Implementing CADR Requirements for NIH Websites

A Case Study

Leslie E Carroll, David G Hacker

Information Management Services, Inc.

November 2025

Executive Summary

To advance scientific discovery and accelerate medical breakthroughs, National Institutes of Health (NIH) researchers are increasingly required to share biomedical data responsibly and effectively. Making research data accessible enables collaboration, reproducibility, and new insights, but the NIH must ensure that the privacy and security of sensitive participant information is not compromised by sharing it. This evolving landscape of biomedical research demands that sensitive clinical and biospecimen data for human subjects be shared securely and efficiently. In response to *Executive Order 14117*[1] and new NIH mandates, Controlled Access Data Repositories (CADRs) are now required to implement stringent security measures, identity verification, and access control standards to protect Americans' sensitive personal data from unauthorized access.

This paper provides a practical case study of how an existing biomedical data platform can be adapted to meet evolving federal cybersecurity mandates, ensuring that the integrity of scientific research is preserved without compromising security. BioShare, a web-based platform developed by Information Management Services, Inc. (IMS), has been recently updated to ensure that it offers a comprehensive solution designed to meet these enhanced NIH CADR requirements. BioShare is currently used by multiple government institutes and programs to provide researchers with a centralized website for searching, requesting, and accessing controlled datasets and biospecimens, supported by robust workflows and strong security measures.

By adapting to CADR-compliant standards, government and research organizations can efficiently meet NIH security mandates, strengthen data governance, and facilitate responsible scientific collaboration, while balancing data protection with accelerating biomedical discovery. The modifications to BioShare discussed below, and its underpinnings in agile development, have streamlined compliance with the new CADR requirements with minimal downtime.

Introduction/Background

Over the past decade, the NIH has increasingly emphasized the importance of secure, centralized platforms to facilitate the ethical and efficient sharing of clinical and research data, as well as biospecimens, across the scientific community. This need stems from the growing scale and complexity of biomedical research, which demands collaborative access to diverse datasets and biological samples to advance scientific knowledge and improve public health outcomes. Data sharing platforms play a critical role in supporting this mission by streamlining data discovery, request workflows, and compliance monitoring. However, as the volume and sensitivity of shared data have grown,

particularly with the inclusion of genomic data, ensuring robust security and access controls has become imperative to protect participants' privacy.

With heightened cybersecurity threats and growing concerns over data sovereignty, the protection of sensitive Protected Health Information (PHI) and Personally Identifiable Information (PII) has become a top priority for research institutions and government agencies alike. Recognizing these challenges, the White House issued *Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*[1], aimed at safeguarding national interests by tightening controls on how sensitive data are accessed, stored, and shared, particularly within research and biomedical domains.

In response to this Executive Order, the NIH has implemented a series of stringent security policies for CADRs[2,3]. These new policies are designed to mitigate the risk of unauthorized data access by foreign entities and ensure that US research data, especially those involving PHI and PII, remain secure and compliant with federal directives.

The Challenge

For existing CADRs, adaptation to new NIH security policies for data sharing presents a challenge. The requirements involve compliance with user authentication and access controls; support for Data Access Committee (DAC) review; maintenance of Data Use Agreements (DUAs); additional security for data delivery; enhanced requirements restricting requestor approval; and compliance with NIST 800-53's[4] moderate baseline controls.

Retrofitting security features into systems that were built without anticipating future needs can be difficult, especially with staff that have limited experience with new technologies. Integrating the new requirements may involve changes across multiple system components, introducing a level of complexity that may result in compatibility issues. Additionally, the time and effort required to complete such upgrades can be extensive, requiring downtimes, configuration changes, and possibly user retraining.

Analysis/Discussion

This section details a case study for upgrading IMS's BioShare platform to comply with the latest CADR standards set forth by NIH. A brief system overview is offered, followed by a selection of challenges presented by the new NIH policies and the implementation approach that was used to bring BioShare into compliance.

System Overview

BioShare, developed by IMS, is a web-based platform that serves as a centralized portal for managing biospecimen and data sharing across research institutions. It enables researchers to search available collections and submit structured requests, while allowing administrators to track request workflows from initiation through approval and delivery within a unified, user-friendly interface. The system's integrated request tracking seamlessly coordinates DAC review, voting, and approval; document and dataset management; DUA generation with optional DocuSign[5] e-signature; secure data delivery; email scheduling; cost tracking; and reporting. BioShare is hosted as a Software as a Service (SaaS) solution in IMS's FISMA-moderate data centers and meets OMB A-130[6] and NIST Moderate-level security standards, including Transport Layer Security (TLS) based authentication, role-based access control, and fine-grained public vs. private data visibility. BioShare has been used as the basis for multiple NIH systems, including NIA's AgingResearchBiobank, NIDDK Central Repository, and NeuroBioBank, among others.

Notably, BioShare is architecturally and functionally inspired by, and built upon components of IMS's NHLBI Biologic Specimen and Data Repository Information Coordinating Center (BioLINCC).

Implementation of Requirements

Implementing NIH CADR requirements within an existing web platform such as BioShare required both technical adaptations and organizational coordination to meet the elevated security, access control, and identity verification standards.

The BioShare platform already partially met the Executive Order requirements. It has always incorporated fine-grained user authentication and access controls, including multi-factor authentication (MFA). Additionally, BioShare's system architecture benefits from deployment in IMS's FISMA-moderate certified environment, which supports encrypted data at rest and in transit, secure audit logging, and regular penetration testing to identify and address vulnerabilities. All public and administrative endpoints have been reviewed and updated to meet NIST 800-53[4] moderate-level controls, including enhanced incident response protocols, system activity auditing, and intrusion detection capabilities.

However, several additional requirements related to the Executive Order were not previously met by BioShare, including the blocking of access from countries of concern, disallowing site registration by those with email addresses unaffiliated with their institution or corporation, federated Identity Assurance Level 2 (IAL2) authenticated login support, and institutionally validated user identity workflows. These additional items had to be integrated into BioShare's already complex authentication workflows.

Role-based permissions that ensure strict separation of duties and limit data visibility based on user clearance levels and project affiliations needed to be refined, as access to controlled data collections now requires oversight by a senior researcher/principal investigator (PI) and robust justification and documentation during the request process, with real-time monitoring and access logging integrated throughout the workflow.

The request review and data governance workflows were also adapted to support NIH's new oversight requirements, including integration of compliance checkpoints, flagging of suspicious access patterns, and configurable restrictions for data export, download, or transfer. Administrative workflows now offer greater visibility into user activity, data request histories, and institutional affiliations to help data stewards monitor for potential compliance risks.

These enhancements were incorporated iteratively using an agile development process in close consultation with existing stakeholders. This approach resulted in minimized impact on production sites and streamlined user acceptance with well-documented change notifications.

Requirement: User authentication and access controls

Challenge:

To align with the mandates of *Executive Order 14117*[1] and the updated NIH security requirements[2,3], CADRs must be enhanced to minimize the risk of unauthorized access, particularly from foreign entities identified as countries of concern. These requirements safeguard sensitive personal data, especially genomic, clinical, and government-related datasets, against exploitation.

Solution:

One of the most significant changes centered on enforcing IAL2, which is now required for all systems managing access to controlled datasets. IAL2 enforcement ensures that users' identities have been properly verified, reducing the risk of unauthorized or fraudulent access. Meeting this requirement necessitated integration with federally approved identity services that support IAL2 credentials. Specifically, BioShare supports IAL2 compliance through:

1. NIH PIV Authentication – used primarily for intramural NIH projects and staff with government-issued Personal Identity Verification (PIV) cards.
2. Login.gov – a federal identity verification platform that supports IAL2-compliant authentication for extramural, US-based user communities.
3. ID.me – A digital identity network that allows users to verify their identity and group affiliations. Supports IAL2-compliant authentication for international user communities.

To avoid interruptions in access among existing extramural users of BioShare-based CADRs, all of whom were previously using the basic IAL1 version of Login.gov, IMS used a measured approach to the IAL2 transition. Since IAL2 enforcement with Login.gov requires a US state-issued ID, the transition began by asking active international investigators to move to ID.me with IAL2 authentication. Only after these international investigators had established their ID.me credentials did we implement IAL2 enforcement with Login.gov for the remaining extramural investigators. NIH investigators continued to use NIH PIV authentication, which is IAL2-compliant.

Additional measures were also implemented to block access from countries of concern via both geofencing and blocking site registration by those not using an institutional email address or those from countries of concern.

Requirement: Data Access Committees (DACs)

Challenge:

As part of the NIH's enhanced security framework for CADRs[2,3], institutions must implement rigorous oversight mechanisms to ensure that only appropriately vetted researchers are granted access to sensitive data. Central to this process is the use of DACs, designated groups of federal employees responsible for reviewing data access requests to ensure they meet scientific, ethical, and regulatory standards, as well as prohibiting access by institutions in countries of concern, before access is granted.

Per the new NIH policy, DACs must include a chair, co-chair, and senior federal employees who possess appropriate scientific, bioethical, or other relevant expertise. These individuals are responsible for evaluating the purpose, methodology, and justification of each data access request. DACs may also invite external consultants with specialized knowledge to provide written input or to participate in review meetings on an ad hoc basis.

Solution:

Many of these requirements were already met by BioShare, including a configurable Review Module designed specifically to facilitate DAC operations. The platform allows administrators to define custom roles and permissions, which were used to create separate review interfaces for DAC members and ad hoc scientific reviewers. This separation ensures that each reviewer sees only the information and tools relevant to their function, maintaining data security and clarity in the review process.

The Review Module aggregates all necessary documentation for each request, including investigator and collaborator contact information, an institutional affiliation attestation signed by a Signing Official (SO) from each investigator/collaborator's institution, research summaries, analysis plans, IRB oversight documentation, and principal investigator CVs. These materials are tagged and organized for easy

identification and review, reducing administrative overhead and enabling a more streamlined evaluation process. By providing a flexible and secure environment for DAC operations, BioShare enables institutions to fully implement NIH-compliant data access oversight while maintaining efficiency, transparency, and accountability throughout the review process.

Additionally, BioShare supports the creation of DAC-specific web pages, viewable only by users with DAC Reviewer roles. These pages can host essential governance materials such as the DAC Charter, Standard Operating Procedures (SOPs), and training documentation, further ensuring compliance with NIH requirements and internal policy frameworks.

Requirement: Data Use Agreements (DUAs)

Challenge:

In accordance with NIH policy, all CADRs must enforce clearly defined DUAs as a condition for granting access to sensitive datasets. These agreements serve as a legal and administrative safeguard to ensure that data are used only for approved research purposes and are handled in compliance with federal privacy, security, and ethical standards.

As mandated, NIH CADRs are required to incorporate specific language into their DUAs using the standardized language provided in the *NIH Security Best Practices for Users of Controlled Access Data*[7] document. This standardized language addresses critical issues such as data security obligations, restrictions on data sharing, acceptable use parameters, and compliance with *Executive Order 14117*[1]. Furthermore, each data access approval must be time-limited, with the duration of access not to exceed 12 months. These restrictions are designed to reduce long-term exposure risks and ensure periodic re-evaluation of data usage and user eligibility.

Solution:

The content and enforcement of DUAs are typically managed by each NIH Institute or Center's Technology Transfer Office. While language and terms may vary slightly across Institutes, all must adhere to the NIH-approved template as the baseline. To assist with enforcing the execution and enforcement of DUAs, BioShare can track signature status, store completed DUAs, and enforce access restrictions until the agreement is fully executed.

To streamline the execution and tracking of DUAs, BioShare supports an optional DocuSign[5] integration that enables institutions to adopt a digitally signed DUA workflow. Using this feature, administrators can configure BioShare to issue the correct DUA version, preloaded with the required NIH CADR template language, and route it electronically for signature by the requesting investigator and institutional SO. Minimal

effort was involved in updating BioShare to include the new NIH CADR language in DUA templates.

In addition, BioShare's request management infrastructure supports automated access expiration tracking, ensuring that data access is revoked or renewed at the 12-month mark, in line with NIH CADR requirements. Notifications and administrative workflows alert both investigators and oversight staff as expiration dates approach, promoting timely compliance and minimizing data exposure risk. When access is revoked, the required data destruction document is tracked in BioShare. A configuration change was used to enforce the new 12-month access limit in each BioShare-based CADR.

Requirement: Secure Data Delivery

Challenge:

Following the approval of a data access request (DAR) through the BioShare platform, the final step in the CADR sharing process is the secure and compliant delivery of authorized datasets. NIH CADR policy requires that each approved request explicitly identify the project title and specific datasets that the PI or data requester is authorized to access. Data must be accessed only by the PI or senior official who will provide institutional oversight for its usage. Additionally, CADRs and their associated access management systems must tag and retain this metadata to support monitoring, auditing, and federal reporting requirements.

Solution:

To meet these expectations, IMS enhanced BioShare's optional Data Delivery Module that enables secure, permission-based distribution of datasets. Once a request has been reviewed and approved by the appropriate DAC, communications or data management staff use this module to select a tailored data package associated with the approved project and make it available for download only to the authorized user(s). Permissions are tied to the specific user profile and request ID, ensuring strict adherence to project-specific access limits.

This delivery process is further enhanced by the system's ability to assign expiration dates to data download windows, after which access to the data package is automatically revoked. This is a configurable date for each data transfer.

Importantly, BioShare also ensures full auditability by maintaining download activity logs within its secure database. These logs capture key metadata, including user identity, project association, dataset delivered, time and date of access, and expiration status. These data support institutional and NIH-level compliance audits, facilitate oversight of individual data use, and provide traceability in the event of a security review or policy breach. While the audit trail existed previously, it was expanded to capture additional metadata.

Requirement: Requestor Eligibility

Challenge:

New CADR security policies[2,3] require that DARs must be submitted by senior officials or PIs who will be accountable for ensuring that all aspects of data usage align with the terms of the DUA and institutional policy. Additionally, an institutional SO from each collaborator's institution must be identified. All communication with requestors, collaborators, and SOs must use their affiliated institutional email addresses. Collaborators from different institutions must submit their own DAR and identify an SO from their own institution.

Solution:

BioShare's request form is fully configurable and can be used to collect contact information and institutional affiliation for the PI, their SO, and each of their collaborators from the same institution. Because collaborators from different institutions are now required to submit separate requests and identify their own institutional SO to sign their own DUAs, BioShare has implemented a linked request feature to associate collaborator requests with the originating request.

To further comply with this requirement, BioShare was updated to ensure that all requestor, authorized user, and SO communication are affiliated with the appropriate institutional domains. The request form can be translated into a PDF and provided as a supporting document in the Review Module. This allows DAC members to more easily confirm that appropriate access is granted.

Requirement: FIMSA-moderate Computer Center

Challenge:

All CADRs and their access management systems must protect the confidentiality, integrity, and availability of the data in accordance with NIH NIST 800-53's moderate baseline controls[4].

Solution:

BioShare has always been hosted in the IMS Computer Center, which provides a firewall, a virtual private network (VPN), and an intrusion prevention system with continuous monitoring and logging. Alerts are generated and delivered to the appropriate staff in real time as situations arise. Routine security checks of IMS computer resources are made with security analysis software tools. The production network is housed in physically separate and secured computing facilities. Network access requires authorized user ID and password-protected access with MFA. IMS has multiple NIH-approved IT system security plans in place that meet the OMB Circular A-

130[6] guidelines and the NIST guidelines[4] for IT system security at the “moderate” level. No changes to BioShare were needed to meet this requirement.

Requirement: Transparency and Utility

Challenge:

NIH CADRs must collect and make publicly available metadata to enable discovery, reuse, and citation of datasets. CADRs must also provide publicly available information on research uses including data use statements/summaries with project dates, and user and institution names.

Solution:

BioShare provides study pages which can be used to describe each collection of biospecimens or data. These study pages contain structured data about the collection that can be used to foster transparency and discoverability. In addition, BioShare has an Approved Projects page that lists a summary of each request, including the PI name and institution and any resulting publications.

Impact

This approach to implementing upgrades aligned with the new NIH CADR policies[2,3] allowed IMS to provide all necessary security measures without disrupting live website usability for existing CADRs. IMS’s experience with rapid turnaround from requirements to a fully operational data sharing platform was reinforced by the adoption of enhanced security protocols, streamlined researcher access, and compliance with evolving federal mandates, ultimately reducing both risk and administrative burden.

Another key strength of the approach IMS took to enhancing BioShare’s security posture lies in its flexible, highly configurable architecture, which allowed enhancements to be made with minimal time and effort. By leveraging templates, configurations, and customizable workflows, BioShare was rapidly upgraded to meet the new policy requirements without extensive redevelopment efforts. This modular approach also promotes easier transitions in the future, as requirements continue to be refined to protect data security and privacy.

Conclusion

As NIH strengthens security requirements under *Executive Order 14117*[1] and its mandates for CADRs, existing government and research data platforms face increasing pressure to enhance their identity verification, access controls, and data governance capabilities. To enhance existing systems, many changes may be required. Systems that enact these changes while keeping the evolving nature of the data security

landscape at the forefront of their designs position themselves strategically to benefit from those considerations later. Configurability and flexibility are the cornerstones of producing a CADR site that meets both NIH policy and research community needs, while also anticipating how those needs will change in the future.

BioShare offers a robust, configurable, and rapidly deployable solution designed specifically to meet these evolving standards. The architecture of the IMS BioShare platform incorporates advanced features such as integrated DAC workflows, enforceable DUAs, secure data delivery mechanisms, and stringent requestor requirements to enable institutions to confidently safeguard sensitive biomedical data while maintaining streamlined researcher access.

Government data platforms currently operating outside of CADR compliance should strongly consider adopting a CADR-compliant platform that is forward thinking, such as BioShare. Doing so not only addresses federal security mandates but also enhances operational efficiency, transparency, and auditability, ultimately fostering a trusted environment for scientific collaboration that protects both research participants and national interests.

References

1. Executive Office of the President. (2024, March 1). Preventing access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern (Presidential Document No. 2024-04573, 89 Fed. Reg. 15421). Federal Register. https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related
2. National Institutes of Health. (2025, September 24). Required security and operational standards for NIH controlled-access data repositories (Notice No. NOT-OD-25-159). https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-159.html
3. National Institutes of Health. (2025, September). NIH Controlled-Access Data Repository (CADR) Implementation Guidebook (Version 1.0). https://grants.nih.gov/sites/default/files/flmngr/NIH-CADR-Implementation-Guidebook.pdf
4. National Institute of Standards and Technology. (2020, September). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations (Update 1). https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
5. DocuSign, Inc. (n.d.). DocuSign [Homepage]. https://www.docusign.com/

6. Office of the Chief Information Officer, United States Government. (n.d.). OMB Circular A-130: Managing information as a strategic resource. https://www.cio.gov/policies-and-priorities/circular-a-130/
7. National Institutes of Health. (2025, September 30). Requirements for NIH Controlled-Access Data Repositories and Users. https://grants.nih.gov/policy-and-compliance/policy-topics/sharing-policies/accessing-data/requirements#nih-security-best-practices-for-users-of-controlled-access-data-and-repositories