



ANITA B.ORG 2024
GRACE HOPPER
CELEBRATION

me
+we

Open Source in Government:

Raising the Floor & Ceiling at the
Centers for Medicare & Medicaid Services (CMS)
as an Early-Career Software Engineer



Natalia Luzuriaga

- Software Engineer in the CMS Open Source Program Office
- U.S. Digital Corps Software Engineer Fellow

Agenda

- What is Open Source Software?
- Open Source in Government
- Open Source at the Centers for Medicare and Medicaid Services
- Journey of Standing Up the CMS Open Source Program Office (OSPO)



What is Open Source Software?

What is Open Source Software?

Open source means source code that anyone can **inspect**, **modify**, **enhance**, and **share**.



What is Open Source Software?

97% of software depends on Open Source Software

From 2022 Open Source Security and Risk Analysis Report by Synopsys

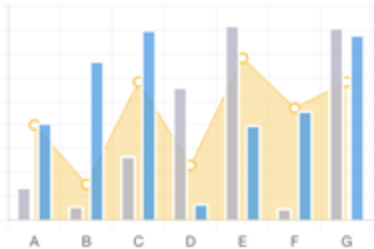


chart.js



Firefox & Chromium



Linux



NGINX & FFmpeg



Wikipedia



OpenSSL



“Much like roads or bridges, which anyone can walk or drive on, open source code can be used by anyone...This type of code makes up the digital infrastructure of our society today.”

*– Nadia Asparouhova,
Roads & Bridges: The Unseen Labor
Behind Our Digital Infrastructure*



Open Source in Government

Every year, the Federal
Government spends
\$12 billion on software

*Senators Ted Cruz (R-TX) & Gary Peters (D-MI)
on the [SHARE IT ACT of 2024](#)*

Where does the United States currently stand?

U.S. Federal Open Source Policy [M-16-21](#) – 2016:

- Requires new custom-developed source code to be made available for **sharing and re-use across all Federal agencies**
- Reduces cost & federal vendor lock-in, streamlines development, apply uniform standards and ensure consistency in creating and delivering information
- Requires each agency's CIO develops an **agency-wide policy** that addresses requirements of the Federal Source Code Policy

High Profile Cyber Attacks

- Log4J Vulnerability – November 2021
 - New guidance and initiatives that erupted as a result
- Emphasized focus on OSS due to cybersecurity concerns



OSS Efforts in the Executive Branch

In 2021, Biden-Harris Administration released directives on Cybersecurity

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

 BRIEFING ROOM • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023



OSS Efforts in the Legislative Branch

S.917: Securing Open Source Software Act 2023

[INTRODUCED]

Duties of the Cybersecurity & Infrastructure Security Agency (CISA) regarding Open Source Software Security, includes publishing a framework to assess risk of OSS components

S.3594: SHARE IT Act

[INTRODUCED]

Requires agencies to publicly list custom-developed source code and share this code with the rest of the government

H.R.3208 - DHS Cybersecurity On-the- Job Training Program Act

[PASSED HOUSE]

Establishes a cybersecurity training program for DHS employees holding non-cybersecurity positions



Open Source at CMS

Centers for Medicare & Medicaid Services (CMS)

We provide health coverage to

62M

Medicare Beneficiaries
as of 11/2021

88M



Medicaid Beneficiaries
as of 04/2022

31M

Healthcare.gov Beneficiaries
as of 06/2021

CMS Open Source Policy

Preview Code Blame 56 lines (26 loc) · 10.9 KB

Raw    

Introduction

The [Centers for Medicare & Medicaid Services \(CMS\)](#) has been an active supporter of and has utilized the [Open Source Software \(OSS\)](#) on several IT projects for its mission-critical programs. Several CMS business units and offices have been actively releasing OSS as part of IT modernization projects. CMS has many active open source communities, such as the BlueButton, [Healthcare.gov](#) StyleGuide, and the [MMIS Provider screening module](#) on Github. CMS has embraced the OSS for our development projects and is looking forward to releasing software codes to the open source community to promote its reuse. This policy will help CMS achieve the goals outlined in the [OMB directive M-16-21](#) for Federal agencies.

OSS Consideration & Applicability

This policy applies to the CMS project teams that engage in the development of code for the Open Source community. This policy assumes that before OSS development, and in accordance with the [three-step software solution analysis](#), the project team has conducted market research and analyzed commercial and other open source alternatives that may meet their business need. This OSS policy applies when the project team ventures into custom code development and chooses the project code as a candidate for OSS. The project teams must verify [if they may release](#) the source code that has been developed using Government funds.

Government Data Rights

The CMS Office of Acquisition and Grants Management (OAGM) has an established IT procurement procedure that sets the [rights to the custom-developed code](#), including at a minimum, rights to Government-wide reuse and rights to modify the code. CMS contractors who develop software for CMS business use are covered by the procurement clauses that provide the Copyright of the CMS-funded custom designed software to CMS and prohibits the contractors from reselling it to other Federal Government agencies. Such custom produced software for CMS can be made freely

Open Source at CMS



CMS Blue Button 2.0



**Beneficiary
Claims
Data API**



**Data at the
Point of Care**

CMS Open Source Program Office

An Open Source Program Office (OSPO) serves as the center of competency for the agency's open source operations and structures.

CMS Open Source Program Office (OSPO) Functional Statement

*“Establish and maintain guidance, policies, practices, and talent pipelines that **advance equity, build trust, and amplify impact** across CMS, HHS, and the Federal Open Source Ecosystem by working and sharing openly.”*

How do we 'do' Open Source at CMS?



Policies

How we **inbound** and **outbound** open source contributions and content



Projects

How we **solve real world problems** by working in the open



Programs

How we **measure**, and **manage** contributors, projects, **risks**, and **opportunities**

How does our OSPO provide value?



Save us Money



Save us Time



Accountability for
Contract Performance



Engine for Talent



Reduce Duplicate
Work



Reduce Duplicate
Costs



Reduce Security
Risk



Reduce Continuity
Risk



Standing up the Open Source Program Office

CMS OSPO Team



Remy DeCausemaker
Open Source Lead



Natalia Luzuriaga
US Digital Corps Fellow '23



Isaac Milarsky
US Digital Corps Fellow '23



Dinne Kopelevich
US Digital Corps Fellow '24



Sachin Panayil
US Digital Corps Fellow '24



Interns
Coding It Forward Fellows



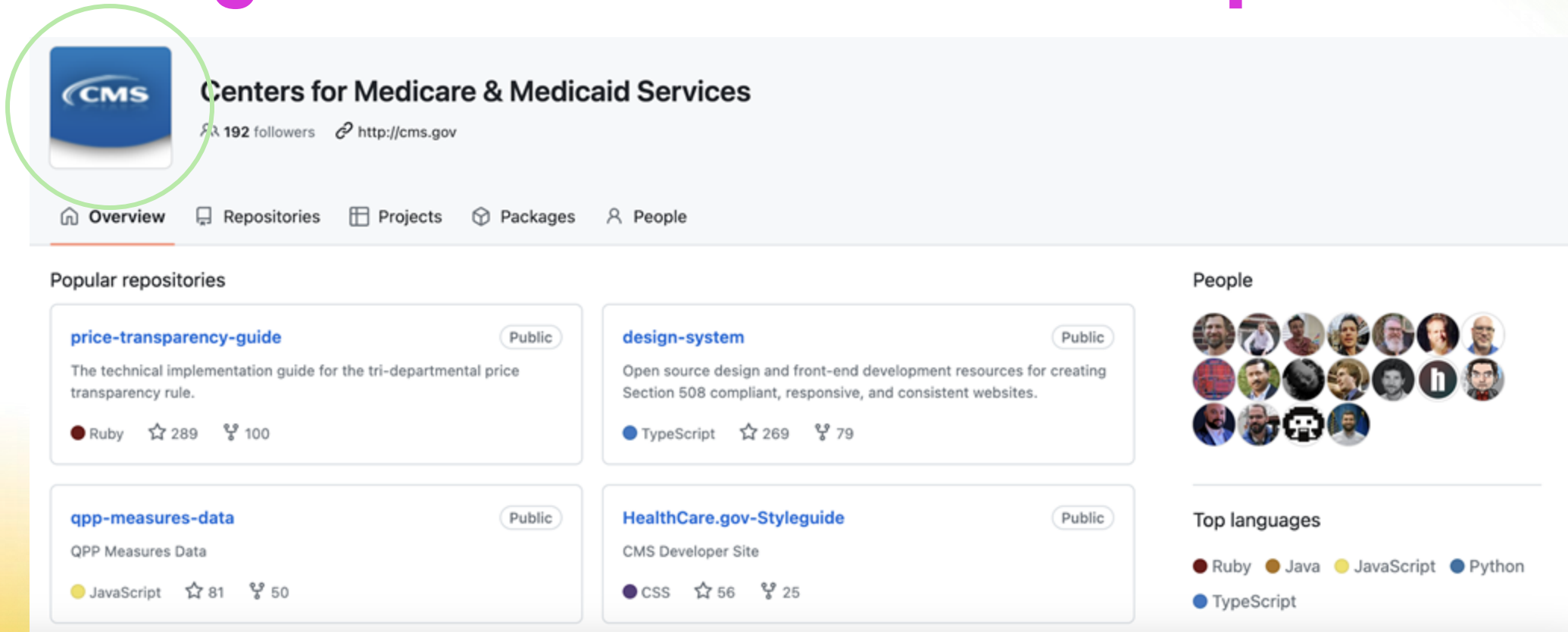
Interns
CodeInTheSchools




Raising the Floor

Contributions that benefit all software projects across the open source ecosystem

CMSSgov GitHub Profile Picture Update






 **Centers for Medicare & Medicaid Services**
192 followers <http://cms.gov>

[Overview](#) [Repositories](#) [Projects](#) [Packages](#) [People](#)

Popular repositories




price-transparency-guide Public

The technical implementation guide for the tri-departmental price transparency rule.

 Ruby  289  100




design-system Public

Open source design and front-end development resources for creating Section 508 compliant, responsive, and consistent websites.

 TypeScript  269  79




qpp-measures-data Public

QPP Measures Data


 JavaScript  81  50

HealthCare.gov-Styleguide Public





CMS Developer Site


 CSS  56  25

People




Top languages

 Ruby  Java  JavaScript  Python



 TypeScript






July 2023

CMShgov GitHub Profile Picture Update



Centers for Medicare & Medicaid Services




 369 followers  <http://cms.gov>

 Overview  Repositories 208  Projects  Packages  People 14

Popular repositories




[price-transparency-guide](#) Public

The technical implementation guide for the tri-departmental price transparency rule.

 Ruby  359  110




[design-system](#) Public

Open source design and front-end development resources for creating Section 508 compliant, responsive, and consistent websites.



 TypeScript  313  86

[qpp-measures-data](#) Public


QPP Measures Data

 TypeScript  89  46





[hospital-price-transparency](#) Public


 61  5

People



Top languages

 Ruby  Java  Python  JavaScript

 TypeScript

September 2024

Establishing a Baseline

- Created processes, best practices, and tools that benefit and support all projects across the ecosystem



Maturity Models



Templates



Checklists



Metrics

Maturity Model Framework

Reducing Duplicate Work

Level	Name	Purpose	Description
Tier 0	Private Repository	Experimental, Historical	Project is private, usually with a single developer. Typically working projects , example code , and early prototypes .
Tier 1	One-Time Release	Publication for Informational, Accountability, or Transparency Purposes	Project released publicly, but without planned future activity or maintenance from original author(s).
Tier 2	Close Collaboration	Collaboration with smaller, mostly internal teams	Project within a team or operational division, internal repo for innersource-style work .
Tier 3	Working in Public	Collaboration in the open with smaller, semi-open source teams	Project developed Open Source by CMS or CMS contractor. Limited external contributions, CMS-led (by choice or by statute).
Tier 4	Community Governance	Collaboration broadly in public	Project donated to or stewarded by an external community that welcomes public input and purposefully develops an open governance structure.

Maturity Model Framework

Reducing Duplicate Work

File	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4
LICENSE	M	M	M	M	M
SECURITY.md	N	M	M	M	M
README.md	M	M	M	M	M
CONTRIBUTING.md	R	R	M	M	M
MAINTAINERS.md	N	N	R	M	M
GOVERNANCE.md	N	N	N	R	M
CODEOWNERS.md	N	N	R	M	M
COMMUNITY_GUIDELINES.md	N	N	M	M	M
CODE_OF_CONDUCT.md	N	N	M	M	M

Level	Description
M	Mandatory
R	Recommended
N	Not Recommended

Repo-scaffolder

Reducing Duplicate Work

repo-scaffolder Public

Edit Pins Watch 2

main 33 Branches 0 Tags

Go to file Add file Code

natalialuzuriaga Merge pull request #171 from DSACMS/nat/changelog-wor... 16a6493 · 3 days ago 583 Commits

.github	Merge pull request #167 from DSACMS/nat/templates	3 days ago
assets	Updated Markdown to according to feedback	3 days ago
tier0	Updated VDP reporting text in README and CONTRIBUTI...	2 months ago
tier1	added blank date field to json	3 days ago
tier2	added raw tags to fix changelog workflow errors to tier 2-4	3 days ago
tier3	added raw tags to fix changelog workflow errors to tier 2-4	3 days ago
tier4	added raw tags to fix changelog workflow errors to tier 2-4	3 days ago

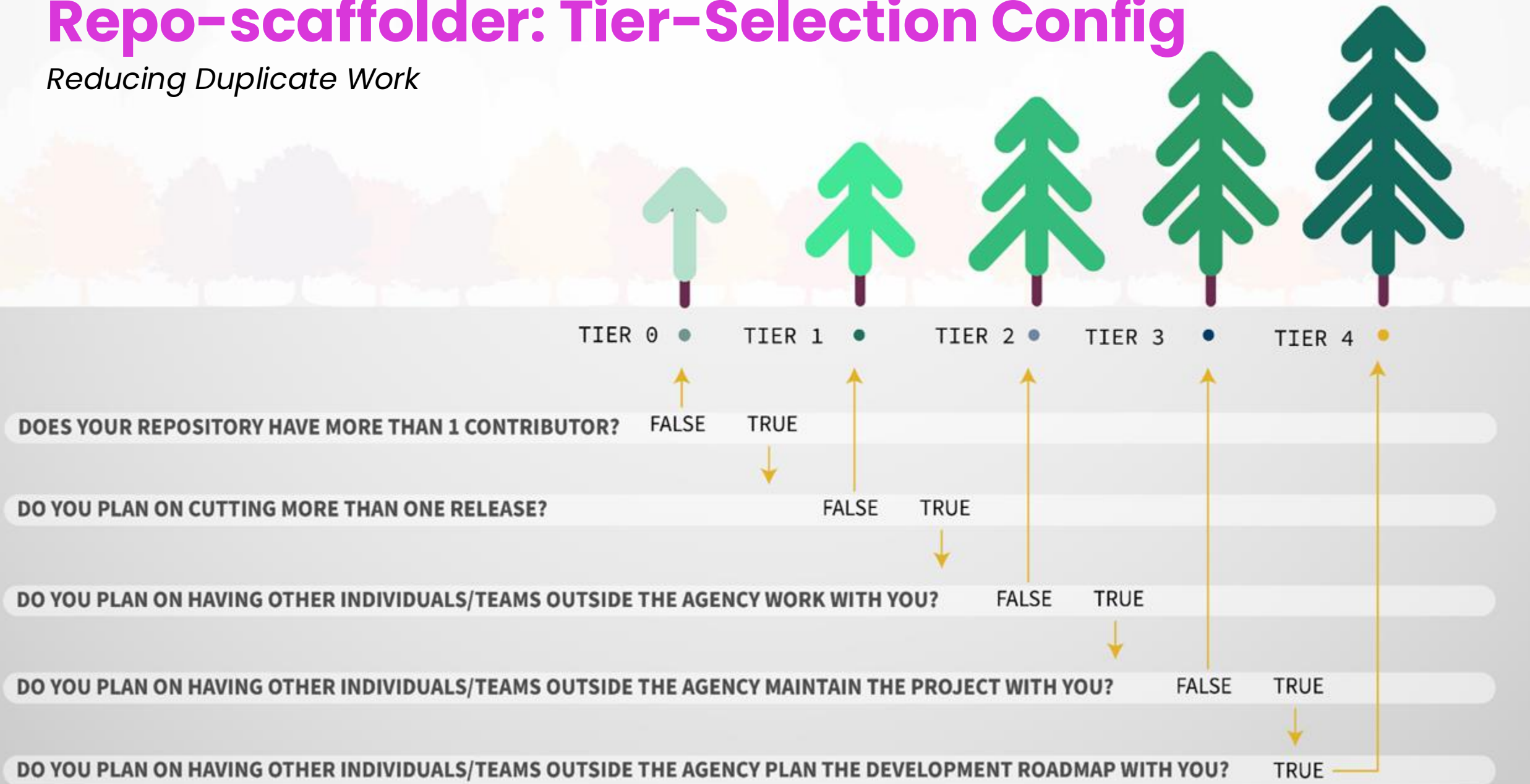
repo-scaffolder / tier3 / {{cookiecutter.project_slug}} /

natalialuzuriaga moved location of repometrics directory to .github

Name
..
.github
CODEOWNERS.md
CODE_OF_CONDUCT.md
COMMUNITY_GUIDELINES.md
CONTRIBUTING.md
GOVERNANCE.md
LICENSE
MAINTAINERS.md
README.md
SECURITY.md
repolinter.json

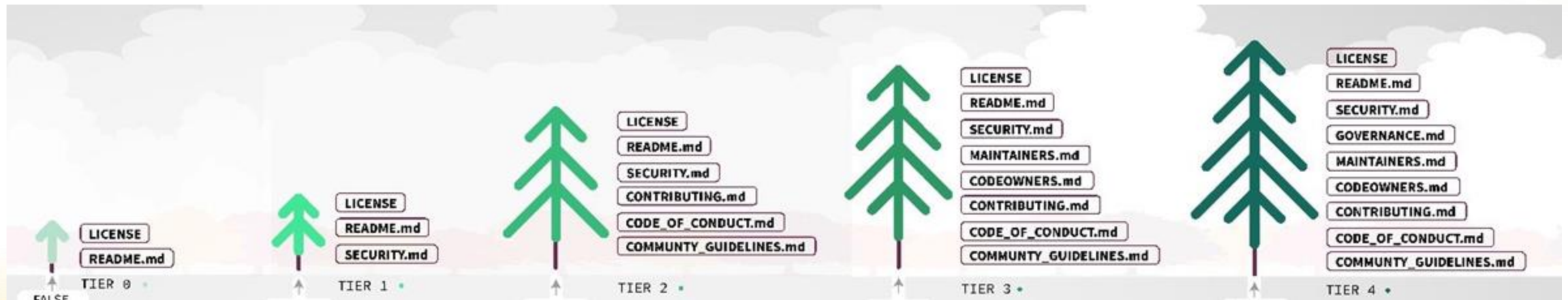
Repo-scaffolder: Tier-Selection Config

Reducing Duplicate Work



Repo-scaffold: Repo Creation

Reducing Duplicate Work



Repo-scaffolder

Reducing Duplicate Work

repo-scaffolder / tier3 / {{cookiecutter.project_slug}} /

 nataiialuzuriaga moved location of repometrics directory to .gith

Name

..

.github

CODEOWNERS.md

CODE_OF_CONDUCT.md

COMMUNITY_GUIDELINES.md

CONTRIBUTING.md

GOVERNANCE.md

LICENSE

MAINTAINERS.md

README.md

SECURITY.md

repolinter.json

repo-scaffolder / tier3 / {{cookiecutter.project_slug}} / README.md

 nataiialuzuriaga Updated VDP reporting text in README and CONTRIBUTING

beb0fcb · last month History

Preview Code Blame 132 lines (80 loc) · 7.71 KB

Raw Download Edit History

{{ cookiecutter.project_name }} variables can be swapped out
with user input obtained
from cookiecutter

{{ cookiecutter.project_description }}

About the Project

{project statement}

Core Team

An up-to-date list of core team members can be found in [MAINTAINERS.md](#). At this time, the project is still building the core team and defining roles and responsibilities. We are eagerly seeking individuals who would like to join the community and help us define and fill these roles.

Documentation Index

{list of .md at top directory and descriptions}

Repository Structure

{list directories and descriptions}

Development and Software Delivery Lifecycle

The following guide is for members of the project team who have access to the repository as well as code contributors. The main difference between internal and external contributions is that external contributors will need to fork the project and will not be able to merge their own pull requests. For more information on contributing, see: [CONTRIBUTING.md](#).

Outbound Review Checklists

Reducing Risk

Tier 1: One Time Release

Tier 2: Close Collaboration

Tier 3: Working in Public

Tier 4: Open Governance



Outbound Review Checklists: Tier 3

Making the Repository public

Flipping the Switch: Making the Repository Public

Once the repository has passed outbound review, we are ready to “flip the switch” and officially make it public. Once made public, there are a couple of actions that need to be taken:

Repository Actions

Please enable the following features to enhance repository security and maintain code quality:

- ☐ **Dependabot Alerts**
A GitHub Feature. Get notified when one of your dependencies has a vulnerability
- ☐ **Secret Scanning Alerts**
A GitHub Feature. Get notified when a secret is pushed to this repository. Ideally set this up to run after each new commit is pushed to the Repository.
- ☐ **Branch Protections**
Ensures the integrity of important branches by preventing unauthorized actions like force pushes and requiring pull request reviews with specific checks before merging. Dev and main should be protected branches in the repository.
- ☐ **Git Branching**
After making the repository public, make sure there is a coherent git branching plan in place. For example: agree to merge feature related pull requests into dev but merge bug fixes into main instead of dev first.
- ☐ **Add Repolinter GH Action to CI**
For ongoing adherence to repository hygiene standards, integrate the [repolinter GitHub Action](#) into your CI pipeline. This addition enhances your workflow by automatically enforcing repository cleanliness standards.

Communications & Rollout 📢

Share the good news with communities both inside and outside CMS!

☐ Draft a launch announcement

Be sure to include the following information:

- *Repo Description*
- *Repo URL*
- *Authoring Team Email Contact*
- *Authoring Team URL*
- *Authoring Team Slack Channel*
- *Call to action (file issues, contribute PRs)*

☐ Post launch announcement to CMS slack channels

- *#cms-opensource*
- *#cms-api-community*
- *#cms-data-community*
- *#cms-engineering-community*
- *#ai-community*

☐ Send a launch announcement email

☐ Add launch announcement to a Confluence Wiki Page

OSPO Repo Metrics Website

Reducing Risk

Organization

☐ DSACMS
☐ CMS-Enterprise
☐ CMSgov
☐ Enterprise-CMCS

Maturity Model Tier

FISMA Compliance Level

Project Type

Search

Project Name

DSACMS 😊

.github

Template repo for CMS Open Source Projects

☆3 🍴2 🗨3 📄4 👁2

cms-gource

Gource.io Visualization of Developer.CMS.gov Open Source repositories

☆0 🍴0 🗨0 📄0 👁0

dedupliFHIR

Prototype for basic deduplication and aggregation of eCQM data

☆8 🍴1 🗨21 📄147 👁4

Report for [metrics](#)

GITHUB.COM

CMS/OA/DSAC

WEBSITE

TIER 3

LOW ^

project type midsize

Repo Stats

☆ Stars	🍴 Forks	🗨 Issues	👁 Watchers	📄 Pull Requests
6	2	40	4	197

Summary Table

Metric	Latest	Previous	Diff	% Diff
Commits	1151	1145	6	0.52%
Issues	40	40	0	0%
Open Issues	19	19	0	0%
Closed Issues	21	21	0	0%
Open Pull Requests	13	13	0	0%

How are metrics helpful?

Reducing Risk by tracking our projects

Maturity Metrics

- Tiering of public repositories quantify **security and continuity risk**

Cost Metrics

- Quantify **time and effort invested** into repositories

Burden Metrics

- Quantifies **time and effort needed to contribute & improve** repositories

Open Source Policy V1.1

CMS Open Source Policy V1.1 #6

Edit < > Code

Merged decause-gov merged 9 commits into CMSgov:main from DSACMS:main 1 hour ago

Conversation 1

Commits 9

Checks 0

Files changed 2

+115 -17



natalialuzuriaga commented 1 hour ago

Member ...

V1.1 Updates

The CMS Open Source Program Office is updating this repository to fix links, reference our tools and guidance, and better reflect the current state of open source software usage and development at the agency.

Below are changes we made to each section:


Introduction

- List of CMS open source projects include our Developer APIs and CMS OSPO metrics website that serves as a software inventory
- Updated various links

OSS Consideration and Applicability

- Update links
- Include exceptions of releasing source code as cited from the Federal Source Code Policy M-16-21

Reviewers

 decause-gov ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may

<https://github.com/CMSgov/cms-open-source-policy>

Open Source Policy V1.1

Incorporates the
baseline tools and
processes we created
into guidance

OSS Implementation & Infrastructure

Any CMS project team that wishes to publish their code as OSS must set a clear expectation of their level of involvement in sustaining that project. The project team shall define an OSS release process that begins with a determination of if the intended software can indeed be released as OSS, considering any security and other CMS policy restrictions. Depending on the nature of the OSS and associated licensing model, the project team shall adequately allocate resources to be able to sustain and flourish the project in the open source community.

The project team shall utilize an existing public-facing website to convey information about the project and provide a link to the project's GitHub repository. The project team should implement tools to support the community around an open source project, such as mailing lists, message forums, a version control, wiki, and tracking mechanisms, such as Kanban boards to track issues and bugs on the GitHub repository.

For every iteration of the code release, the project team must ensure that the software code is adequately peer reviewed ~~and is free of~~ security vulnerabilities that can be exploited by malicious actors and that any discovered vulnerabilities are removed prior to release. Until the software code is adequately reviewed, it should be either 1) maintained in an internal code repository that replicates the intended public repository or 2) checked by publicly available services providing the same functions on all code check-ins to the public source code repository. The software should also contain automated unit tests; and build scripts and should be checked for software vulnerabilities, code quality and code coverage using available standard CMS tools and guidance. The code should be built with CMS's standard continuous integration (CI) ~~server~~servers. The project team should include ample documentation with the software code for increased adoption and modification by the community. The documentation should provide the information on project's mission, philosophy, goal, design, decision-making process, product roadmap and instructions on how to submit issues, feature requests and how to contribute towards a fix or enhancements. The documentation should be accessible to the Open Source community via the repository.

<https://github.com/CMSgov/cms-open-source-policy>



Raising the Ceiling

Releasing & developing open source projects
that solve real-world problems

Repositories we've outbounded

12 repositories released in the past 6 months



CMS OSPO tools

Facing a Financial Shock

Income Verification Pilot

AI Explorers Program

CMS Medicare Handbook Project

Raising the Ceiling

- Building prototypes where we identify gaps in the software ecosystem



DedupliFHIR



Hospital Price
Transparency Tools

Raising the Ceiling

- Building prototypes where we identify gaps in the software ecosystem



DedupliFHIR



Hospital Price
Transparency Tools

Problem

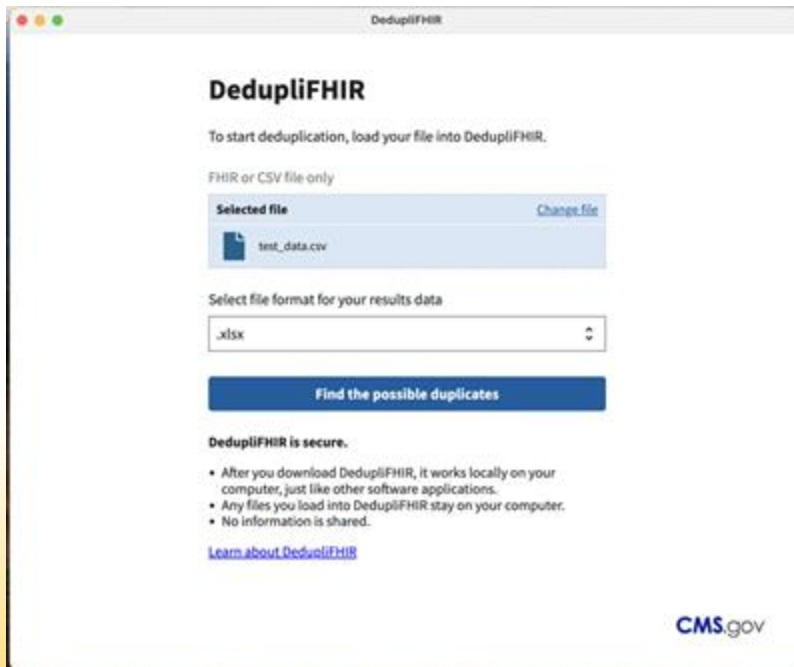
- Accountable Care Organizations (ACOs) report electronic quality of care measures (eCQMs) to CMS annually as part of the Share Savings Program
- ACOs will need to transition from reporting eCQMs via the CMS WebUI, to a “real-time electronic system” by 2025
- During our listening sessions with users, ACOs reported when preparing this data, **identifying duplicates in patient records was a challenge**

Solution

- ☒ Conduct a Discovery Sprint
- ☒ Conduct Listening Sessions
- ☒ Build a Prototype
- ☐ Conduct User Research 🔴
- ☐ Ship a modular, standards compliant, open source project
- ☐ Build a community around the project

DedupliFHIR

Data Linkage & AI Deduplication tool that assists ACOs with identifying duplicates within their patient records




DedupliFHIR

To start deduplication, load your file into DedupliFHIR.

FHIR or CSV file only

Selected file [Change file](#)

 test_data.csv

Select file format for your results data

.xlsx

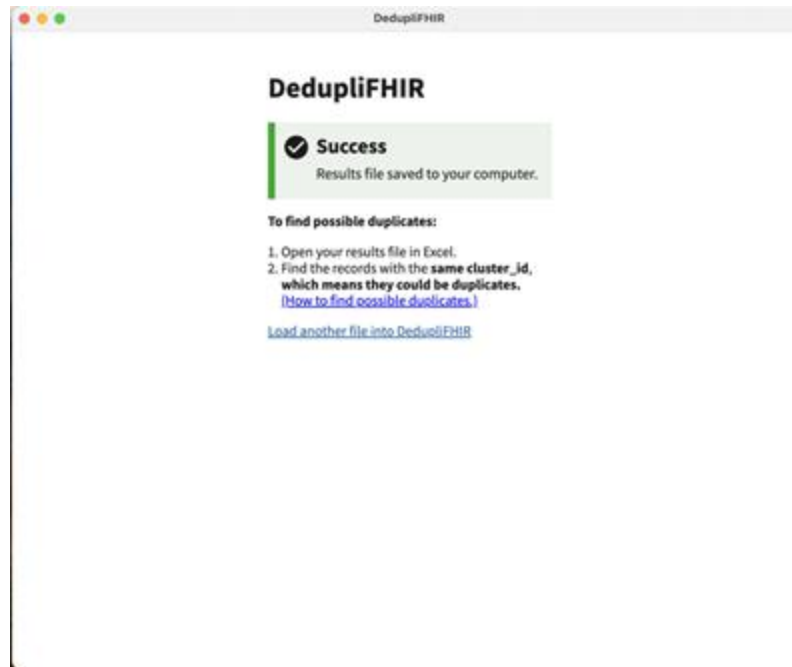
Find the possible duplicates

DedupliFHIR is secure.

- After you download DedupliFHIR, it works locally on your computer, just like other software applications.
- Any files you load into DedupliFHIR stay on your computer.
- No information is shared.

[Learn about DedupliFHIR](#)

CMS.gov



DedupliFHIR

Success
Results file saved to your computer.

To find possible duplicates:

1. Open your results file in Excel.
2. Find the records with the same cluster_id, which means they could be duplicates. [\(How to find possible duplicates.\)](#)

[Load another file into DedupliFHIR](#)



Powered by Splink, open source tool developed by UK Ministry of Justice

DedupliFHIR

Received feedback on tool through feature requests and user research sessions

Incorporate data normalization for relevant demographics #55

 Closed cooperthompson opened this issue on May 3 · 2 comments · Fixed by #75, #99, #110 or #111



cooperthompson commented on May 3

Is your feature request related to a problem? Please describe.

It doesn't appear that Splink handles data normalization. There are several demographics that either benefit from, or essentially require data normalization. For example:

- Different punctuation for patient names. E.g. "Jean-Claude Van Damme" vs. "Jean Claude Van Damme".
- Different phonetic spellings of names. E.g., "Jon" vs. "John".
- Different abbreviations in both names and addresses. E.g., "St" vs. "St." vs. "Street", Or "Jr." vs. "Junior" for names.

Describe the intended behavior

The demographics for these two patients probably should be normalized prior to submission to the record linking process.

Jon Smith at 123 Main Street

John Smith at 123 Main St.

Allow User to Choose File Output and Format #47

 Closed IsaacMilarky opened this issue on Apr 25 · 0 comments · Fixed by #53



IsaacMilarky commented on Apr 25

Member ...

Is your feature request related to a problem? Please describe.

Right now the output is always an excel file named `deduped_record_mapping.xlsx`. This is clunky and bad.

Describe the intended behavior

The user should be able to determine the file format and filename of the de-duped data file.

Describe the solution you'd like

The output file will be determined by the last CLI argument passed into the CLI.

The format will also be determined by the last CLI argument passed into the CLI.

Additional context

Feature requested by cocotavius@mdinteractive.com



What's Next

It's Official!



6. **Establish the First U.S. Government OSPO:** The Department of Health and Human Services (HHS) Center for Medicaid and Medicare Services (CMS) recently established the first Open-Source Program Office at a United States Federal Agency.^{x1} The function of the OSPO is to establish and maintain guidance, policies, practices, and talent pipelines that advance equity, build trust, and amplify impact across CMS, HHS, and Federal Government's open-source ecosystem by working and sharing openly.

THE WHITE HOUSE



AUGUST 09, 2024

Fact Sheet: Biden-Harris Administration Releases Summary Report of 2023 RFI on Open Source- Software Security Initiative

ONCD • BRIEFING ROOM • PRESS RELEASE

August 9, 2024

[Read the full report here](#)

Today, the White House Office of the National Cyber Director, in partnership with members of the Open-Source Software Security Initiative (OSSSI), is publishing a summary report on the *Request for Information (RFI) - Open-Source Software Security: Areas of Long-Term Focus and Prioritization*. This builds on the commitment the Administration made in the *National Cybersecurity Strategy*, "to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools."

SUMMARY OF THE 2023 REQUEST FOR INFORMATION ON OPEN-SOURCE SOFTWARE SECURITY

AUGUST 2024



CMS.gov



Science and
Technology



U.S. DEPARTMENT OF
ENERGY

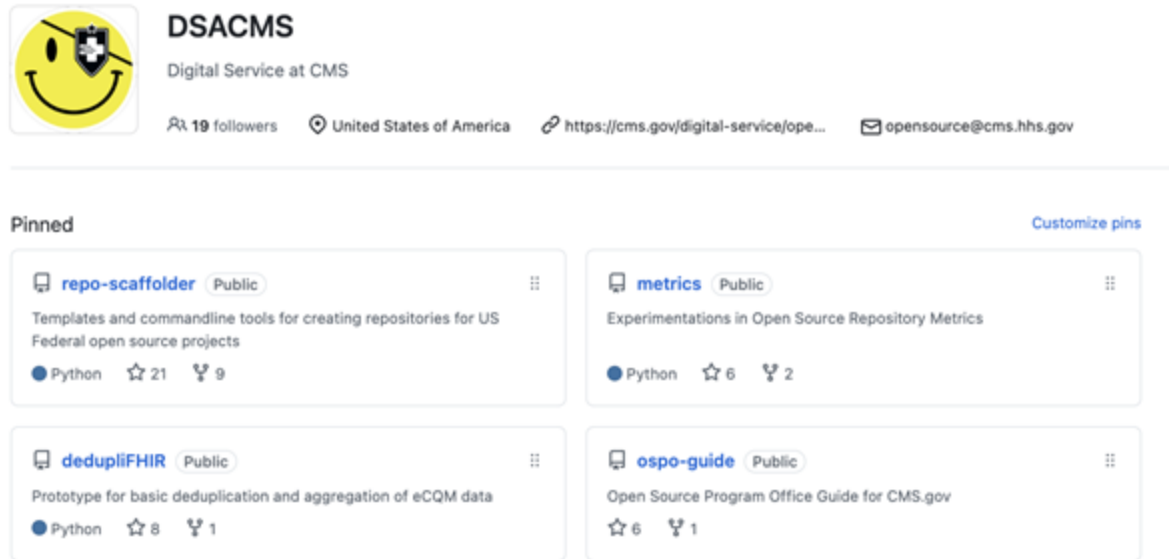
OPEN-SOURCE SOFTWARE SECURITY
RFI SUMMARY

Looking Forward

- Word of the Year 2024: Execute
- Word of the Year 2025: Integrate
- Align with OSPOs across the Federal Government
- Align with OSPOs around the world



How to Contribute



Follow what we are up to: github.com/DSACMS

**US DIGITAL
RESPONSE**



USWDS

Simpler.Grants.gov



CMS Blue Button 2.0

Contribute to federal open source projects

Join us!



digitalcorps.gsa.gov

A 2 year government fellowship program
for early-career technologists
to launch impactful careers in public service

coding it forward >

codingitforward.com

A 10 week summer fellowship program
for early-career technologists
to work in government

THANK YOU



opensource@cms.hhs.gov



github.com/DSACMS



go.cms.gov/ospo



linkedin.com/company/digital-service-at-cms/

me
+we