



VA API Governance

Discovery Readout

How might we build an authorization framework that is

- Easy for outside developers to integrate with
- Easy for Veterans to control access to their data
- Easy for us to maintain over time
- Allows for flexibility as standards and technology change?
- Insulates API owners from the implementation details of end-user authorization

Based on where we felt we could be most effective, we focused on product-centered questions:

How could you make authorization the best experience possible for end users? And how can you ensure that the apps using our APIs do the same?

- Five user research interviews
 - API consumers
 - API providers
 - Public sector APIs
- Industry research for best practices
 - Public and private sector APIs

Very high number of conversations given the short time frame of this project = excellent data set

Best authorization practices for end users

Provide multiple 2FA options
and explain when necessary
why these security features
are in place

Be intentional about when
you require 2FA/MFA

The screenshot shows the LOGIN.GOV website's account security setup interface. At the top, a dark blue header contains the text "An official website of the United States government" and the "LOGIN.GOV" logo. The main heading is "Secure your account", followed by a subtext: "login.gov makes sure you can access your account by adding a second layer of security." Below this, a prompt says "Select an option to secure your account:". There are three radio button options: "Text message / SMS" (selected), "Phone call", and "Authentication application". Each option has a brief description of how the security code is delivered. At the bottom of the options is a blue "Continue" button and a link for "Cancel account creation". On the right side, a green sidebar contains a section titled "Why do I need to store my new key on paper?". This section explains the importance of storing the key on paper for privacy and security, noting that login.gov does not store passwords or personal keys. It also states that users must store their personal key outside their computer or mobile device. A "Close" button is at the bottom of this sidebar. At the very bottom of the page is a large green "Continue" button.

An official website of the United States government

LOGIN.GOV

Secure your account

login.gov makes sure you can access your account by adding a second layer of security.

Select an option to secure your account:

- ☒ **Text message / SMS**
Get your security code via text message / SMS.
- ☐ **Phone call**
Get your security code via phone call.
- ☐ **Authentication application**
Set up an authentication application to get your code without providing a phone number.

[Continue](#)

[Cancel account creation](#)

Why do I need to store my new key on paper?

To protect your account, you need a password and access to your telephone or authentication application at sign-in. If you can't use your phone or app, you can sign in with your personal key instead.

For your privacy and security, login.gov does not store your password and personal key. Only you know them. Only you can access or share your personal information.

We require you to store your personal key outside your computer or mobile device so that it will be safe even if your devices are stolen or your online accounts are hacked.


If you don't have your personal key and you forget your password, the only way to keep your account safe is to verify that you are the legal owner.

[Close](#)

[Continue](#)

Make it obvious what data is being shared when authorizing third party applications

LOGIN.GOV U.S. Customs and Border Protection | Trusted Traveler Programs



You are now logging in for the first time

You can now log into CBP Trusted Traveler Programs.

Continue

This is the only information login.gov will share with DHS:

✓ Email address

[Return to your login.gov profile](#)

Medicare.gov

Do you approve the application TestApp to access your Medicare information?

TestApp WILL BE ABLE TO:

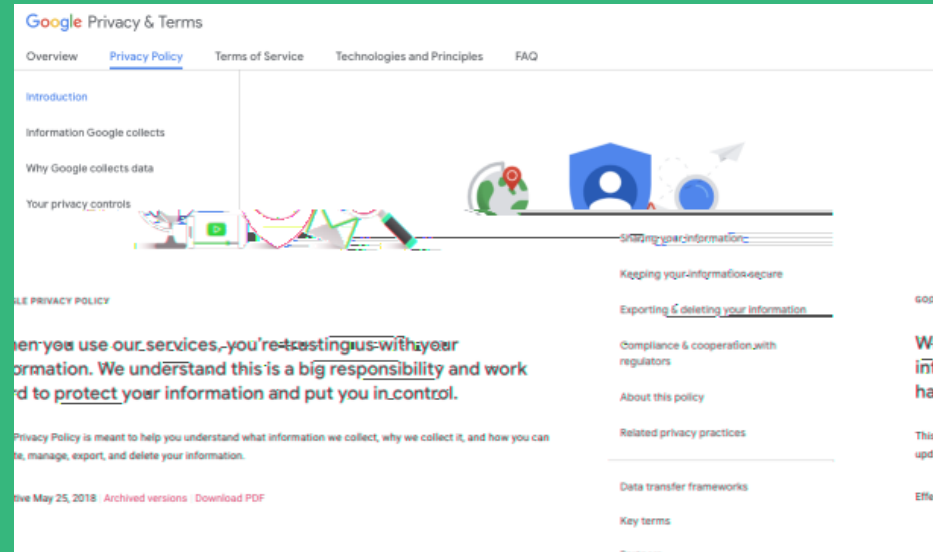
- Access at least 4 years worth of Medicare claims information.
- Access your profile and demographic information.
- Create copies of your Medicare data.
- Get updates to your Medicare data so long as you do not revoke access.

Yes, approve access

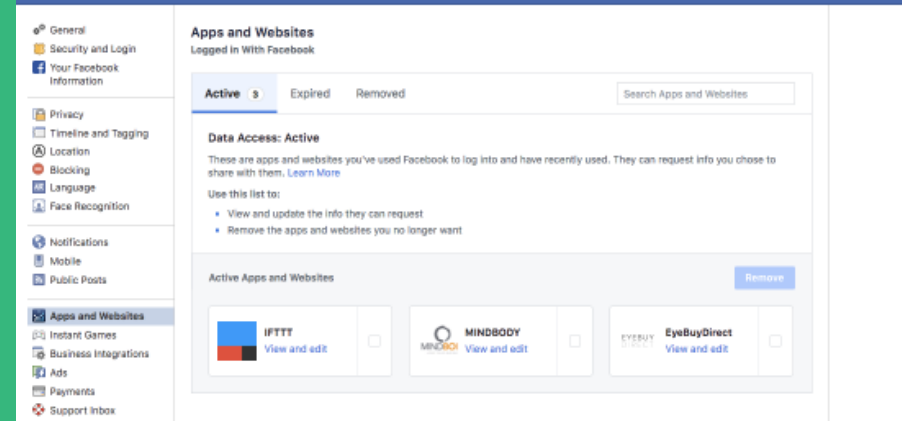
No, do not approve access

Use plain language in
privacy policies and terms of
service

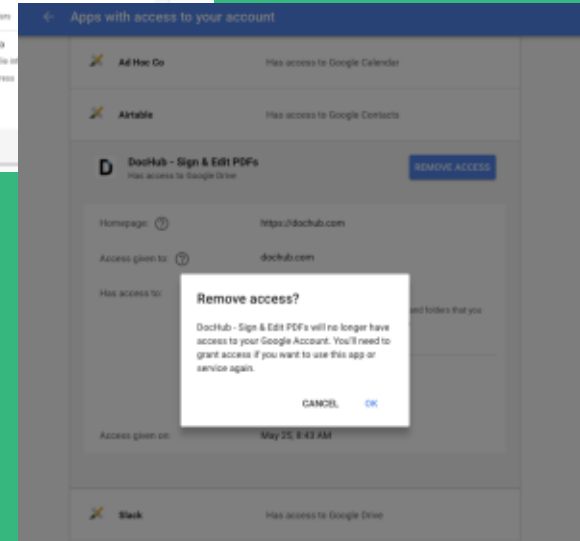
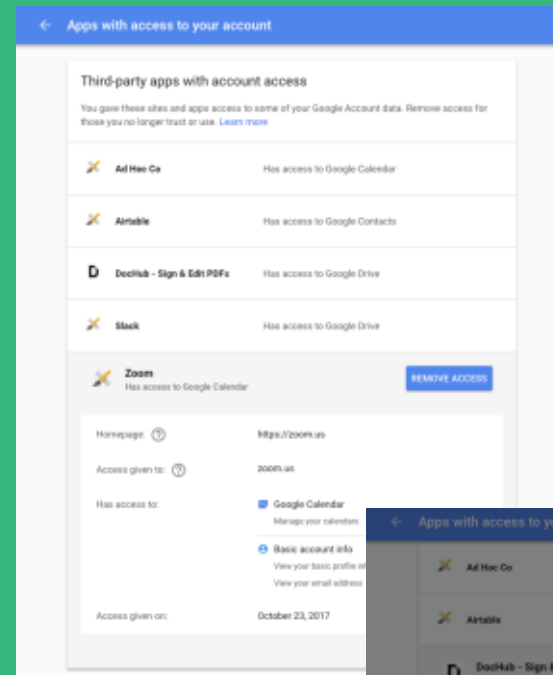
Call out important pieces in
a summary and add detail
below



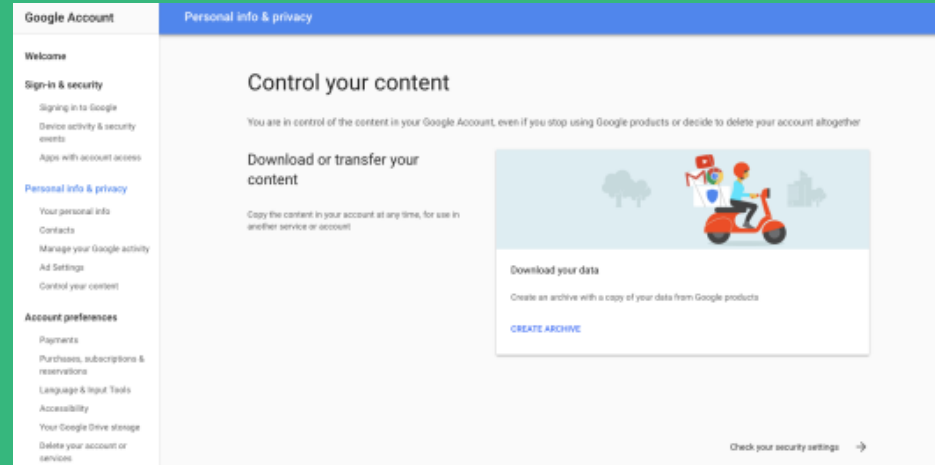
Allow a user to easily see
who has access to their
information



Allow a user to easily revoke
a third party's access to their
information



Allow a user to access all their data associated with an account



The screenshot shows the Google Account settings interface. The left sidebar contains a navigation menu with sections: 'Welcome', 'Sign-in & security' (with links for signing in, device activity, and app access), 'Personal info & privacy' (highlighted in blue), and 'Account preferences' (with links for payments, purchases, language, accessibility, and storage). The main content area is titled 'Personal info & privacy' and features a 'Control your content' section with a sub-header 'Download or transfer your content'. It includes an illustration of a person on a scooter with a shield and a cityscape in the background. Below the illustration, there is a 'Download your data' section with the text 'Create an archive with a copy of your data from Google products' and a blue 'CREATE ARCHIVE' button. At the bottom right, there is a link to 'Check your security settings' with a right-pointing arrow.

Google Account

Personal info & privacy

Welcome

Sign-in & security

- Signing in to Google
- Device activity & security events
- Apps with account access

Personal info & privacy

- Your personal info
- Contacts
- Manage your Google activity
- Ad Settings
- Control your content

Account preferences


- Payments
- Purchases, subscriptions & reservations
- Language & input Tools
- Accessibility
- Your Google Drive storage
- Delete your account or services

Control your content

You are in control of the content in your Google Account, even if you stop using Google products or decide to delete your account altogether

Download or transfer your content

Copy the content in your account at any time, for use in another service or account



Download your data

Create an archive with a copy of your data from Google products

[CREATE ARCHIVE](#)

[Check your security settings](#) →

Authorization API best practices

When building APIs with authorization...



- Use established and tested technical standards
- Provide high quality documentation, and put it in the API docs instead of in a privacy policy at the bottom that no one reads
- Refine the approach over time
- Provide self service options as much as possible but be prepared for white glove support, especially in the beginning
- Require and reinforce best security and privacy practices for API consumers dealing with PII; apply the standards where they're needed

Provide comprehensive
documentation about
authorization

“I think bad documentation would be documentation that excludes steps....Bad documentation would be, I make the first call, it gives me a peace to authentication, but they don't list what I need to do next to get the next piece of authentication...As long as all the steps are there and defined and I know exactly what I need to call, what information I need to pass, I think the documentation is good.”

Protect end user privacy and
maintain high security
standards

“Each agency can request what attributes they want to receive. But, if an agency wants to use SSN, but they only have a LOA1, we won’t allow that. LOA3 attributes are first name, last name, address, SSN, driver’s license. We maintain that information in our database encrypted...If you request an account deletion, we won’t do it right away, we send an email, wait 24 hr, etc, in the instance it’s a malicious users.”

“We have a demo meeting with the customer, they walk us through the application, and then we ask them questions about privacy policy/terms of service, how they handle security and data breaches. “

Reinforce best practices
amongst consumers

“So if an agency wants to integrate with us they need to have best practices, good documentation, and plan with us in advance, documenting questions people could be asking.”

Recommended next steps

- Evaluate other APIs that share PII to develop processes to manage compliance over time
- Design and test lightweight prototypes for users to grant, revoke, or review permissions they've granted for their data
- Continue to perform user research with API consumers so we can refine the tools we provide for integration
- Technical discovery to ensure our authorization framework with future flexibility in mind
- Simplify and streamline API Playbook

General best practices

Provide self-service options
to developers as much as
possible

“They have since done a whole new dashboard where you can kind of go in and see what configurations you have out there and you can actually add the configurations yourself instead of going through them. So that helped out a lot.”

Use past experiences of end user results to inform decisions when implementing with a new consumer

“I would say they were able to provide us guidance based on previous projects. They had just gone through [integration with] Global Entry and working with them so they were able to tell us, you know, kind of use that as a use case and say, well, in that case we would advise because of our experience, they're not to do this and maybe try this other thing.”

Provide open lines of communication about releases to API customers

“If we had known a delete account feature was coming up a relatively soon, you know, maybe a couple months out, then we could have had a lot of discussions on that and see what changes we want to make on our side to meet that new feature that being implemented...”

“I think because of that change [releasing a new feature] we asked for more advanced notice of what changes they’re making because we were sort of getting them like the morning of.”

Provide versioning of APIs.
Versioning standards allow for
easier integration and future
development

“..typically an API would follow a versioning best practice where there would be a version endpoint that was stable so that all the groups using that API could develop against it and you know, sort of have their flexibility to do what they needed to do. But then also giving the team who's developing that API, the ability to develop the next version independently of all of the groups using the API.”

Embed provider team
members if possible during
API integration

“They [login.gov team] did provide .. a designer to work with who had worked for awhile on their interface. They could answer questions about the design decisions they made there, as well as help vet our designs for possible problems. He was just a really great reference for my team and myself... to bounce ideas off of and to ask questions... He was a guest in our slack and vice versa....So we were able to get fairly immediate answers when we are in the design phase.”

Give consumers data on use cases that help sell reluctant state holders on the value of integrating with your API

“We’ve mostly tried to answer from our perspective: this is the benefits and this is what it’s costing us today and what have you. But they [login.gov team] actually did help quite a bit with convincing folks this [integrating with their API] is the right way to go.”