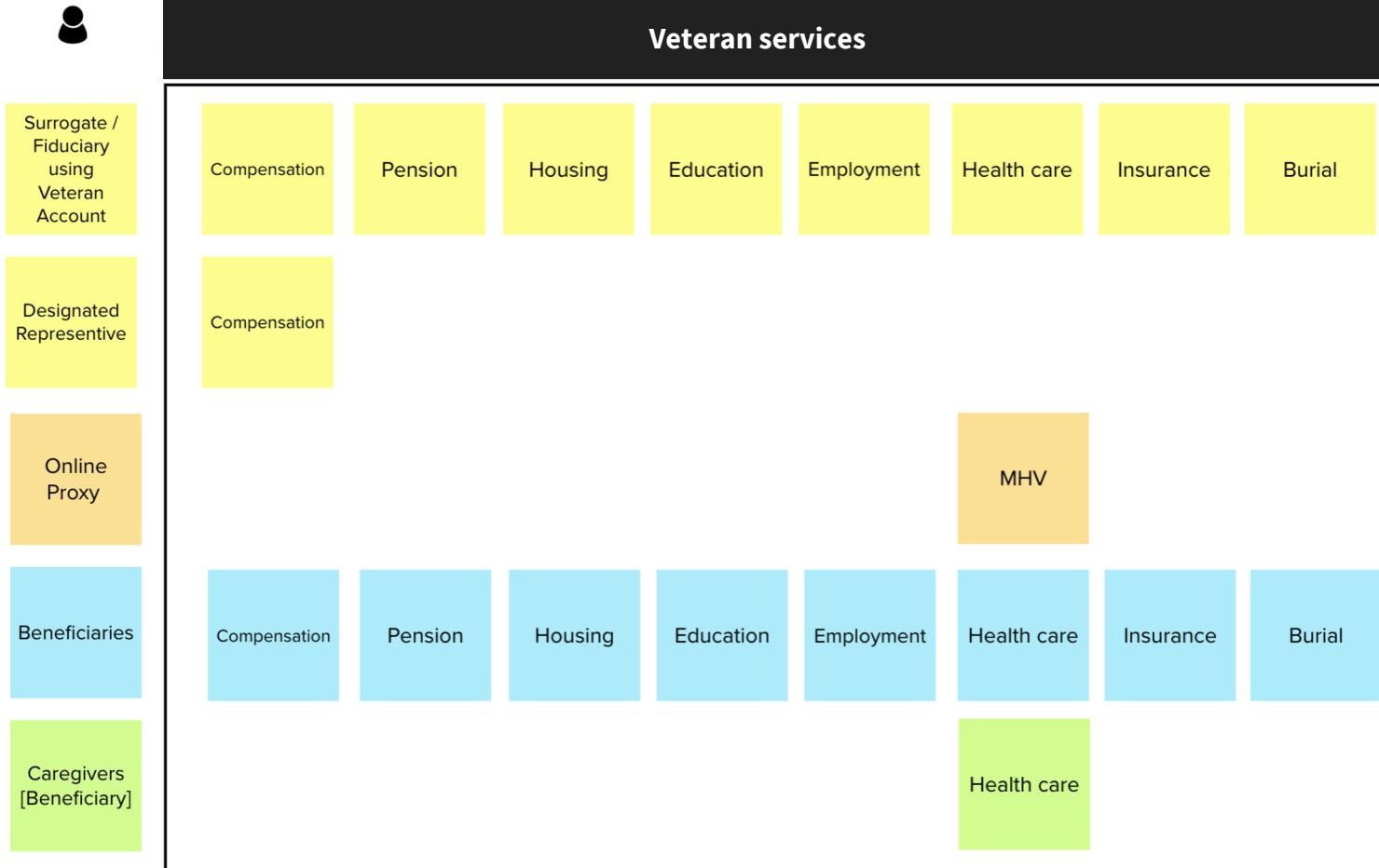
Other VA services:

Although Healthcare has been a primary focus, Veterans want to be able to give proxy access to their benefit information and other VA services as well. Providing this view will require nuance, because in many cases the proxy may also be a beneficiary and would potentially have two different views of the Veterans benefits.

While hugely important, healthcare is not the only place non-Veterans need access

Recommendation: Whether voluntarily by the Veteran, or as a result of delegated authority, provide the ability and controls to give total or partial access to healthcare and benefit information to those providing care to Veterans.

Current access by user role



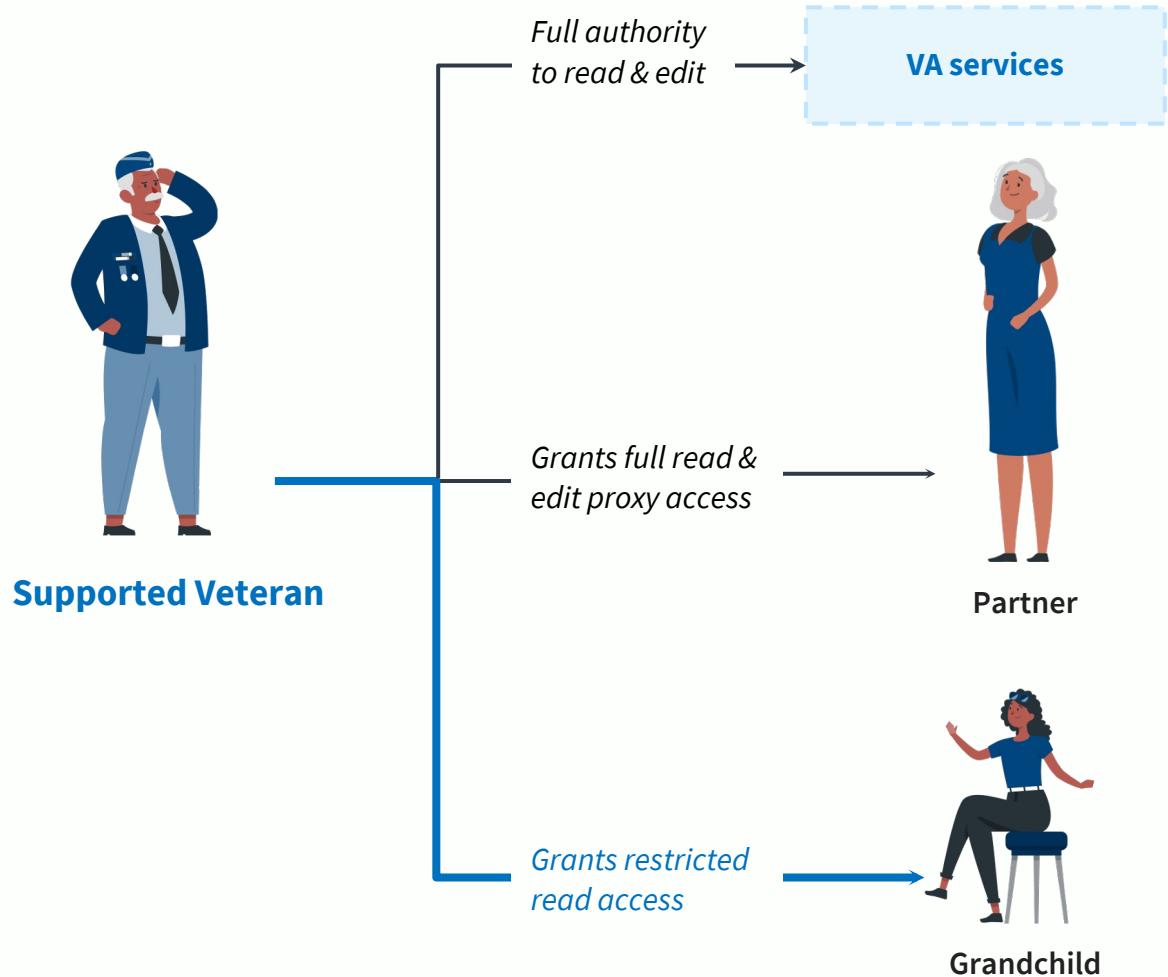
Key takeaways:

- **Online Proxy:** currently only have access through MHV to Health Care and we recommend that tool access expands to cover all VA Services (as needed)
- **Beneficiaries:** some capabilities are existing but need to expand level service access outside of just MHV
 - *Their coverage spans across all VA Services. Online interactions need to be tailored and enhanced specifically to address unmet online services applicable to them*
 - *Further discovery is needed to determine the specifics around levels of access*

How do these roles come
together to support Veterans in
real human relationships?

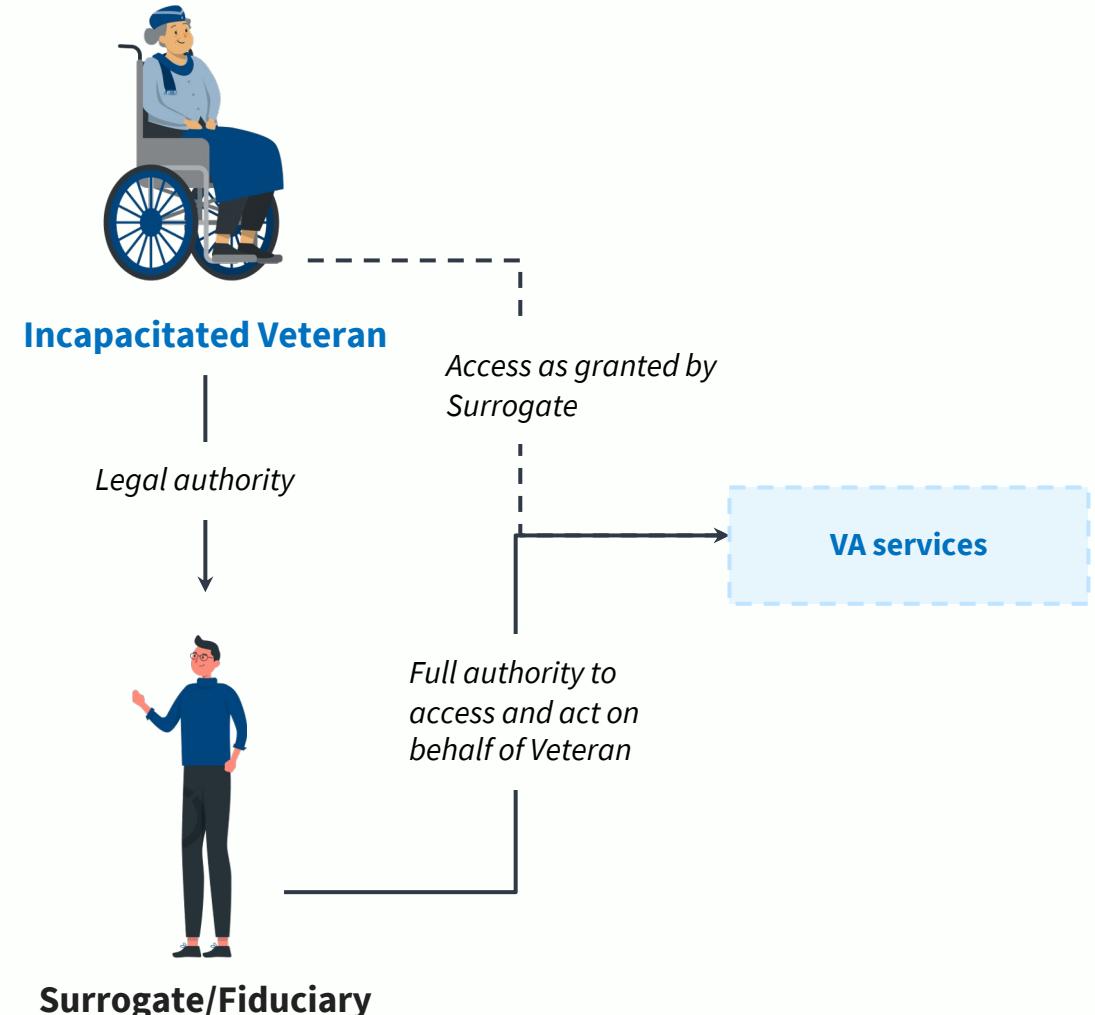
Archetype: Supported Veteran

- Veteran is legally competent and can choose to grant read and edit access to their VA information and to revoke that access.
- Veteran has designated an emergency contact and a durable power of attorney in the event they are no longer able to make decisions.
- The Veteran has a robust support system and so has granted full read and edit proxy access to their VA information to their partner who participates in considering medical decisions and helps the Veteran monitor their activity and medication (provides care as part of a reciprocal relationship). The Veteran has granted read and edit access to their prescription information for a college age grandchild who often refills and picks up prescriptions for their grandparent.



Archetype: Incapacitated Veteran

- Veteran has been deemed legally incompetent to make medical and financial decisions.
- Primary authority to make decision for the Veteran with regard to VA benefits and health services has been delegated to their adult son (Surrogate & Fiduciary).
- Veteran has partial read access to their VA information and their son has the authority to set how much information the Veteran can access.



Archetype: Supportive Partner

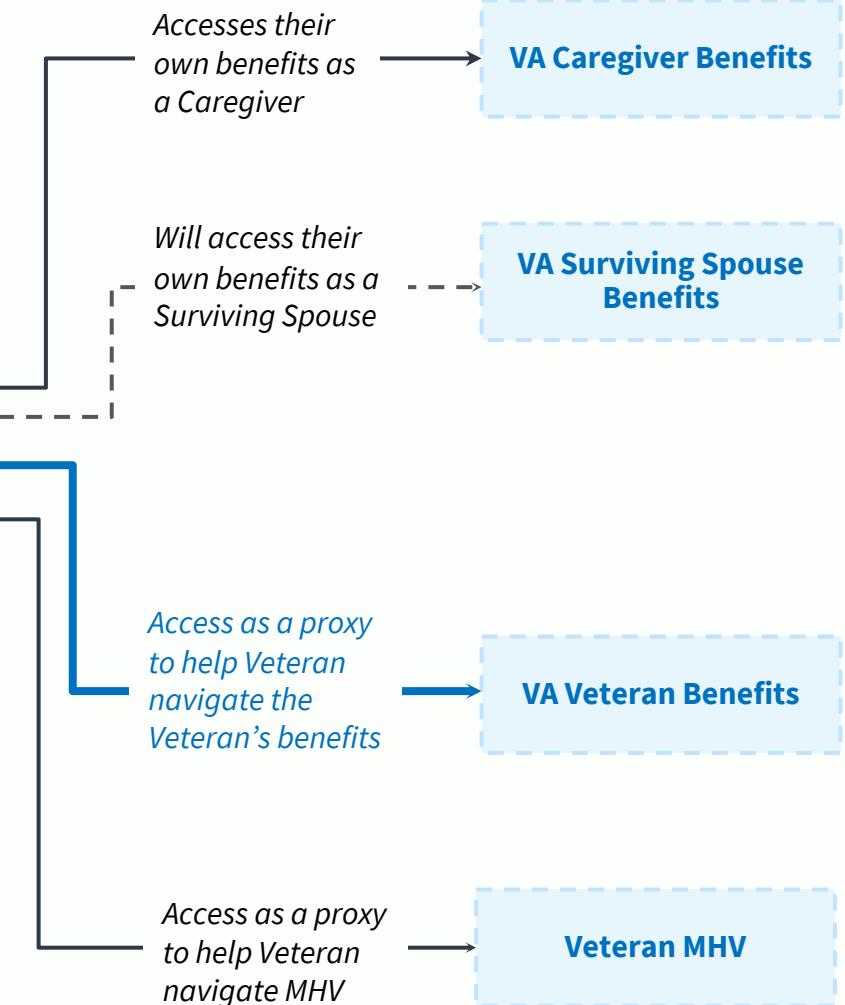
Roles: Proxy, Caregiver [Beneficiary]

Relationship: Partner, care provider, advisor

- Partner to a Veteran who is legally competent.
- Provides significant care to the Veteran and so receives Caregiver Benefits. Will also receive benefits from the VA in the event of the Veteran death.
- Has proxy access to read and edit the Veteran's information regarding VA Benefits and Health Services. This proxy access was given by the Veteran and could be revoked by the Veteran.



Supportive Partner

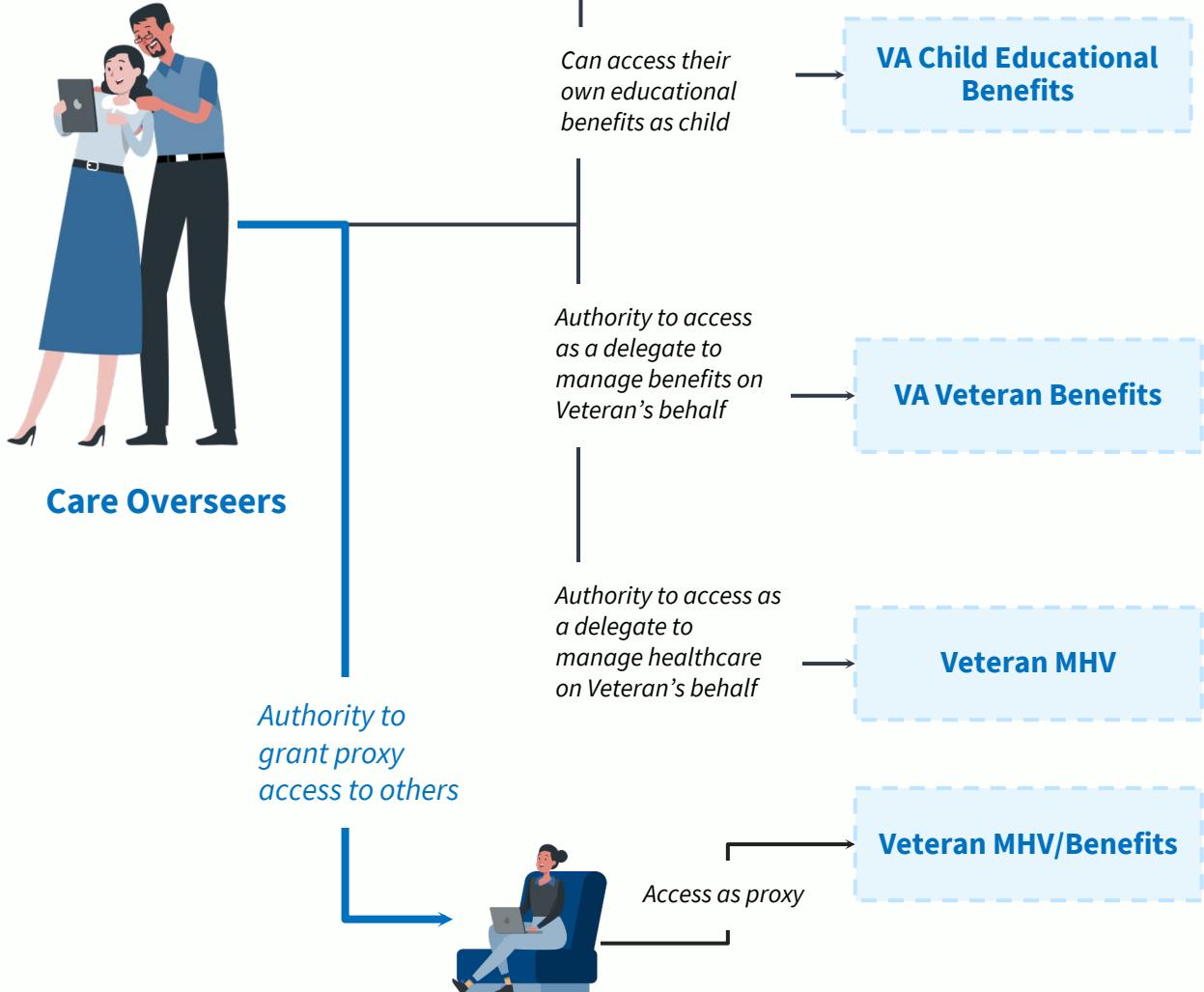


Archetype: Care Overseer

Roles: Power of Attorney [Delegate], Caregiver [Beneficiary]

Relationship: Child, care provider

- Adult child of a Veteran who has been declared legally incompetent to manage their own medical care and so serves as Power of Attorney for medical and financial matters
- Provides significant care to the Veteran and so receives Caregiver Benefits. Also receives educational benefits from the VA as a child of the Veteran.
- Has delegated authority to read and edit the Veteran's information regarding VA Benefits and Health Services. *Also has the authority to manage tiered proxy access for others who also support the Veteran.*



Consolidated use cases

Surrogate (Power of Attorney)

- Manage appointments
- Prescription refills
- Messaging healthcare providers on Veteran's behalf
- Scheduling appointments
- Make medical decisions

Fiduciary (Power of Attorney)

- Accounting
- Payment
- Financial Fund usage
- Earned pension

Accredited representative (Limited Power of Attorney)

- Manage monetary benefits
- Potential to need full access to health information

Caregiver

- Need access to their own benefits information
- May need access to the Veteran's information (as proxy of delegate)

Beneficiary

- Only need access to their own benefit information
- May also be a Veteran themselves (receiving benefits) AND the beneficiary for their spouse who has passed away
- May need to access their own benefits and help the Veteran navigate their benefits

Consolidated recommendations

Definitions

- Be explicit about the difference between roles and relationships
- Understand that caregiver as role is a type of beneficiary, and as relationship is highly varied and does not imply anything about the need or right to access Veteran information
- Align internal use of delegate to legal definition, and stop using delegation to mean voluntarily granted access
- Align on term proxy or other to mean voluntarily granted access that can be granted and revoked by the Veteran and rename the “Delegation toolkit” accordingly

Functionality

- Proxy access for all VA Services
- Time-delimited access
- Veteran visibility into who is accessing their information
- Tiered access
- Reminders about access status
- Ability for delegates to grant limited proxy access to others

Recommendations on further research

1. **Beneficiaries:** Lack specifics of unmet needs (for beneficiaries being able to access their own benefits), beyond what is already available on VA.gov
1. **Caregiver Program:** Talk to someone there to confirm and learn more of caregiver needs beyond the sharing information/online proxy use case
1. **Online Proxy:** What are additional priorities for expanding this capability. This may include needs for Representatives, Fiduciaries, Caregivers, Nursing homes, clinical staff, family members, etc.



A photograph of a modern architectural complex. In the foreground, there's a curved road with a barrier gate. A sign on the gate reads "STOP HERE FOR ACCESS PIV CARD ONLY". To the left is a large, multi-story building with a grid-patterned glass facade. To the right stands a tall, white cylindrical water tower. Several flagpoles with flags are visible in the background. The sky is blue with scattered white clouds.

From a vision to reality,
a strategic roadmap

Moving from concepts on a blueprint to concepts on a **roadmap**

Three priority focuses:

1

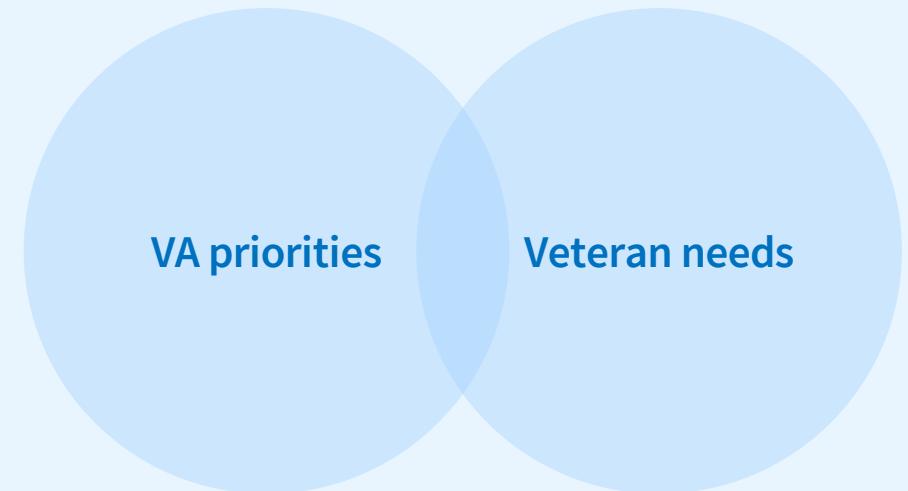
The pathways into migration, focusing on the variety of ways into this experience and in particular how we can meet people **if they encounter a problem**

2

Exploring some of the key aspects that will inform **tailoring communication to specific Veteran audiences** with special focus on how this applies to comms for those migrating from DS Logon

3

In-person proofing for Login.gov utilizing existing MHV processes:
Navigating the transition from digital asynchronous processes to in-person processes (e.g., Concept: Targeted email comms for Veteran who abandons digital flow, offering in-person solution)



Roadmap themes and related epics

		NOW	NEXT	LATER
Legacy credential migration	1. Migration of DSL and MHV users to Login.gov	● ● ● ●	●	● ●
	2. DS Logon sunset awareness	● ● ● ● ●		
	3. Create a comprehensive and universal communication plan to drive Login.gov adoption	● ● ●	● ● ●	●
Adoption	4. Proactive ID-proofing to start Login.gov account creation	● ● ●	●	
	5. Evaluate TAP Curriculum to increase adoption among newly transitioning Veterans	● ● ● ●	● ●	● ●
	6. Incorporate in-person support options (e.g., in-person proofing)	●	● ● ●	● ●
Support	7. Develop a centralized and comprehensive support process for Login.gov adoption assistance that will be supported by all VA offices in partnership with Login.gov	● ●	● ●	
	8. Tech recommendations, support, and training	● ● ●	● ● ●	● ●
NVUR	9. Create a Shared Access Platform to support proxy access	● ● ● ● ●	● ●	● ●

Legacy credential migration

1 Migration of DSL and MHV users to Login.gov

Leverage previous identity proofing to streamline the transition to Login.gov for existing users. Understand how Veterans proofed with legacy credential in order to determine eligibility for a streamlined experience and acceptable risk criteria.

IAL1 technical and design considerations within VA ecosystem

Opp area 4 - Daily hassle trumps theoretical risk

Provide clarity to users on their account level, IAL1, with an easy opportunity to proof (remote/in person) at any time. Post banner on ongoing basis of current risks and encourage promoting.

2 DS Logon sunset awareness

Create multiple paths of awareness that DS Logon is sunsetting by September 1st, 2023 so that users begin migration early.

Countdown clock ahead of DS Logon sunset

Opp area 1 - Don't sell me, just tell me

Create a countdown clock that shows when different login credentials will be sunset, so that users are aware of the upcoming change.

Considerations: Where the clock is shown, when the clock goes up (and down), and how to communicate two different login sunsets at once

Adoption

3

Create a comprehensive and universal communication plan to drive Login.gov adoption

Incorporate all major change activities in a comms plan so the entire VA ecosystem, including Veterans, non-Veteran users, staff and other parties are unified in what they know about the initiative. This allows us to think about the how, who, and when we will share relevant information.

Targeted communications based on segmentation and likely path of migration

Opp area 1 - Don't sell me, just tell me

Leverage data around user segmentation for paths of migration to curate targeted communication.

Consideration: *DS Logon users (who among them are eligible for inherited/grandfathering vs. those who aren't)*

4

Proactive ID-proofing to start Login.gov account creation

Enable Veterans to start the Login.gov account creation process by ID-proofing as part of other VA services such as VHIC appointments with Benefits/Eligibility.

Create integration with VA/Login.gov to create a shell account for individuals who have opted in during VHIC proofing

Opp area 5 - Meet Veterans where they are

Allow users to "opt-in" to process of Login.gov creation during VHIC creation and alleviate the burden of needing to re-proof when establishing a Login.gov account.

5

Evaluate TAP Curriculum to increase adoption among newly transitioning Veterans

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 and support creating an account, if needed. This area has unknowns including a lack of contact points and relationships, and a lack of general knowledge. There is an opportunity to align with VEO on the work they are doing on the veteran journey.

User research with TAP coordinators

Opp area 5 - Meet Veterans where they are

We need to do research with VA TAP coordinators in order to understand their perspective on what happens during TAP and the best ways to introduce proactive Login.gov account creation during this key moment in a Veteran's journey.

This task requires further definition in order to understand the objectives of the study more closely. Also, we won't have access to the newest TAP curriculum until January 2023, and this will help us shape the study.

Support

6

Incorporate in-person support options (e.g., in-person proofing)

Ensure users, especially those who are not tech savvy or that need further assistance, have the support needed pre, during and post-Login.gov account creation.

7

Develop a centralized and comprehensive support process for Login.gov adoption assistance that will be supported by all VA offices in partnership with Login.gov

As a complement to Login.gov, the VA should provide its own white glove hands-on support to Veterans as the first line of support.

8

Tech recommendations, support, and training

Educate and support Veterans to make better technical decisions when setting up their new Login.gov account and maintain ongoing best security practices.

Enable MHV coordinators to verify and record Veteran IDs for Login.gov ID proofing

Opp area 2 & 5 - Humanized, contextualized, and dedicated support, Meet Veterans where they are

Building off the interface available to USPS workers who are ID proofing for Login.gov as part of the USPS pilot to create an interface that allows MHV coordinators to access a Veteran's in-process application and record ID proofing for that application.

Considerations: *Insure MHV coordinators have visibility into phone/address verification step of the Login.gov process and how it might affect timing for ID proofing.*

Establish a direct point of contact at Login.gov for VA My HealtheVet Coordinators

Opp area 2 - Humanized, contextualized, and dedicated support

To help My HealtheVet coordinators facilitate support with Login.gov, we will establish a direct point(s) of contact at Login.gov.

Considerations: *Collaboration with Login.gov how this might scale beyond My HealtheVet, for example, to play out across other benefit programs*

Conduct in-person security key research with less digitally-connected users

Opp area 4 - Daily hassle trumps theoretical risk

We need to do further research to understand how users who are less digitally-connected interact with MFA. If they have used MFA before, we need to understand issues they've faced with set up or use; and if they've not used it before, we need to understand the issues they may encounter. In particular, this research needs to include unhoused Veterans.

Non-Veteran user roles

9

Create a Shared Access Platform to support proxy access

Give Veterans the ability to voluntarily grant full or partial access to their VA data and services to their loved ones and those who care for them. Veterans needs to be able to manage the level and duration of access.



Build VA-wide alignment on the definition of proxy access and on needed features

Opp area 6 - Trust and life events guide access decisions

Continue process of internal alignment on definitions related to NVUR, gaps analysis, and exploration of needed features.

A few additional concepts that surfaced for Login.gov consideration

Some of these may already be accounted for, but just in case they haven't been we wanted to share them with you today.

Save Login.gov account creation progress

Opp area 2 - Humanized, contextualized, and dedicated support

Enable each step of creation process to auto saved so that users who fail to complete the process have fewer steps to complete.

Surface the option to get in-person help from Step 1 of Login.gov account creation—not just after failure to upload credential

Opp area 2 - Humanized, contextualized, and dedicated support

We could give Veterans the option to do in-person proofing if they wish to, not just if they face an issue with online proofing, first. This will allow Veterans to choose the option that works best for them, and we won't lose them from that first point of failure.

Chatbot intercept at moment of abandonment or repeated error states

Opp area 5 - Meet Veterans where they are

Leverage a proactive pop-up from a chatbot to reach out and triage help at the moment of need.

What's next for the roadmap?

Wednesday, Dec 7

Implementation Kickoff

- 
- Kick-off implementation
 - Onboard new team members
 - Create a mid-level plan for implementation
 - Write sprint goals for the next few sprints
 - Size stories and prioritize the backlog



Thank you from the Discovery Team,
onwards and upwards into
Implementation!

