get-nih-ready

NIH and You: MFA, Identity Assurance, and Coming Requirements

A Roadmap to Be NIH Ready

To enable its mission, the National Institutes of Health (NIH) is expanding its NIH Login Service gateway to facilitate secure access to NIH IT resources by biomedical researchers, faculty, and scientists around the globe. Resources protected by the NIH Login Service include controlled-access research data and grants administration systems.

InCommon participants whose users access NIH resources via federated access need to update their identity providers meet three requirements:

- **Release Basic User Information** about the people accessing NIH resources so that we can provision and manage efficient and secure access.
- **Perform Multi-factor Authentication** (MFA) to minimize risk to NIH IT resources.
- **Provide Identity Assurance** that each person who logs in is who they say they are so that NIH can provide appropriate authorization to access NIH data.

What does this mean?

NIH is asking InCommon (and international R&E federation) Participants to update their federated single sign-on service to support three research and education federated access standards.

NIH's Requirement	InCommon Participant's To Do
Release Basic User Information	Release the user information defined in the REFEDS Research and Scholarship (R&S) entity category when a user signs into NIH resources.
Perform Multi-factor Authentication (MFA)	Perform MFA for a user when requested by the NIH Login Service; support MFA request and response signaling using the REFEDS MFA Profile.
Provide Identity Assurance	Perform appropriate identity proofing and credential binding for users accessing federated resources; at sign-in time, communicate each user's identity proofing level using the REFEDS Assurance Framework.

Getting Started, Step-by-Step

We understand this can be a complicated undertaking. You do not have to do everything at once. We've prepared a Step-by-Step Guide to help everyone along this journey. NIH also provides a Compliance Check Tool to help you to determine your campus' identity provider progress toward meeting these requirements.

workbox Read the Step-by-Step Guide to Implement NIH Requirements

success Test your IdP with the NIH Security Compliance Check Tool

Schedule

Phase I - eRA MFA Requirement Rollout

Event Calendar

Upcoming Events

Past Events

(September 8, 2021) Microsoft / Cirrus Identity Webinar - Leveraging Azure AD & Cirrus Identity Bridge to meet the NIH MFA Mandate

Join Microsoft and Cirrus Identity to learn how the Cirrus Identity Bridge makes it easy for educational institutions to leverage Azure AD and their membership in the InCommon Federation to meet NIH's MFA requirement.

(Session Recording)

(May 12, 2021) IAM Online - Increasing Identity Assurance and Improving NIH Readiness

(Slides and Recording)

(April 14, 2021) IAM Online - National Institutes of Health (NIH) New MFA and Identity Requirements

(Slides and Recording)

(April 1, 2021) NIH Office Hour

Join representatives from InCommon and the National Institutes of Health to discuss the coming changes to the NIH electronic Research Administration (eRA) modules.

(Zoom Recording)

March 10, 2021 - NIH Office Hour

(Zoom Recording)

Resources

- REFEDS MFA Profile
- REFEDS Research and Scholarship (R&S)
- REFEDS Assurance Framework
- R&S Explained in Plain English
- REFEDS Assurance Working Group wiki

Duration: November 2020 to September 15, 2021.

Phase I lays the foundation for a new standard of federated login to NIH systems and sites, starting with the NIH Electronic Research Administration (eRA) system. Starting September 15, 2021, a user signing into eRA using federated credentials needs to authenticate with MFA. To support the requirement, federated partners need to be able to interpret and correctly respond to this signal. Further, NIH requires basic user information including persistent unique identifier, name, email, and affiliation. This basic information equates to the REFEDS Research and Scholarship Entity Category (R&S).

The eRA modules included in this rollout are: eRACommons, ASSIST, InternetAssistedReview(IAR), CommonsMobile.

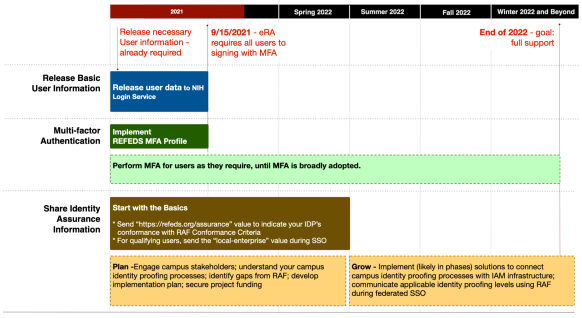
If your organization receives NIH grants and does not yet meet these requirements, it's not too late. researchers can return to using campus credentials to sign in to eRA when your IdP is ready. Use the eRA Readiness Guide to update your identity provider to enable your users to sign in to eRA using your campus credential.

Phase II - Share Identity Assurance Level to enable user access t o Controlled Access Research Data

Duration: Now to December 2022

Identity assurance is a measure of confidence that the person using a credential to login is the person to whom the credential was issued, and is in fact who they claim to be. As the NIH Login Service expands to protect additional NIH online resources, some, particularly access to sensitive controlled-access research data, will require the campus to disclose the level of identity proofing (identity assurance) in addition to performing MFA for a user signing into these sensitive resources.

Continue on to the Requirement III: Provide Identity Assurance section of the Step-by-Step Guide to find out how to plan and implement the appropriate identity assurance process on your campus.



Community Activities

Several InCommon and international working groups are working to develop additional materials to clarify additional implementation details.

The Assured Access Working Group, chartered by the InCommon Trust and Assurance Board (CTAB), has developed the *REFEDS Assurance Framework Implementation Guidance for InCommon Participants* document to provide campus-level implementation guidance on implementing the REFEDS Assurance Framework by leveraging common campus identity proofing processes.

The REFEDS MFA Subgroup, a taskforce chartered by the REFEDS Assurance Working Group, is answering detailed questions around MFA transaction handling.

Consulting Assistance

Partners participating in the InCommon Catalyst Program are skilled and ready to help you design and implement solutions to meet these NIH requirements. If you need help, these Catalysts are great resources:

- Cirrus Identity
- Research Data and Communication Technologies (RDCT)
- Spherical Cow Group
- Unicon

- Assured Access Working Group wiki
- eRA Security Compliance Check Tool

Resources

- Cirrus Helps Institutions Meet NIH Requirements with the Bridge Federation Adapter
- **Educause Review:** Cloud-First Approach for NIH and Academic Research Access

---

Key Dates (as they become known)

Details of specific deadlines and requirements are gathered here, as they become known to InCommon. Some of the following are placeholders that represent a subset of the information InCommon expects to learn in the coming months.

Electronic Research Administration Portal (eRA)

Date	September 15, 2021
Access Requirements	1. **Release Necessary User Information** - Release the user information defined in the REFEDS Research & Scholarship (R&S) entity category. 2. **Multi-factor Authentication** - Accept multi-factor authentication requests and signal outcome using the REFEDS MFA Profile.

Effective September 15, 2021, eRA (https://era.nih.gov) will require all of its users to sign in with MFA. eRA will accept qualified federated credentials. To qualify, the IdP needs to authenticate the user using MFA and signals the outcome using REFEDS MFA Profile. In addition, eRA will require the IdP to release user attributes defined in the REFEDS R&S category.

About eRA

eRA is NIH's research administration portal. Principal Investigators and grant administrators from universities and research organizations use eRA to apply for and manage NIH-funded grants. eRA has about 40,000 users and over 204,000 grants in its database. Over 130,000 of the grants are issued to InCommon participants.

Impact

If your institution receives NIH funding, your research administrators and principal investigators likely have access to eRA.

Users who cannot sign in using a qualified credential from their home institution will be directed by eRA to create and use a login.gov credential to sign into eRA.

IdP Operator: sign into the eRA Security Compliance Check Tool to determine if your IdP meets eRA requirements.

National Center for Biotechnology Information (NCBI; PubMed)

Date	To be announced
Access Requirements	**Release Necessary User Information** - Release the user information defined in the REFEDS Research & Scholarship (R&S) entity category.

The National Center for Biotechnology Information (NCBI) operates PubMed, MyNCBI, SciENcv, MyBibliography, and a number of NCBI-managed data services. It will transition its services to use only federated credentials for user access (https://ncbiinsights.ncbi.nlm.nih.gov/2021/01/05/important-changes-ncbi-accounts-2021/).

NCBI requires a federated IdP to release attributes defined in R&S. It does not require MFA or identity assurance information.

About NCBI and PubMed

The National Center for Biotechnology Information (NCBI) is a division of the National Library of Medicine (NLM) at the National Institutes of Health (NIH). As a national resource for molecular biology information, NCBI's mission is to develop new information technologies to aid in the understanding of fundamental molecular and genetic processes that control health and disease.

PubMed is one of the world's largest online biomedical research databases. It has millions of users around the world. It is likely that all universities have some students or faculty accessing PubMed today.

NIH Login Service

Milestone	Date
Diagnostic aid for identity provider operators	TBD
Process identity assurance information	TBD
REFEDS MFA Profile support	TBD
Support self-service account selection	TBD

About NIH Login Service

The NIH Login Service is an NIH Identity and Access Management service offered by CIT to provide centralized authentication and Single Sign On (SSO) capability for web-based applications. The NIH Login is a "one-stop shop" which allows logins from all of NIH staff, eRA Commons, HHS employees, and various Federated partners.

Researcher Authorization Service (RAS)

Date	TBD
Access Requirements	1. **Release Necessary User Information** - Release the user information defined in the REFEDS Research & Scholarship (R&S) entity category. 2. **Multi-factor Authentication** - Accept multi-factor authentication requests and signal outcome using the REFEDS MFA Profile. 3. **Share Identity Assurance Information** - Signal user identity assurance information using the REFEDS Assurance Framework.

About RAS

RAS (https://datascience.nih.gov/researcher-auth-service-initiative) facilitates access to NIH's open and controlled data assets and repositories in a consistent and user-friendly manner. Overtime, RAS will become the access gateway to many of the NIH data services. Among them:

dbGaP - dbGaP is the database of Genotypes and Phenotypes (dbGaP) was developed to archive and distribute the data and results from studies that have investigated the interaction of genotype and phenotype in Humans.

All of Us - The All of Us Research Program is inviting one million people across the U.S. to help build one of the most diverse health databases in history. We welcome participants from all backgrounds. Researchers will use the data to learn how our biology, lifestyle, and environment affect health. This may one day help them find ways to treat and prevent disease.

NIMH Data Archive - The National Institute of Mental Health Data Archive (NDA) makes available human subjects data collected from hundreds of research projects across many scientific domains. NDA provides infrastructure for sharing research data, tools, methods, and analyses enabling collaborative science and discovery. De-identified human subjects data, harmonized to a common standard, are available to qualified researchers. Summary data are available to all.