WHITEPAPER

Mayo Clinic Platform **Keeps Data Behind Glass***

MAYO CLINIC PLATFORM

Mayo Clinic Platform is the chief architect of this new **model for digital health.**

Introduction

In the wake of COVID-19, global markets delivered a mandate to critical infrastructure providers: implement adaptive digital capabilities or suffer repeat consequences during the next crisis.

In response, leaders in government, academia, and industry reaffirmed their commitment to transforming health care.

Yet even elite institutions face an uphill climb in their journeys to reimagine digital solutions. To better serve patients and meet policy goals, these institutions must address several challenges:

- Access to quality data at scale
- Emerging regulations for intellectual property
- Artificial intelligence (AI)
- Patient privacy
- Supply chain risks

Pipeline data businesses cannot solve these challenges holistically. Health data brokers and point solution providers, as examples, shoulder heavy regulatory burdens. They also continue to be challenged to balance quality control at the point of sale, and they often lack diversity in their offerings.

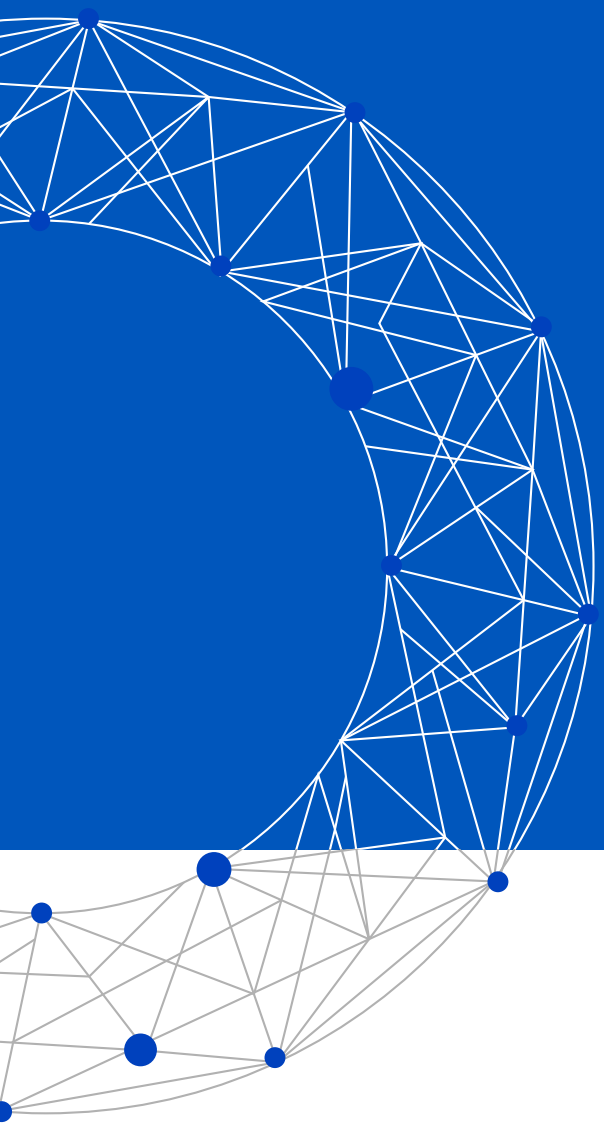
These complex and evolving issues require a new playbook for health care — one rooted in platform thinking.

A robust platform model allows data quality to persist throughout the lifecycle. It allows us to meet regulatory expectations. And most importantly, platforms help us strengthen and maintain patient trust.

Mayo Clinic Platform is the chief architect of this new model for digital health.

Mayo Clinic Platform enables new knowledge, new solutions, and new technologies that improve patients' lives. We partner with providers, pharmaceutical companies, medical device companies, health tech startups, and payers to drive innovation in diagnosis, treatment, and operational improvement.

Mayo Clinic Platform_Connect



To make all of this happen, Mayo Clinic Platform and select partners formed Mayo Clinic Platform_Connect, also known more simply as Connect.

Connect is a distributed data network in which partners contribute their unique data. All partner data conforms to an agreed-upon standard for shared collaboration, but each organization maintains strict control over their own data within the confines of their organizational IT infrastructure and cybersecurity boundaries. These characteristics set Connect apart as a federated network. We call each contributing network partner a data node partner (DNP).

In turn, Mayo Clinic Platform customers view and analyze data in a federated manner across the network when they use the data to develop, train, and validate algorithms.

All Connect partners and customers operate within Mayo Clinic Platform's Data Behind Glass* model. This model relies upon a unique collaborative design philosophy with technical and administrative controls that ensure privacy and confidentiality.

While network controls vary from partner to partner, two overarching principles ensure consistency and promote trust:

1. **Data de-identification:** Mayo Clinic Platform customers cannot see or interact with identifiable data and cannot export, co-mingle, or attempt to re-identify individual de-identified records.

   Depending on the data owner's jurisdiction, Connect uses a variety of techniques to accomplish de-identification or its equivalent.

2. **Secure, federated architecture:** Data and intellectual property remain under the control of each respective Connect partner or model developer and are only viewed or used as authorized.

More about data de-identification

Mayo Clinic Platform assesses each partner's data for quality, completeness, and unique value. To enable federated learning, each partner adheres to a consistent data standard applied across the network.

Within a partner's federated environment (see Figure. 1), experts certify the data as de-identified using industry-accepted statistical methods in alignment with governing privacy laws and regulations.[1] They use techniques such as hashing and uniform date-shifting for de-identification while allowing data to retain its relevance and value for Mayo Clinic Platform customers.

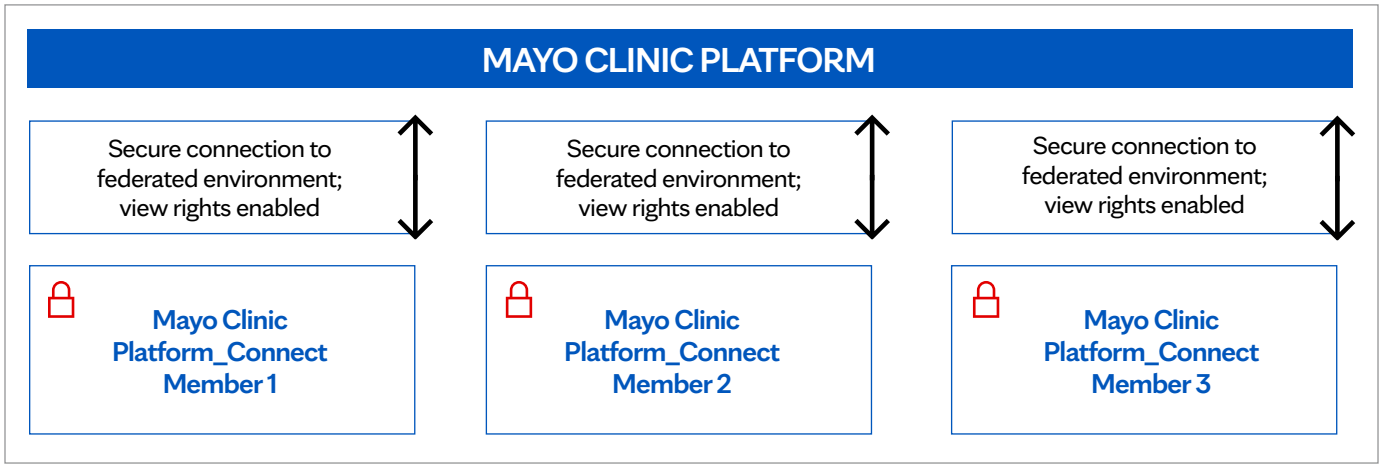
Sometimes Mayo Clinic Platform uses industry-accepted obfuscation techniques, such as tokenization, to mitigate risk while customers view data across nodes on the network. These techniques also help preserve the integrity and value of data. This secure but masked linkage of disparate datasets provides a comprehensive view of factors contributing to patient outcomes.

More about federated architecture

Mayo Clinic Platform follows a secure-by-design development approach.

A Connect partner's current infrastructure is configured to operate as a data node within the network. A node represents a database over which each partner retains local control and administration rights, including security. Connect partners continuously monitor their respective nodes, while Mayo Clinic Platform provides oversight and governance of the entire network.

Figure. 1

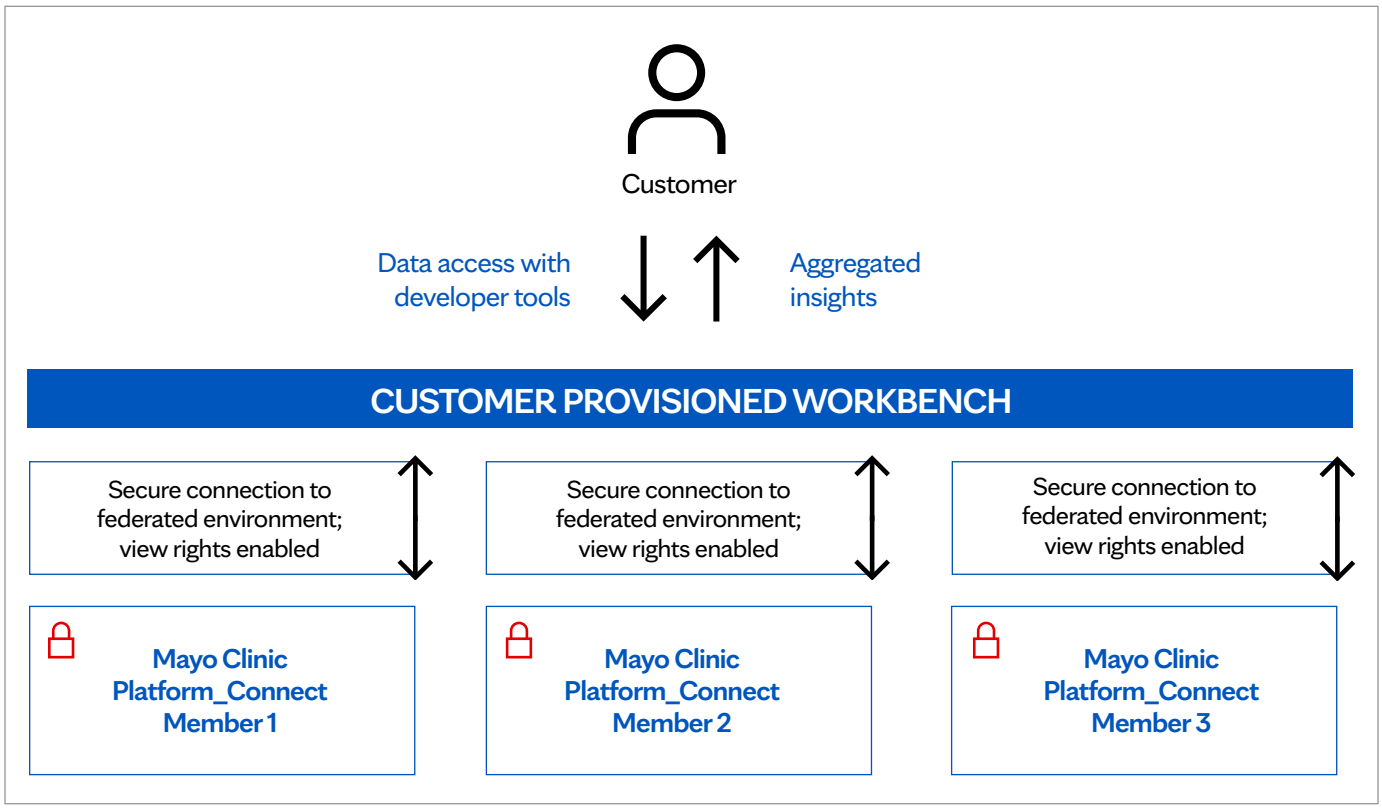


Analytics, development, and training

Mayo Clinic Platform customers use a combination of embedded developer tools, as well as their proprietary and open-source code, to analyze, develop, and train algorithms on Mayo Clinic Platform-approved data cohorts. (See Figure 2.) Customers may view individual record-level de-identified data but removal is prohibited. Further controls include, but are not limited to these:

- Reviewing and whitelisting customer code repositories prior to use.
- Implementing strict identity and access management controls for all Mayo Clinic Platform users.
- Imposing prohibition on data imports and exports from customer provisioned environments.
- Permitting exports of aggregated results through a Mayo Clinic Platform-controlled reporting format. All exports must meet Mayo Clinic Platform's aggregated data threshold prior to approval.[2]
- Contractually prohibiting customers from co-mingling Mayo Clinic Platform data with any other data, regardless of environment.

Figure. 2

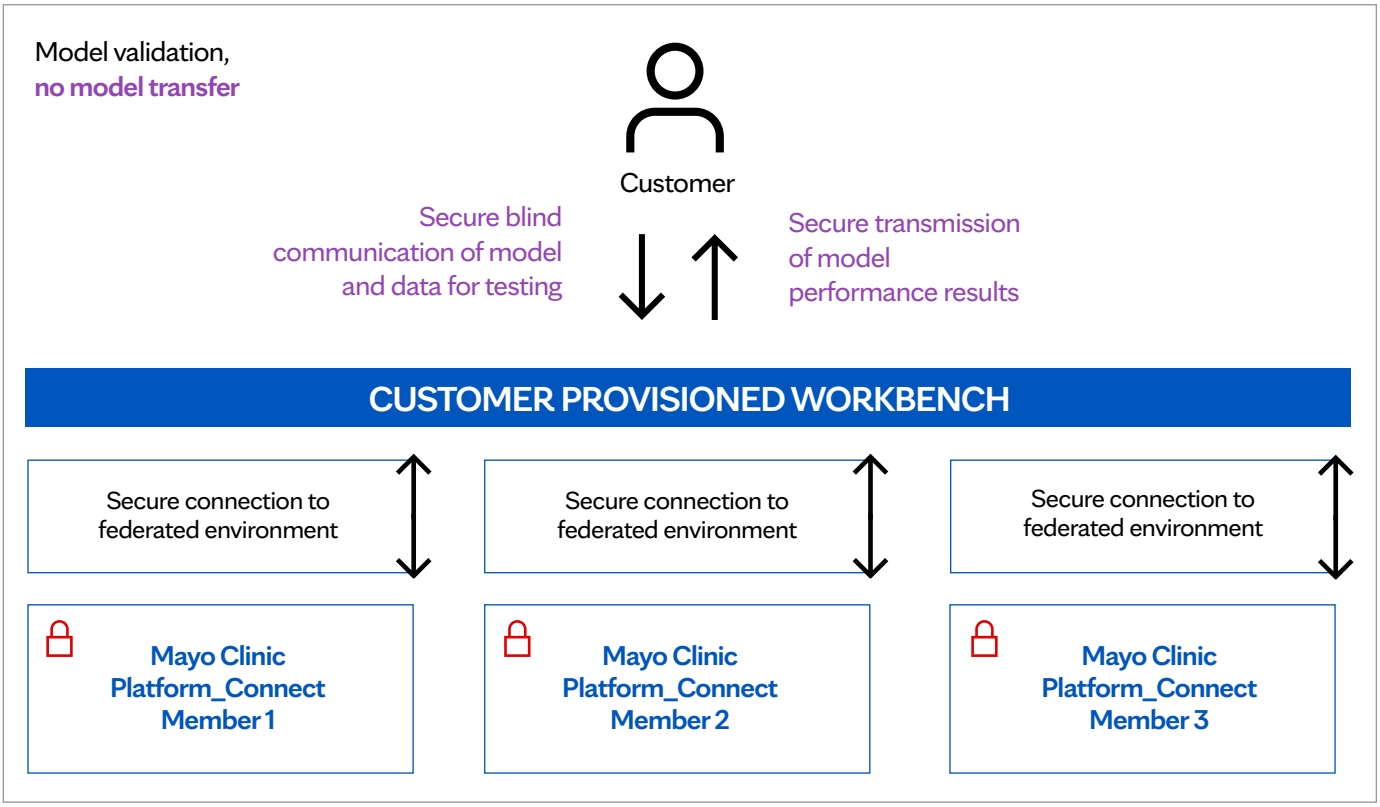


Model validation

In addition to developing and training models, customers are also able to validate their performance. During validation, data and models remain with their respective owners.

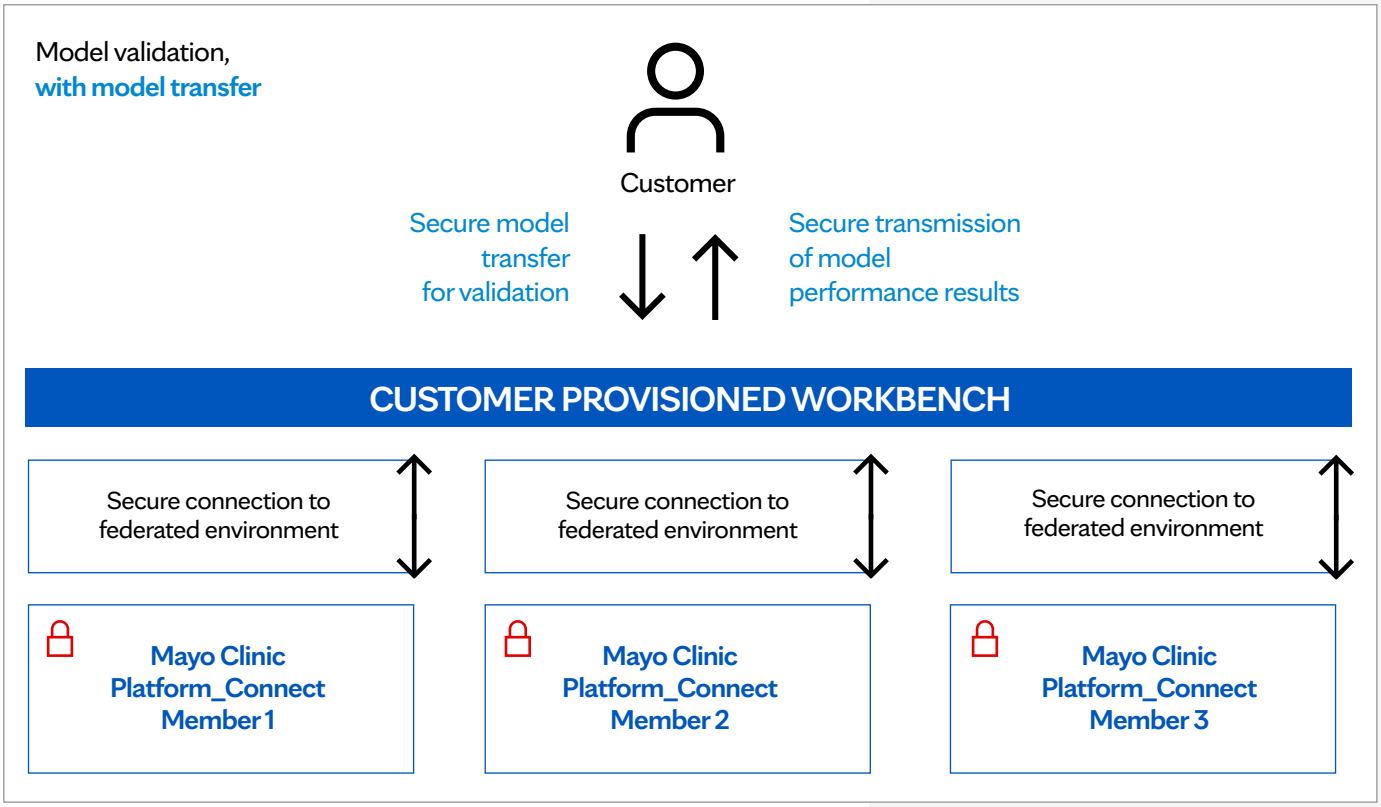
Using unique cryptographic methods, Connect partners and model developers communicate about subsets of data and models via cloud-enabled, federated tools within their respective nodes. Complete copies of models or data are never exchanged, and neither model developers nor Connect partners can view the models or data at any time. In practical effect, this communication between data nodes is blind and secure. (See Figure 3.1.)

Figure. 3.1



In limited cases, a model developer may agree to securely transmit their model to Mayo Clinic Platform for validation testing. The model is never visible to Mayo Clinic Platform, as it remains encrypted while in Mayo Clinic Platform's possession. In all validation use cases, a report detailing model performance is securely transmitted back to the customer. Mayo Clinic Platform securely disposes of any models in its possession once testing is complete. (See Figure 3.2.)

Figure. 3.2



Data Behind Glass* — ready today, adaptable for tomorrow

International regulators continue to increase their focus on the use of machine learning and AI. New and proposed rules signal increased accountability for patient safety and efficacy, as well as the protection of patients' most sensitive information.

In the United States, new applications of well-established health care privacy rules must be considered for novel technologies. And globally, a rapidly growing number of security and privacy rules represent an evolving patchwork of regulations in major economies for innovators to navigate. These include the following:

- General Data Protection Regulation (GDPR) in the European Union,
- Lei Geral de Proteção e Dados (LGPD) in Brazil; and
- China's rapidly growing number of security and privacy rules.

Mayo Clinic Platform's Data Behind Glass* model is adaptable by design, providing global collaborators visibility to the data they need today while preparing for future regulatory developments.

By de-identifying, securing, and federating data, Mayo Clinic Platform democratizes its use without compromising patients' ever-increasing data rights, international transfer rules, processing transparency, or heightened incident response obligations.

A mission to transform health care and improve patients' lives cannot be achieved without patient trust. Mayo Clinic Platform's values and unwavering focus on patients, including respect for their most sensitive information, form the foundation for its Data Behind Glass* model. As such, patients are Mayo Clinic Platform's most important partners.

*Trademark pending

[1] Currently Mayo Clinic Platform applies de-identification requirements outlined within Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164.514(b). Mayo Clinic Platform will align to network partners' de-identification, anonymization, or obfuscation requirements based on their respective jurisdictions. All Mayo Clinic Platform network partners follow a robust quality assurance process to ensure appropriate permissions are obtained to process data for de-identification purposes.

[2] This threshold is reviewed by Mayo Clinic Platform's de-identification experts at regular intervals and Mayo Clinic Platform reviews all exports to ensure compliance with this policy.

MC####-01rev0423

MAYO CLINIC PLATFORM