VA Lighthouse Governance Model Microconsulting

Cat Greims

Blue Button

6/27/2018

* **For any APIs you use, how do you manage security/privacy concerns?**
  + **For an indiv** 
    - On the app, they click the button “share my data”
    - Client application owns UX until you get a page with mymedicare.gov
    - They log in if they have an account or create one at that time
    - A third of ppl create an account
    - Address verification
    - Another screen -> are you sure you want to give access to X, this app will be able to do X,Y,Z
    - Haven’t done research
    - Beneficiaries own their data make it as clear as possible what/who they are accessing
    - They can revoke access in their profile
    - Stops any future data from coming through, does not remove existing
    - Thinking about linking privacy policy and terms of service
    - **Do user research**
    - Crazy drop off
    - 57 million beneficiaries, 8 million have medicare.gov accounts, 1.7 have logged in in the last year, so only 3%
    - No comms
    - For any APIs you use, how do you manage security/privacy concerns?

- Couple layers beneficiaries. Standpoint- medicare bene. To use their data, they will use the app. Connect medicare data, mymedicare.gov. (one screen is a login or create a login at that time. 1/3 who create an account go to the next stop

- If they have an account they login, are you sure you want to give  
access to (app name). beneficiaries own their data, make it as clear as possible  
for them to understand, can revoke access (revoke access button, stops future data  
from coming through won't stop current data

- Adding logo of the app you're giving data to….. they exist and that it’s a 2rd party service

What isn’t working: there is no research with beneficiaries on this

Authorization structure CMS is conservative against that and this is there data, here is what is looks like on other, depends on ben having that account 57 million beneficiaries we have

8 mill with medicare accounts 1. 7 who have logged in out of 57 million

advertising with AARP

* + **For a developer**
    - Join developer sandbox
    - They have a django app into air table to manage customers
    - Need to register before they can make a call, sandbox has synthetic data they can play around with
    - They can see documentation but not sandbox pre registration
    - Interactive documentation is nice before creating an account
    - The data that they have in the sandbox is de-identified and so they tore 30,000 records apart and put them back together, customers said the data is crappy
    - Davita is one of their clients, working with the customers to understand their data needs
    - You get a developer account in the sandbox, you don’t get a login when you get moved to production
    - One day they were thinking about having a developer profile that they could log into to see what beneficiaries they’re connected to
    - Getting ppl into production is still manual is going well, once they are ready BB can turn it around pretty quickly
    - Funnel of interest -> production, 330 leads
    - 6 ppl in production
    - 15 requests to access
    - Evaluate privacy policy, terms of service, security and breaches, incidents
    - Manually giving out keys
    - They copy their application from sandbox to production, there’s no portal at all
    - **Interview Ryan**
    - **Kelly Taylor from Digital Service**
    - **Jonathan Sullivan**

**From recording:**

The data that we have in the sandbox.

To de identify the claims data, they had torn it all apart and mismatched things back together. So we have 30k fake patients, and their claims history, rather than being one patient’s history is a bunch of different patients pulled together. So it’s hard to get a sense..it doesn’t make sense as a health record...they aren’t a real person’s record.

So they ask for patient with good examples of use cases. Eg Dialysis.

* **Once you’ve created an account, do you get a dev account?**

You get one in sandbox. There’s no production login. We can imagine in the future, you have an account and your logged in and you can see your beneficiary, apis you’re connected to. We don’t have that yet.

We just have the one api [right now].

* **What’s working well?**

Getting people into prod while still a manual process, is going well. Once they’re ready, we’re able to turn that around pretty quickly. Think of it as a funnel. We’ve grown interest in our sandbox, we have like, 330 orgs in there right now. But then we have 6 people in prod, we’ve had maybe 15 request access, some of whom aren’t quite ready yet. We don’t understand that gap in between very well, there’s some big drop-off happening there.

* **Information you collect when evaluating for the program, what are you keeping in mind?**

I think we would want to keep some review process, it’s hard for me to imagine in the medium term anyone getting comfortable with letting people straight into prod without a check on it. 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. I think the things we would automate would be things like, where are we storing all of that information, privacy policies, etc, where are we storing that status of companies. We have a log on confluence, but that is not the long term solution to this. Giving out of keys is still totally manual.