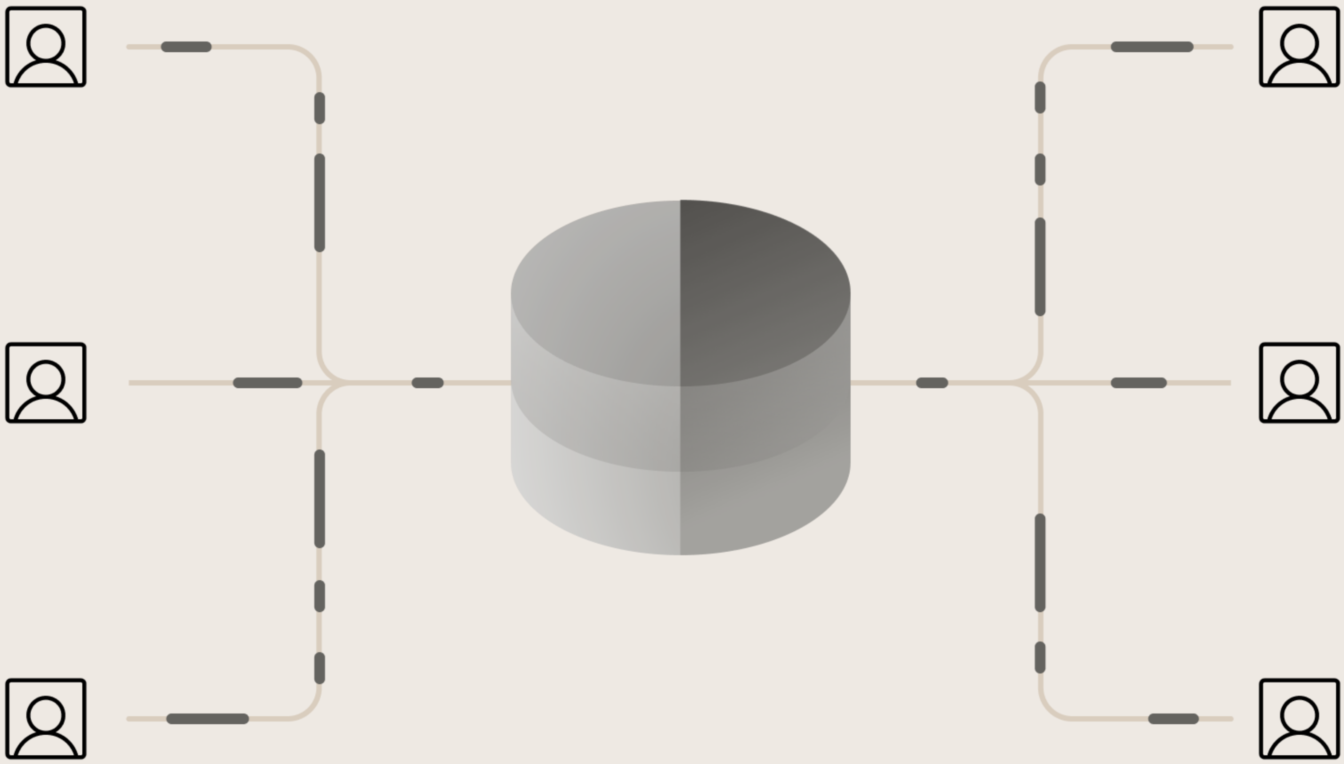
IMMUTA

De-Risk Your Data Sharing: Confidently Drive Business Value Through Collaboration



Contents

Introduction

Data sharing is essential for any growth-oriented business, helping to maintain a competitive edge and deliver business value. By allowing teams to deploy data products, collaborate with internal and external partners, and monetize insights, data sharing drives business outcomes. So why are so few organizations actually sharing data at scale? What makes it so hard?

If you're struggling with data sharing, you're not alone. Despite its numerous advantages, many organizations struggle with a minefield of **data security**, **compliance and regulations**, and a lack of a data-confident culture. **One recent survey** found that 33% of data professionals say their biggest security challenge is a lack of visibility into data sharing and usage. And, a recent **IDC InfoBrief** found that security is the most significant challenge impacting respondents' ability to share data with their peers.

The major hurdles to achieving a secure and scalable data sharing culture are:

Misplaced Focus

Everyone wants to get to the point where data flows freely, driving monetization and increasing business productivity. But an integral step precludes external collaboration: successful internal data sharing.

Fear

Fear of exposing or misusing data is warranted. Whether uncertain about the security of their data sharing framework, wary of regulatory restrictions, or scared that they may accidentally expose sensitive data, even the most data-driven teams approach data sharing with apprehension.

Luckily, neither of these challenges is insurmountable. With the right support, **secure data sharing** can go from out-of-reach to unlocking business value in no time.

De-risking your data sharing practices is both a technological and cultural process. On the technical front, discovering and tagging sensitive data in your ecosystem provides a full view of what data you have and where it lives. Applying dynamic **attribute-based** and **purpose-based access controls** ensure that this data is governed compliantly, regardless of where it travels. Add consistent **data monitoring**, and your team will maintain a watchful eye over all data sharing within your ecosystem.

These technical changes, in turn, inspire a more responsible data sharing culture. With the right controls in place, your team can confidently share and derive value from data without the specter of risk or misuse hanging over their heads.

When done correctly, data sharing breaks down silos, drives efficiency, and aligns data insights with business outcomes. By reframing your approach to internal and external data sharing, and investing in tools that make it secure and efficient, you will be better positioned to drive revenue, reach business goals, and outperform your competition.

A collaborative culture unlocks a number of valuable use cases in any industry. Healthcare institutions are able to securely track and mitigate disease transmission, financial services organizations can collaborate to detect and prevent fraud, and pharmaceutical companies are able to lead research-informed clinical trials – all without the fear of risking data's security or privacy.

Reframing data sharing – from a risk-prone practice to a rewarding one – is possible through the implementation of a capable **data security platform** with effective **data discovery and classification**, **data access controls**, and consistent activity monitoring and auditing. In this bundle, we've included key resources to help your team de-risk data sharing and drive valuable business insights with increased confidence.

IMMUTA

The Top 5 Barriers to Data Sharing and How to Overcome Them

Technology has made our world increasingly interconnected and interdependent, and as a result, the need to share data to remain competitive is more important than ever. Yet, despite the competitive advantages associated with **data sharing**, many organizations still treat it strictly as a data function instead of a business priority.

According to Gartner's report Data Sharing Is a Business Necessity to Accelerate Digital Business, "Organizations that promote data sharing will outperform their peers on most business value metrics." Promoting data sharing is just one part of the equation. Implementing an effective data sharing strategy is the other — arguably more challenging — part.

Gartner interviewed nearly 300 Chief Data Officers (CDOs) and identified the top five challenges associated with internal and external data sharing. Here, learn what they are and how to overcome them.

A Data Sharing Primer

Before we jump into the top barriers to data sharing, it's important to understand the two types of data sharing — and why organizations in every industry from government to commercial transportation rely on both.

Internal Data Sharing

Sharing data amongst stakeholders in the same organization may seem obvious — after all, teams within a single enterprise are generally working towards the same goals. But, in reality, sharing across lines of business (LOBs) can be quite difficult, risky, and even avoided by many teams.

For instance, in large enterprises like this global bank, sharing data across LOBs can create conflicts of interest and violate compliance regulations if done incorrectly. While data may easily be shared too broadly with unauthorized users in these cases, some teams run the opposite risk by avoiding data sharing altogether. This leads to siloed data use, which is inefficient and risky in its own right, as it is often associated with unmanageable data copies.

When done correctly, internal data sharing can help ensure efficient collaboration and development of insights that can drive decision making.

External Data Sharing

Sharing data with third parties or utilizing licensed data is a boon for business: According to Gartner's report, within the next two years 85% of data sharing strategies that include external data sources will drive revenue generating digital business outcomes.

For organizations like a health data company, which relies on external researchers and data scientists to derive insights about critical public health and policy issues using sensitive data, external data sharing is not optional — it is a necessity. External data sharing can bring essential resources into the data analysis process and accelerate speed to insights, but organizations must ensure that they account for geography-based data use regulations and have oversight into how data is being used by data consumers outside of their domain.

The Top 5 Data Sharing Challenges

According to CDOs, these are the top five challenges to effective data sharing, both internal and external.

01 Data Management

Efficient **cloud data management** is a central component of successful data initiatives. By creating standardized, centralized processes around ingesting, classifying, storing, organizing, and maintaining data, organizations are able to ensure that any data they collect and create is accessible, and that it's being used appropriately.

Without a strong data management strategy and framework, it's easy to lose sight of how data is being used and shared, particularly internally. When teams do not know where or how to find data, they are more likely to create data copies that elude governance teams. In turn, this introduces risk of inadequate **data access contro**l policies and unauthorized access.

Weak data management processes prevent data engineering and operations teams from applying effective data access controls and limit the ability to oversee data sharing and use throughout an organization. Modern data management strategies and frameworks should prioritize **data security** and access control as critical factors in utilizing data to its fullest potential while maintaining its privacy and security.

02 Perceived Regulatory Prohibitions

As data **compliance laws and regulations** become more ubiquitous, CDOs see data sharing as increasingly challenging. This is particularly pronounced for external data sharing. Many regulations require a high degree of transparency as to how exactly data is being used; explicit opt-in from data subjects regarding data collection and usage; and comprehensive **data audit trails** to prove organizations are in compliance with all applicable laws and regulations. These strict requirements can become nonstarters for data sharing, or at the very least limit data sharing initiatives.

One of the most complicated facets of compliant data sharing is how to translate legal jargon into policy. This is compounded by the need for data use agreements between organizations when data is shared externally. Without the right tools and processes in place, approval workflows between legal/compliance teams, data engineering/operations teams, and any third parties can be slow and disjointed.

Perhaps the most straightforward way to bypass this barrier is with a combination of **legal automation** and human inspection, which vastly reduces the time needed for approval processes. Tools that simplify the **data policy authoring** process by offering plain language and as-code options make it easier for technical and non-technical users alike to easily understand policies.

03 Risk Assessment of Security

Once you have data privacy and security measures in place, how do you know they're working as intended? Simply applying **data de-identification** techniques does not guarantee that your data is protected. **Risk-based assessments of anonymization approaches** are the best place to start — but many organizations lack the resources to perform such assessments, especially as the number of data sources grows.

Understanding your organization's level of data risk can be complicated, particularly if no clear path toward closing gaps exists. For this reason, CDOs deemed data security risk assessments a top barrier for sharing data, particularly externally. While developing an understanding of risks to data privacy and security is a critical starting point, the ability to automate **dynamic data masking** and **privacy enhancing technologies** (PETs) consistently across all cloud data platforms can streamline anonymization and overcome any gaps in data security so data can be securely shared internally and externally.

04 Insufficient Tools and Technology

We've mentioned how technological resources enable data engineering and operations teams to resolve some of the top barriers to data sharing. CDOs recognize the impact of these resources as well, and cited insufficient tools and technology as a primary data sharing challenge.

Often, technology is regarded as simplifying data-related processes, not increasing complexity. But, many different cloud data providers are now available, each offering a different set of data access controls. As data teams continue adopting multiple cloud data platforms at an accelerated pace, this disparate patchwork of capabilities often doesn't scale consistently across diverse cloud data platforms. The result is overly restrictive data policies that may inhibit data sharing altogether, or overly broad policies that can cause sensitive data to slip through the cracks, leading to a data breach or leak.

Overcoming this barrier requires a centralized data security solution that works across all platforms, decouples policy from compute platforms, and automates otherwise-complicated processes, such as dynamic policy enforcement and **data monitoring**.

05 Fear

The final, and perhaps most pervasive, barrier to data sharing is stakeholder resistance based on fear — which CDOs chose as a top challenge for both internal and external data sharing initiatives.

Just as some organizations are hesitant to migrate to the cloud because it is perceived as less secure than on-prem infrastructures, risk aversion is also a barrier to data sharing. The fear of changing ingrained processes or allowing third parties to access data for which the organization is liable may make key stakeholders, particularly in high level positions, uncomfortable. In this scenario, the risk of downstream data misuse seems to outweigh the potential benefits of data sharing.

Gartner's report discusses how data sharing is often considered a data function instead of a business priority, and how the traditional "don't share data" approach ultimately leads to data hoarding and unnecessary limitations on data-driven outcomes. To unlock data's potential, the report suggests, organizations should flip the "don't share data" mindset to a "must share data unless" approach. The report outlines a model that encourages data sharing so long as it satisfies regulatory requirements and data protection standards. Defined processes; clear task ownership; constant communication; and trustworthy, automated tools and technology can also contribute to overcoming stakeholder resistance and accomplishing more with data sharing.

Conclusion

Analysts anticipate that data sharing and collaboration will become increasingly important to organizations' success and ability to compete in the next two years and beyond. And, while 70% of respondents in a Harvard Business Review survey admitted to being "not very effective at data sharing," solutions to the top five barriers associated with data sharing are at your fingertips.

By prioritizing data sharing and management as business necessities, reframing your organization's approach to sharing data both internally and externally, and investing in tools and technology that enable secure, efficient data sharing, you will be better positioned to drive revenue and reach business goals than competitors.

IMMUTA

Enforce Compliance & Audit Reports for Data Sharing in Snowflake

Data use agreements (DUAs) are vital to ensuring individuals' data is used compliantly and transparently. Just as data use agreements help protect data subjects' personal privacy, avoiding misuse of personal data can protect organizations in every sector, from healthcare and financial services to the government, from liability, fines, breaches of trust, and reputational harm.

In defining contractual obligations for how sensitive data will be transferred and used, organizations commit to restricting the use and disclosure of personal data. But translating DUAs into policy can be ambiguous and challenging for data engineering and operations teams.

For Snowflake users, Immuta helps close the gap between DUAs and policy enforcement with Snowflake compliance and audit reports for data use agreements.

Challenges to Secure Data Sharing

Data use agreements are extremely common in the healthcare industry, as requirements of HIPAA's privacy rule. For purposes of example, let's assume two researchers, Ingrid and Harry, are collaborating on a project using Snowflake as their data warehouse. Ingrid is an admin in **`Database_Clinic1`**, while Harry has admin privileges for **`Database_Clinic7`**; **`FLU_Vax`** is a separate database to which they both have access via a specific role called **`Project_FLU_Vax`**. The project requires data from both Clinic 1 and 7, and therefore has reference permissions on both databases.

When Ingrid creates a view in the **`Project_FLU_Vax`** database, Harry can see it, and vice versa. However, this scenario means that Ingrid and Harry are responsible for isolating the data that they think should be included in the project, which could lead to exposure and use of too much or too little data — which could either put the project in violation of HIPAA guidelines or stifle the ability to draw meaningful insights from the data. By tying roles to views, they are setting up a proliferation of roles that can become unmanageable, inefficient, and risky. Ultimately, it is very difficult to prove compliant data access and track down violators to the data use agreements.

Implementing Snowflake Attribute-Based Access Control

To minimize the imminent proliferation of roles in this scenario, you need to implement attribute-based access control, which leverages user and data attributes to drive data access policies. Instead of creating a common role (**`Project_FLU_Vax`**), you assign a relevant and global attribute, **`ClinicID`**, but specify its value relative to the user's main clinic — Ingrid sees records where **`ClinicID=1`** and Harry sees records where **`ClinicID=7`**.

Immuta's native integration with Snowflake allows **Snowflake data** to be easily registered in Immuta and tagged for direct identifiers, indirect identifiers, and other sensitive attributes. Once the data set has been registered, you apply a global policy that filters rows so that **`ClinicID`** matches the value in the column ID. Now, when a query is run in Snowflake, Ingrid will automatically see records where **`ClinicID=1`** and Harry will see records where **`ClinicID=7`**. This is in contrast to Snowflake's object tagged role-based control model that requires management of predefined roles and user mappings.

Implementing Snowflake Attribute-Based Access Control

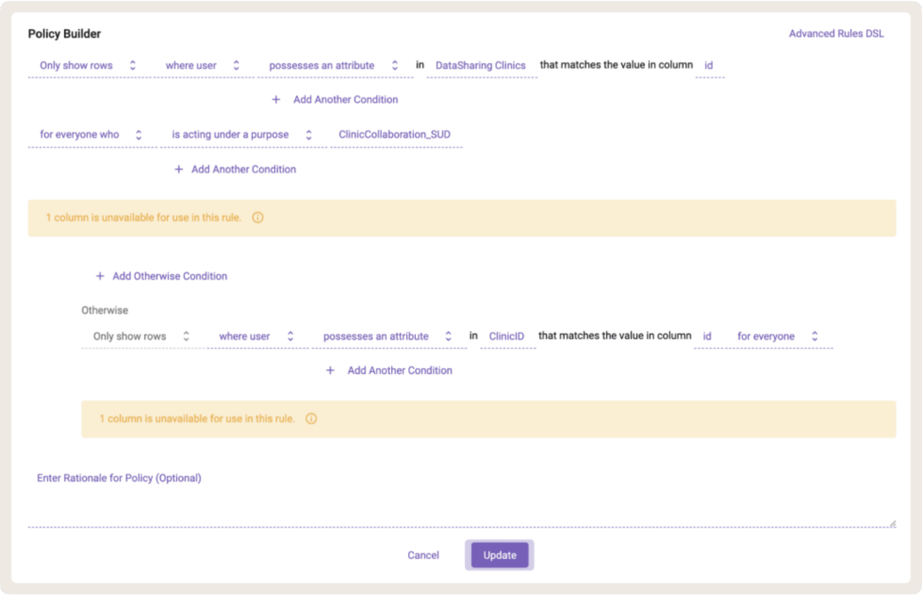
In order to collaborate as efficiently as possible, Ingrid and Harry need to be able to work together on a common set of data — and they need to be sure that data is being accessed and used compliantly, in accordance with the DUA. How is this done if their attributes are such that each sees a different clinic's data?

Immuta enables data teams to work together under a special declared purpose. This can be accomplished by creating a collaborative space used for special data analytics and data sharing initiatives that allows group members to collaborate on specific data sources, bound by a common purpose and defined policies. In Immuta, this capability is called a **Project**. These defined policies allow for access to data for a narrowly defined reason, which is a requirement of major regulations like **HIPAA** and **GDPR**.

When a purpose is assigned to the project, data access is equalized, meaning the data set is limited to the lowest common denominator of accessible data. So, if Ingrid had permission to see PII but Harry did not, both Ingrid and Harry would see records with PII hidden. Data equalization helps prevent unauthorized access in a data sharing scenario.

Declaring a purpose for the data use carves out an exception for data access within that project, and legal and compliance teams are able to incorporate legal language into the purpose statement to help draw a direct line of sight from DUAs or regulations to access control policies. Essentially, this adds a layer of assurance to Snowflake compliance and auditing by creating transparency and accountability at both the front end and back end.

In practice, Ingrid and Harry would be assigned an attribute, DataSharingClinics, and the purpose would be assigned as **`ClinicCollaboration_SUD`**, as shown here:



Policy Builder

Only show rows where user possesses an attribute in DataSharing Clinics that matches the value in column id

for everyone who is acting under a purpose ClinicCollaboration_SUD

1 column is unavailable for use in this rule. ⓘ

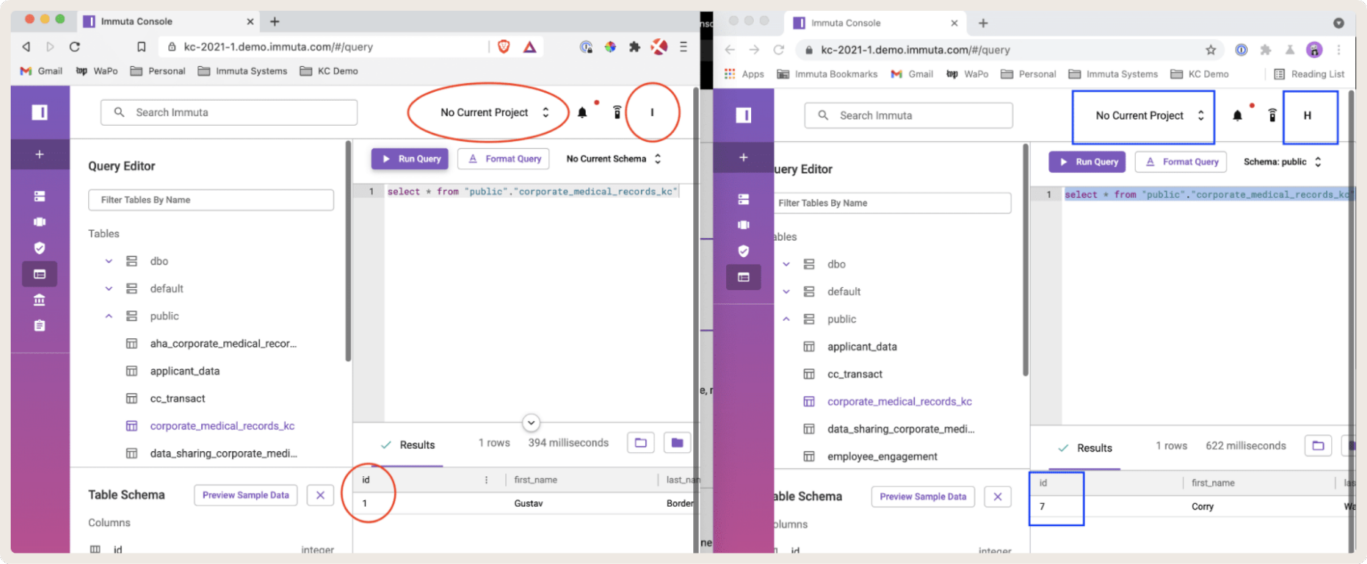
Otherwise

Only show rows where user possesses an attribute in ClinicID that matches the value in column id for everyone

1 column is unavailable for use in this rule. ⓘ

Enter Rationale for Policy (Optional)

Once collaborators have accepted the purpose statement and the project context has been declared, let's look at how the same query will return different results. Here, Ingrid (on the left) and Harry (on the right) are not working under a specific project; therefore, when Ingrid runs a query she only sees records for Clinic 1, while Harry only sees Clinic 7 data.

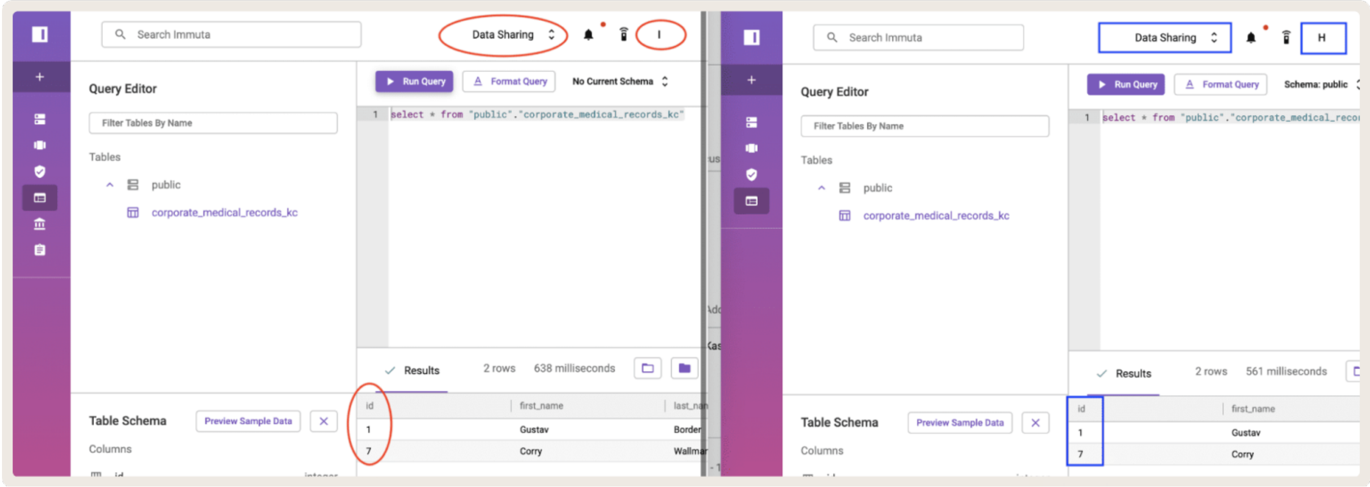


```
select * from "public"."corporate_medical_records_kc"
```

id	first_name	last_na
1	Gustav	Border

id	first_name	las
7	Corry	Wa

When the purpose changes, however, they are both able to see data for Clinics 1 and 7.

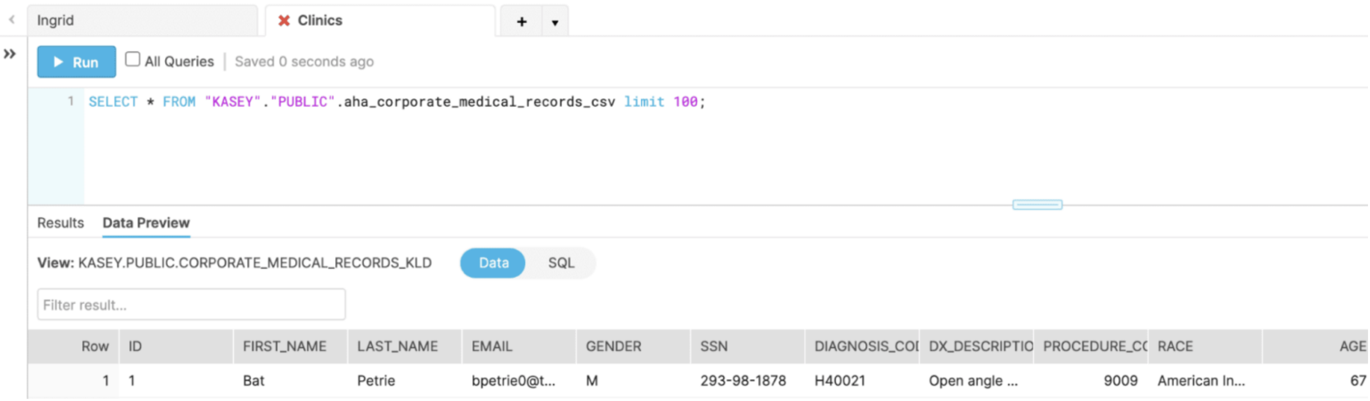


```
select * from "public"."corporate_medical_records_kc"
```

id	first_name	last_na
1	Gustav	Border
7	Corry	Wallmar

id	first_name
1	Gustav
7	Corry

Note that all UI operations can also be done programmatically “as code” in Immuta, and all policies are enforced transparently to Snowflake users without any performance overhead.



```
SELECT * FROM "KASEY"."PUBLIC".aha_corporate_medical_records_csv limit 100;
```

View: KASEY.PUBLIC.CORPORATE_MEDICAL_RECORDS_KLD

Row	ID	FIRST_NAME	LAST_NAME	EMAIL	GENDER	SSN	DIAGNOSIS_COI	DX_DESCRIPTIO	PROCEDURE_CC	RACE	AGE
1	1	Bat	Petrie	bpetrie0@t...	M	293-98-1878	H40021	Open angle ...	9009	American In...	67

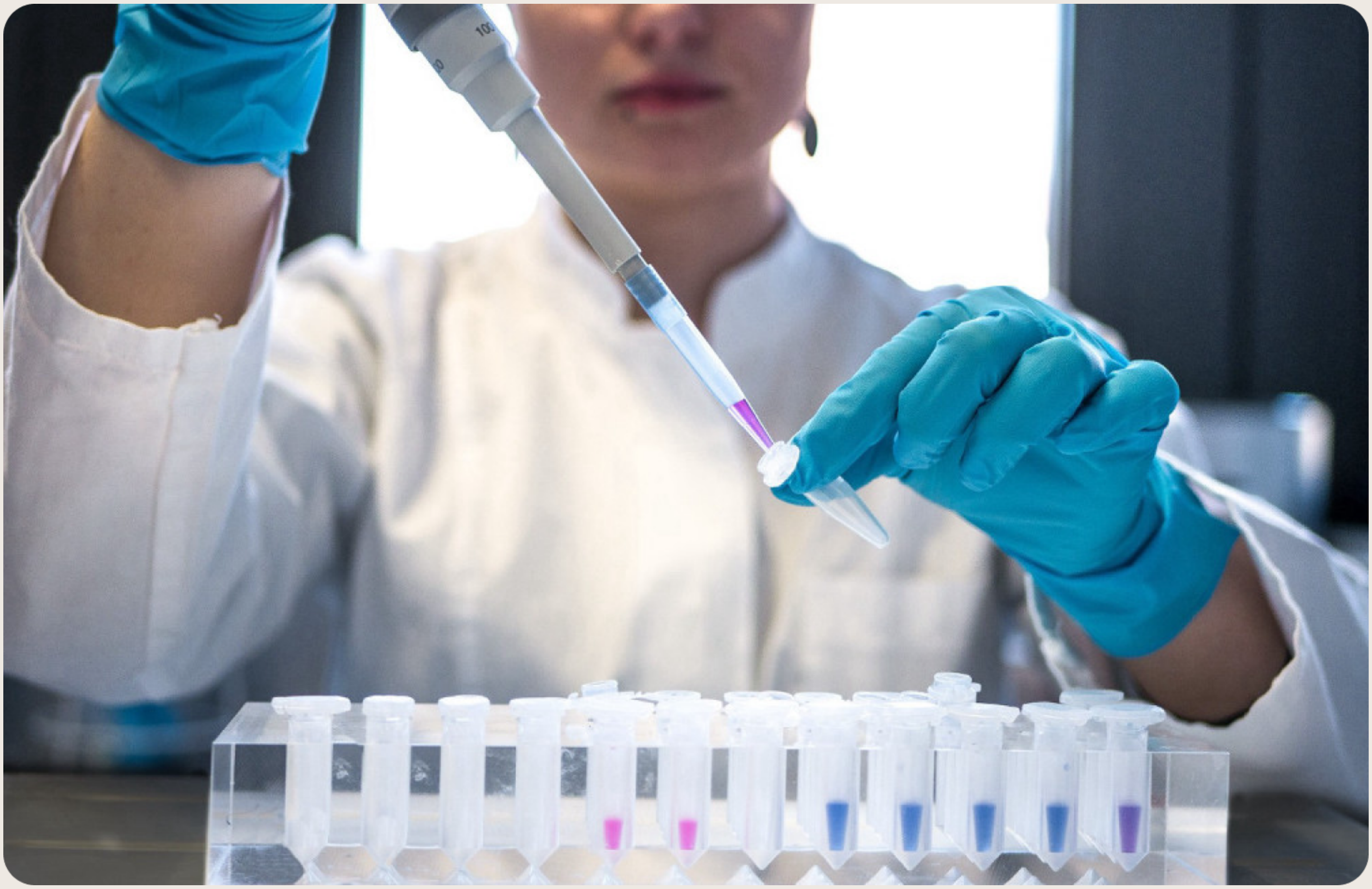
Snowflake Compliance & Auditing for Data Use Agreements

By creating a single global data policy and updating specific attributes, Immuta enables dynamic data sharing to account for all data use agreements and rules. When conducting an audit on DUAs, legal and compliance teams are able to use Immuta’s automated reporting and data audit trails to substantiate that anyone who accesses specific data has an appropriate purpose for doing so, as well as every user subscribed to a data set, who queried data when, and what the specific queries were.

Controlling access at the front end and being able to easily audit it on the back end through Immuta helps organizations in every sector substantiate appropriate data sharing and use. Immuta Projects enables secure data sharing and collaboration, so data teams can efficiently access and use data, and accelerate speed to insights. This also helps mitigate liability for unauthorized access and avoids having to reverse engineer data usage in order to prove compliance with data use agreements, or track down responsible parties for violations, which can require substantial time and overhead.

IMMUTA

Advancing Lifesaving Pharmaceutical Research & Development with Immuta



Introduction

Global pharmaceutical company with a focus on producing innovative therapeutics and delivering top-notch patient care.

With more than 10,000 employees worldwide, this global pharmaceutical company takes a patient-first approach to therapeutic development, focusing on neurology and oncology. In addition to running clinical trials and producing four global brands, its researchers are exploring how to measure biomarkers for Alzheimer's treatments and leverage DNA sequences to fight cancer more effectively.

The organization operates more than 40 subsidiaries, and has R&D, clinical research, and production facilities around the world. To improve patient outcomes, scale cost efficiencies, and fuel drug development and innovation, it needs to efficiently share data across regions and lines of business, comply with industry regulations, and leverage predictive analytics and machine learning on sensitive health data, without compromising patient privacy.

Key Takeaways

Inability to centralize and consistently enforce access controls led to a proliferation of data copies and silos.

Operationalized a BI and analytics platform that enables fast, secure, self-service data access.

Operationalized a BI and analytics platform that enables fast, secure, self-service data access.

Architecture

aws databricks IMMUTA

Challenge

The company's ability to deliver the best service possible to its customers through data was inhibited by three primary issues: an outdated data storage solution, inaccessible and siloed data, and enterprise-wide reliance on sensitive data use.

Siloed data use among business groups and data owners proved to be the most pressing issue. The oncology and neurology teams stored and used distinct types of data, ranging from patient health statistics to medical and X-ray imagery, which required compliance with a long list of **compliance laws and regulations**. To manage this in a global organization, teams established different controls for different projects, leading to complex data silos and access management processes that were manual, time intensive, and risky.

Exacerbating the issue was the compliance team's lack of visibility and authority across the organization. For example, data containing personally identifiable information (PII) and protected health information (PHI) was frequently downloaded to individual workstations and shared via email, and third-party tools were installed without proper vetting for security compliance. These risky practices were not a product of the data team's ignorance, but rather a result of a lack of methodology. To truly scale operations and deliver meaningful solutions while maintaining patients' trust, the organization needed a more streamlined, comprehensive data strategy..

Solution

To start the process of building a new data strategy, the data team worked backwards. Considering general company goals and collaborating with data scientists and analysts across departments, they determined that a cloud-based, big data repository with a global catalog for medical images and textual data would best suit their short- and long-term goals. Working in tandem with a unified data science and BI/analytics platform, their approach needed to be capable of:

- Enabling atomic storage
- Producing a detailed data audit trail
- Querying data at a point in time
- Securely sharing data across multiple business units
- Analyzing, reporting, and dashboarding data use
- Supporting compliance with a range of privacy regulations

The team began its data transformation with **data security** and governance in mind. From the start, they knew that they wanted to leverage a data lake that would act as a repository for structured and unstructured data. Originally, they chose **AWS** as a cost effective, cloud-based storage solution with a wide variety of advanced compute and analytics capabilities. While AWS's capabilities provided a strong foundation, they found that a more diverse data analytics solution was still needed to meet their goals.

To extend support for **SQL**, **R, and Scala** — and gain access to advanced auditing capabilities — the data platform team also adopted **Databricks**. Databricks' **Delta Lake** provides an open format storage solution with widespread support for analytics languages, as well as dashboarding and auditing that is compatible with other leading reporting tools. Databricks' flexibility and advanced reporting capabilities allowed the company to consolidate many of its central data analytics activities into a single, unified platform.

After establishing storage and analytics platforms, the team turned its attention to finding a method for securing them. Immuta ultimately stood out among competitors for its holistic approach to data security, which includes **data discovery**, access control, and **data monitoring**, as well as its ease of integration with AWS and Databricks. With Immuta, they were able to apply **fine-grained access controls** authored in plain language, **dynamic data masking**, and **privacy enhancing technologies** (PETs) without additional overhead, manual attention, or lengthy approval processes. The team also discovered that Immuta's auditing and reporting were more powerful than their initially desired capabilities.

Results

Data lakes offer a high degree of flexibility and analytics power, can become inaccessible and diminish in value if mismanaged. But by integrating Immuta into its tech stack, the company was able to avoid this outcome and instead leverage the full potential of its data lake.

Immuta's automated data discovery and classification, **attribute-based access control**, and data monitoring and auditing empowered the data team to make security and access control a priority, and helped to fully unlock the value of its investments in AWS, Databricks, and the cloud as a whole.

To fill the need for a modern and secure system to control and monitor data use, the organization uses Immuta, AWS, and Databricks as its 100% cloud-based, unified data warehouse and analytics solution. Not only can they leverage Delta Lake as a big data repository, but their unified data science platform allows analysts to use data to develop deep learning models. By securely operationalizing self-service BI and analytics, data users can analyze, report, and dashboard data after ETL and data science experimentation, so they can innovate with data more effectively.

Meanwhile, row-, column-, and cell-level access control and on-demand data auditing of all activity across Immuta, AWS, and Databricks helps ensure that **data sharing** challenges and data silos remain a thing of the past. Now, teams are better able to collaborate with sensitive data, without having to worry about **data localization** laws or industry regulations laws like HIPAA. Having a purpose-built toolset at their fingertips allows data users across all departments to work more quickly and efficiently toward developing the next pharmaceutical breakthrough.

With faster time to data access, more efficient security and compliance efforts, reduced data storage and management costs, and increased collaboration across teams, the organization's data warehouse, security, and analytics transformation empowers improved patient treatments and outcomes.

IMMUTA

Redefining Data Sharing for Financial Services

As business continues to shift to increasingly digital environments, the aggregation and sharing of financial data is predicted to have a staggering impact on the global economic future. According to research by McKinsey, “economies that embrace data sharing for finance could see GDP gains of between 1 and 5 percent by 2030.” Ensuring that this kind of data is safely shareable and accessible to all who can benefit from it is paramount.

The issue with data sharing, however, is how it has come to be defined. We often think of data sharing as taking a snapshot of the information and passing it along to someone else. Whether this be internal, between organizations, or with customers, sharing a static image of data is no longer a functional approach for financial organizations. Data itself is by no means static, so a shared view of it should not be either. Sharing idle data limits its versatility, hindering the range of purposes for which it can be leveraged.

Beyond the evident limitations of sharing idle data, financial services (FS) organizations are witnessing a sea change in how the financial industry and its customers are thinking about data collection and use. A general shift towards more open data sharing is taking root, and the FS industry is beginning to adopt practices that make data both more accessible and widely usable for various applications.

How does this shift uproot our prior understanding of data sharing, and where is it poised to go next?

Why is the Current View of Data Sharing Outdated?

The current industry-wide view of data sharing is, for the most part, hung up on an outdated conceptualization. As hinted at above, much of what is discussed as “data sharing” is used to describe the capturing and conveying of data at a moment in time. A customer might request that an investment firm update them on the current state of their assets, and the firm can respond with a fixed view of their funds at the time of the request.

The problem with this idea is twofold. The first issue is the stagnant nature of the data being “shared” between parties in the scenario. Financial information can be extremely dynamic and fluid, adjusting moment-to-moment based on the ebb and flow of the market. Receiving a static view of this data is like going to see a movie and being handed a single frame of film. You only gain an understanding of how the data is at that exact moment, not how it will continue to develop, which limits the insights you’re able to derive from it.

Individuals have come to expect control over their data as collection practices evolve, and in some jurisdictions this has **even been enshrined into law**. Due to this changing perspective, the traditional view of data sharing can also easily lead to customer discontent. When a bank or fintech service takes that data and offers it back to the consumer under a different label, it can come off as patronizing. No one wants their data to be seemingly relinquished back to them, they want to be able to access it themselves in order to derive their own insights.

Understanding that the current view is limited by these flaws, how should the financial services industry adjust its concept of data sharing to serve modern use cases?

Redefining Data Sharing for Financial Services

Redefining the concept of financial data sharing begins with a simple idea — self-service accessibility. The idea of sharing needs to shift from the current archaic model to an efficient and accessible one. Rather than simply exchanging a snapshot of time-bound data, financial services should look toward a solution that allows stakeholder access at any point in time. This solves the problem of static data sharing by allowing users — internal, external, or customer — to access the most current version of their data assets at will.

Still, this accessible repository of fresh data should not be entirely open to anyone. Rather, access needs to be controlled appropriately so that different users can carry out distinctly different operations. Think about a bank that decides to migrate its financial data to a major cloud provider like **Snowflake** or **Databricks**. Naturally, the bank would want this data to be accessible for analytics stakeholders to analyze and share it as necessary. However, a customer's checking account information should not be accessible to the marketing department or other customers.

This unified data ecosystem needs effective data access controls in place to allow information to be used for different purposes without unnecessary risk. In doing this, the ecosystem could become a resource for safely and efficiently sharing live financial data across internal departments, between businesses, and with customers — as long as they have the right to see it.

The Changing Standard for Financial Data Sharing

The shift away from exchanging fixed data and towards an open mutual resource is already altering the ways in which FS organizations operate. Data ecosystems are evolving, standards are shifting, and new users are requiring new insights. Some examples of this include:

Exchanging Data to Inform Data Ecosystems

Shared data can inform the construction of more self-sufficient FS data ecosystems. Many organizations have traditionally needed to rely on a patchwork of vendors and tools to effectively manage and analyze their data.

When data is regularly and securely made available to the public through a shared resource, this patchwork reliance can effectively be eliminated. Organizations will have the capability to access and assess data on their own.

This self-reliant shift helps banks create a cross-entity view of data, and facilitates tasks like monitoring for fraudulent activity. If George, with a history of bank fraud, tries to open an account at Bank ABC, the data proving his fraudulent activity would be of great importance. If data about George's fraudulent activity were available, showcasing both prior credit history and documented fraud at Bank XYZ, Bank ABC can make an informed decision about his application. This fraud assessment does not require external analysis when Bank ABC can readily access the data themselves.

What's essential, though, is that Bank ABC is not receiving sensitive data that they should not have access to. This is where determining the proper access permissions is key. With the right **masking measures in place**, publicly accessible data could be accessed responsibly and used to make essential decisions in a timely manner. With so much shared information at their disposal, FS organizations can construct a vigorous, self-reliant data ecosystem rather than relying on third party entities.

Combining Data to Create Industry Best Practices

By breaking down silos both inside and outside of company data ecosystems, FS groups can inform a system of best practices that benefit the industry at large. Data can be shared at large in order to provide heightened context for specific pursuits. These guidelines can also inform regulatory adherence and compliance efforts, as well as general industry standards.

These standards are evident through frameworks like the European Central Bank's **Banks' Integrated Reporting Dictionary (BIRD)** and the **Financial Information eXchange (FIX)**.The BIRD database was created with the intention of providing a standardized collection of relevant financial regulations to make regulatory reporting easier for all banks. This shared resource acts as a go-to for up-to-date regulatory financial information, and can be accessed freely as a "public good." Similarly, the FIX is a standardized protocol for the real-time, international electronic exchange of securities information. Acting as an industry principle and informed by the most current data, each of these frameworks demonstrate the value of commonly defined and shared resources for financial services organizations.

Once again, potent and scalable access control measures are required in order to maintain the integrity of sensitive data in this scenario. By mitigating risk to sensitive data, FS firms can better their industry's best practices while maintaining safety and compliance.

Ensuring Customer Success Through Shared Data

Customer clarity is a crucial factor in any business relationship. This is especially true in the financial realm, where banks' transparency helps increase customers' confidence that institutions are making the right decisions with their money. Beyond this, customers seek assurance that the financial insights they are offered are sound enough to inform personal investment decisions. Delivering on these needs requires balancing data privacy and utility.

Providing customers with access to the same repository of innovative data – while ensuring that this access is properly governed – will be the most effective way to facilitate these user insights. We're already seeing movement towards commonly shared data through the concept of **Open Banking**, an ecosystem taking root in places like the U.K. that allows customers and FS institutions to securely share their financial data in order to gain tailored insights and services from third parties. This kind of model gives customers increased autonomy over their financial pursuits, all while maintaining their privacy.

This form of open, secure sharing allows both FS firms and customers to find increased success and satisfaction. Putting more power over data-informed personal financial decisions in the hands of the customer is much more enticing than simply repackaging customer data and sending it right back in an idle bundle.

Achieving Redefined Financial Data Sharing

Enabling accessible repositories of data that allow access for different stakeholder use cases will elevate FS institutions to a new level of shared success. By employing tools with the capacity to discover, secure, and monitor data, financial services institutions can engage in this form of common resource sharing in a safe and effective manner.

The Immuta Data Security Platform combines these capabilities into a simple functional tool, enabling an array of **financial services and fintech customers** to share data while keeping it protected. With automated **data access controls**, **fine-grained auditing and reporting**, and **dynamic data masking capabilities**, Immuta gives financial institutions the confidence to share data and unlock new opportunities while avoiding putting customers at risk and violating data regulations. Using Immuta, FS customers have seen results such as:

100%

Increased data science productivity

100x

Accelerated data access and optimized marketing spend

$50M

Saved in spend by automating 95% of data access requests

To learn more about protecting and leveraging financial data, read **The Ultimate Guide to Data Security for Financial Services**.

IMMUTA

De-risk your data.

Immuta automates security to de-risk data and quickly deliver new value.

The Immuta Data Security Platform helps organizations granularly and holistically control data access across cloud environments and data platforms, so teams can freely, confidently use data to collaborate, innovate, and succeed.

Based in Boston, Massachusetts, Immuta has been removing risk and accelerating business since 2015, and is trusted by Fortune 500 companies and government agencies around the globe.

Visit immuta.com ⟶