AD Workbench as the Interoperability Layer: The Playbook

Alzheimer's Disease Data Initiative

AD Workbench

As our ecosystem grows and collaboration with external organizations becomes increasingly critical, a clear, standardized approach to interoperability is essential. The Interoperability Playbook document serves as a foundational guide to help both internal teams and external partners understand, plan, and execute integration strategies based on established patterns. Defining a clear taxonomy/nomenclature allows us to map our existing partnerships into specific categories and to determine the level of implementation (and ultimately the level of effort) required to engage on mutually agreed approaches that are value add-for all parties.

The AD Workbench seeks to:

- **Unlock** datasets across ecosystems by breaking down silos and supporting interoperable data sharing.
- **Enable** federated metadata search from remote partner repositories without duplicating datasets locally.
- **Provide** seamless user experiences whether through direct downloads, APIs, or managed workflows.
- **Ensure** governance, consent, and security for all data flows.

Interoperability Approaches

- Interoperability describes how two organizations connect their systems so users can sign in, view metadata and request access, and work with data.
- Based on each partner's technical setup, risk tolerance, and operational needs, there are different levels of interoperability. You can think of it as "basic," "standard," or "premium."
- Complete, two-way interoperability between platforms would be "premium," and task-specific, one-way interoperability would be "basic," with "standard" somewhere in between.

Specifically, there are three steps at which partners can make choices to tailor their integration:

1. Authentication and Access

How users and partner systems sign in and how security is established across organizations

2. Catalogue Listing

How metadata is presented, refreshed, and shared across organizations so users can submit Data Access Requests (DARs) and how partners review those requests and record decisions

3. Data Hosting, Sharing, and Governance

Where data resides physically and how researchers access it after their Data Access Request (DAR) has been approved

AD Workbench as the Interoperability Layer: The Playbook

Alzheimer's Disease Data Initiative

AD Workbench

Fig 1: Interoperability Approaches – A generic view of possible interoperability approaches

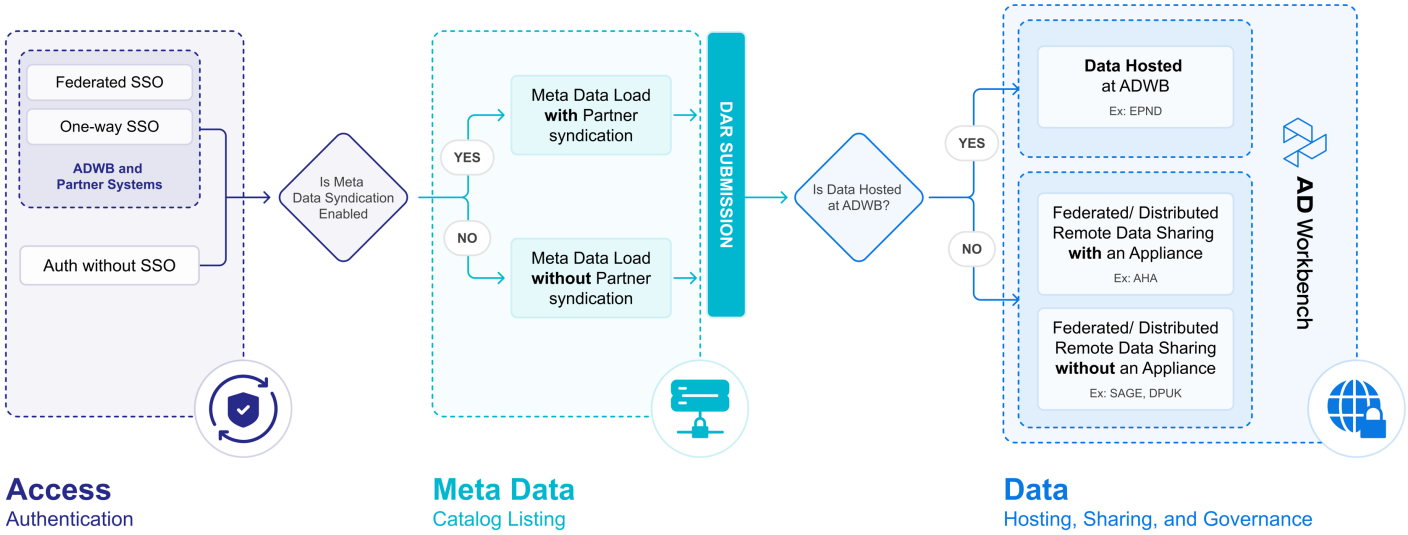
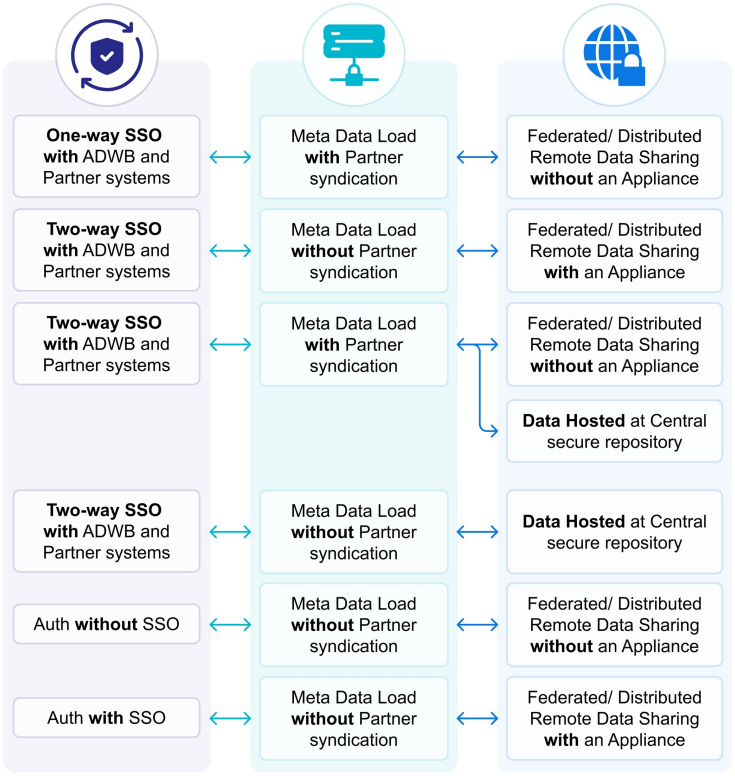


Fig 2: Interoperability – Configuration choices that have been made by existing partners



PARTNERS

AD Knowledge Portal
GAAIN
PRECISION MEDICINE PLATFORM
Dementias Platform UK | Data Portal
GATEWAY TO GLOBAL AGING DATA
the YODA PROJECT
Forging a unified scientific community
epnd European Platform for Neurodegenerative Diseases
ANSWER ALS
CPAD
NACC
UNIVERSITY of WASHINGTON
Vivli
HDRUK Health Data Research UK
Health Data Research Innovation Gateway

*Coming soon

AD Workbench as the Interoperability Layer: The Playbook

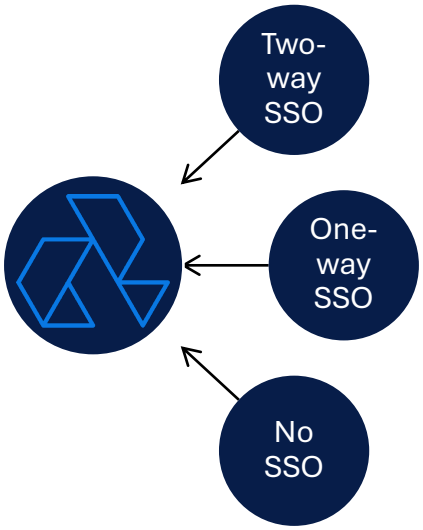
Alzheimer's Disease Data Initiative

AD Workbench
AD Workbench

Authentication Options

How users and partner systems sign in and how trust is established across organizations.

- **Two-way Single Sign On (SSO) with AD Workbench and partner systems**
  In a two-way SSO setup, both organizations trust each other's identity systems and allow cross-platform access for their researchers without needing separate accounts or duplicate logins. This creates a unified experience for researchers and administrators, making it easier to collaborate and manage access.
- **One-way SSO with AD Workbench and partner systems**
  In a one-way SSO setup, external users authenticate using their home organization's Identity provider, and access flows only into the AD Workbench platform. This lets partners maintain full control over their user identities without exposing their internal systems to reciprocal access. It is well-suited for partners who only need their users to enter our environment, not the reverse.
- **Authentication without SSO**
  When SSO is not supported or technically feasible, authentication can be handled through local AD Workbench accounts, username-and-password credentials, or token-based methods. This option is helpful for smaller partners and time-limited integrations.



Three authentication options are available to users and partner systems

Catalog Listing Options

How metadata is presented, refreshed, and shared across organizations so users can submit Data Access Requests (DARs).

- **Metadata with Partner Syndication**
  When metadata syndication is enabled, dataset descriptions are synchronized between organizations so that both parties display consistent and up-to-date information. Updates published by a partner automatically propagate to the shared catalog, reducing manual work and ensuring that researchers always see the most current dataset information available.
- **Metadata without Partner Syndication**
  When syndication is not enabled, metadata is published and maintained locally. Each organization updates its own catalog independently, either manually or through scheduled refreshes. This approach works best when partners prefer tighter control over which datasets appear in the shared catalog or when technical constraints prevent automated syncing.

AD Workbench as the Interoperability Layer: The Playbook

Alzheimer's Disease Data Initiative

AD Workbench

Data Hosting, Sharing & Governance Options

After a DAR has been approved, where data resides physically and how researchers access it.

- **Data Hosted at a Central Secure Repository**
  In this model, also referred to as Level 0, a full copy of the dataset is stored on the AD Workbench. Researchers access and analyze the data entirely within a shared workspace, and no data leaves the controlled environment. Partners define and enforce governance rules, while the platform ensures that approved users can access the datasets appropriately.
- **Federated / Distributed Sharing with an Appliance (FDSA)**
  In this approach, the partner keeps full custody of their data and only returns approved query results to researchers. Researchers run remote queries through a standard interface, and the appliance enforces governance policies, audits every request, and returns only approved results, such as aggregated statistics, filtered subsets, or de-identified extracts, rather than the full raw dataset. Because raw records never leave the partner's environment, this model offers strong security and control.
- **Federated / Distributed Sharing without an Appliance**
  This model connects organizations directly without a central governance appliance. After a DAR is approved and any required output review is completed, record-level data can be shared according to agreed-upon governance rules. In some cases, delivery is as simple as providing a secure download link. In others, it involves creating or delivering to a secure workspace through APIs so that data is never downloaded directly to the researcher's local environment. The two organizations jointly handle compliance responsibilities and establish their own policies for auditing, approval, and monitoring.

Both federated/distributed models (with or without an appliance) can accommodate Level 1 or Level 2 data sharing.

- Level 1 -	- Level 2 -
The data contributor hosts the dataset and allows it to be transferred remotely via FDSA and analyzed on AD Workbench.	The data contributor hosts the dataset, doesn't allow it to leave their storage, but processes remote data queries and sends results to users

AD Workbench as the Interoperability Layer: The Playbook

Alzheimer's Disease Data Initiative

AD Workbench

Guidelines

- **Guidelines for Data Providers**
  Data providers should start by clearly identifying their chosen access model and communicating it to AD Workbench so the correct integration path can be set up. When metadata is not openly shared, providers need to create a syndication endpoint that allows the system to retrieve metadata in near real time without storing it locally. In addition, providers must coordinate firewall rules and IP allow listing with the infrastructure requirements to ensure that systems can communicate securely and reliably. Post data access approval, based on the data user agreements and compliance data delivery is set up between systems on trusted reach environments.

- **Guidelines for Data Users (Researchers)**
  Researchers should begin by reviewing any partner-specific access policies included in the dataset's metadata, so they understand the conditions for access. All DAR submissions should be completed through the AD Workbench user interface, and researchers must attach ethics approvals or other required documents when the partner requests them. After submitting the request, researchers will receive a notification either from the AD Workbench system or directly from the partner system with the necessary access requirements or download links. Once access has been granted, researchers are responsible for using the secure download mechanism or working inside the designated data environment exactly as instructed.

Common Challenges and Resolutions

- **Partners use different metadata schemas**
  This makes it difficult to present information in a consistent way across the platform. This can be resolved by creating a metadata transformation layer that maps each partner's structure into a shared schema.

- **Data access is governed manually within the partner organization, instead of via DARs**
  In these cases, implementing a full DAR orchestration workflow through notifications helps streamline the process. Automated reviewer reminders, and structured approval steps ensure that requests move forward without relying on ad-hoc communication.

- **Network and security restrictions**
  These can also create delays, especially when firewalls block traffic between systems. This can be addressed by establishing intra network support deployment, secure VPN tunnels or by coordinating a shared IP allowlisting document so both organizations know exactly which addresses should be permitted.

- **Inconsistent versioning across endpoints or metadata feeds**
  These can cause unexpected breaks in integration. Maintaining clear changelogs and enforcing backward-compatible semantic versioning helps ensure that updates do not disrupt existing workflows and that both systems remain aligned over time.

AD Workbench as the Interoperability Layer: The Playbook

Alzheimer's Disease Data Initiative

AD Workbench

Governance and Support

Role	Responsibility
Interoperability Steering group	Establishes standards, reviews integration plans, resolves partner clarifications.
Onboarding & Development Integration Support	Helps partners expose metadata, configure API endpoints, test workflows.
Data Access Governance Lead	Ensures all approvals comply with institutional, ethical, and regional regulations.
Compliance Committee	Manages compliance with Data Compliance Agreement approvals, consent tracking, encryption, and access audits.
Partner Success Manager	Liaison between ADWB and each partner, ensuring satisfaction and troubleshooting.

Contact Us

If you have comments or questions, please contact us at: https://www.alzheimersdata.org/contact-us.

Join our global community as we fundamentally transform Alzheimer's disease and related dementias research. Follow us on LinkedIn and visit AlzheimersData.org to learn more and sign up for AD Workbench today using this QR code.