Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 09| 2025

Research Article **Received:** 20-07-2025| **Accepted:** 10-08-2025 | **Published:** 04-09-2025

Privacy-Preserving Risk Analytics Through Data Clean Rooms: An Integrated Platform Engineering and Privacy Technology Framework for Regulated Industries

Sathish Kuppan Pandurangan

Zurich North America, USA

Abstract: Data Clean Rooms represent a transformative solution for organizations navigating the complex crossroads of collaborative analytics and stringent data privacy regulations across the insurance, finance, and healthcare sectors. The controlled surroundings enable multiple parties to perform common analyses on sensitive datasets without exposing raw data to sharing associations, addressing concerns about pressures between logical conditions and non-supervisory compliance. Advanced sequestration-enhancing technologies form the specialized foundation, including Secure Multi-Party Computation protocols that enable parties to concertedly cipher functions over private inputs without revealing individual benefactions, discriminational sequestration mechanisms that give fine guarantees through precisely calibrated noise injection, and allied literacy infrastructures that enable distributed model training without polarizing sensitive information. Modern platform engineering approaches provide the foundational infrastructure orchestration capabilities that enable scalable, secure, and operationally excellent Clean Room deployments across diverse organizational environments. Multi-jurisdictional compliance fabrics accommodate different nonsupervisory conditions across GDPR, CCPA, and HIPAA authorities while enforcing sequestration by design principles throughout system infrastructures. In the fields of healthcare analytics, where population health studies and clinical trial optimisation uphold stringent case sequestration protections, and fiscal services threat analytics, where collaborative fraud discovery and credit threat modelling benefit from cross-institutional pattern recognition, assiduity-specific operations exhibit notable potential. DataOps methodologies integrated with platform engineering practices ensure functional excellence through comprehensive workflow operation, automated infrastructure provisioning, and nonstop confirmation processes that maintain logical dedication despite sequestration, conserving metamorphoses. The integration of sophisticated concurrence operation systems and data subject rights enforcement mechanisms creates coordinated approaches that help address compliance gaps across multiple sharing realities.

Keywords: Data Clean Rooms, Privacy-Enhancing Technologies, Secure Multi-Party Computation, Federated Learning, Regulatory Compliance, Collaborative Analytics.

INTRODUCTION

The combination of strict data sequestration laws and the growing need for cross-organizational analytics has presented a grueling dilemma for businesses in the banking, insurance, and healthcare industries. Companies have to balance rigorously clinging to sequestration laws with gleaning perceptive information from participating databases. Industry cooperation presents itself as an essential solution for lowering compliance costs, through the common regulatory models allowing for up to 30% cost savings through streamlined processes and common resource pooling (Cataligent, 2025). The monetary effect of a dispersed compliance strategy is realized when reviewing the large investments into separate organizational privacy infrastructure creation.

Traditional data sharing methods typically fail to balance both analytical needs and compliance restrictions, calling for new solutions that are able to maintain privacy without compromising analytical integrity. Significant computational costs and accuracy loss issues are associated with direct standard techniques like data masking and tokenisation. Privacy-preserving in federated learning settings exhibit diverse performance metrics, with differential privacy mechanisms having privacy protections against model utility trade-offs (Shalabi, E. *et al.*, 2025). The comparative examination of diverse privacy-preserving strategies demonstrates significant variation in computational complexity and security effectiveness between different implementation contexts.

Data Clean Rooms present themselves as a revolutionary technology that overcomes the essential tradeoff between privacy preservation and analytical value. The regulated environments allow various parties to conduct joint analyses of sensitive data without sharing raw data with any involved organization. Through the establishment of secure computational environments in which information is encrypted and access is strictly controlled, Clean Rooms enable collaboration while ensuring the confidentiality and integrity of personally identifiable information. The success of these implementations depends critically on robust platform engineering foundations that provide scalable infrastructure orchestration, automated

***Corresponding Author:** Sathish Kuppan Pandurangan

DOI- https://doi.org/10.5281/zenodo.17054797

deployment capabilities, and comprehensive operational monitoring across distributed organizational boundaries. Collaboration by industry through standardized Clean Room deployments has potential for substantial cost optimization and better regulatory compliance results (Cataligent, 2025).

New advancements in privacy-preserving analytics illustrate the maturity of federated learning methods and secure multi-party computation protocols. Performance comparisons of several privacy-preserving approaches show diverse results based on various use case demands and security factors (Shalabi, E. *et al.*, 2025). Clean Room technologies evolve to include sophisticated cryptographic methods supporting high-fidelity analytics with mathematical guarantees of privacy, while modern platform engineering practices enable these complex systems to operate reliably at enterprise scale.'

The regulatory environment continues to shift with more focus on collaborative compliance models and shared accountability approaches. Enterprise-wide implementation of standardized privacy-preserving analytics platforms offers the potential for joint cost savings and enhanced operational efficiency. Clean Room deployments across diverse organizations facilitate the creation of integrated risk assessment models with complete individual organizational data sovereignty and regulatory compliance obligations.

TECHNICAL ARCHITECTURE AND CORE COMPONENTS

Privacy-Enhancing Technologies Foundation

The technical underpinnings of Data Clean Rooms depend on advanced combinations of privacy-assuring technologies that support safe collaborative analytics across organizational boundaries. Secure Multi-Party Computation (SMPC) is the computational foundation that supports parties in computing joint functions over private inputs without either party exposing those inputs to the other. Newer SMPC protocols show extensive efficiency gains with enhanced methods that do not require authenticated channels, lowering communication complexity and computational overhead in distributed systems (Vu, D. H. *et al.*, 2020). Cryptographic protocol guarantees that computational outcomes are exchanged while individual data inputs are kept encrypted throughout the process.

Mechanisms for differential privacy offer mathematical assurances regarding privacy preservation by adding carefully selected noise to query responses. The method avoids enemies from deducing particular information about individuals without the loss of statistical utility in aggregate analyses. Noise injection mechanisms are under precise control to ensure analytical correctness while guaranteeing that individual privacy is mathematically assured. Contemporary SMPC protocol implementations enhance security without the need for pre-existing authenticated communication channels, facilitating more versatile deployment environments across various organizational infrastructures (Vu, D. H. *et al.*, 2020).

Federated learning architectures augment these technologies by allowing distributed training of models over many datasets without centralizing sensitive data. Machine learning models are trained locally on individual organizational datasets, with model parameters alone shared and aggregated to form collaborative insights without revealing underlying datasets. Resource allocation techniques in federated learning systems illustrate the essentiality of effective computational resource allocation, with managed virtualized environments needing advanced scheduling methodologies to maximize performance across heterogeneous client hosts (Nikolaidis, F. *et al.*, 2023).

Platform Infrastructure and Orchestration

Data Clean Room implementations require sophisticated platform engineering approaches to manage the complex infrastructure needs of multi-party privacy-preserving computations. Container orchestration platforms like Kubernetes provide the foundational layer for deploying scalable Clean Room environments, enabling dynamic resource allocation and workload isolation across participating organizations . Infrastructure as Code (IaC) practices ensure reproducible deployments while maintaining security compliance across different organizational environments, allowing teams to version-control their Clean Room infrastructure configurations and automate deployment processes with built-in compliance validation.

Service mesh architectures facilitate secure communication between distributed Clean Room components, implementing zero-trust networking principles that complement the cryptographic protections inherent in SMPC protocols. The platform layer abstracts complexity from data

Publisher: SARC Publisher

science teams while ensuring that privacy guarantees are maintained throughout the computational lifecycle. Cloud-native design patterns enable Clean Rooms to scale elastically based on analytical workload demands while maintaining strict data residency and sovereignty requirements across multiple jurisdictions.

Modern platform engineering practices integrate seamlessly with privacy-preserving technologies to create robust, scalable Clean Room deployments. Containerized SMPC workloads benefit from Kubernetes' native resource management capabilities, enabling efficient allocation of computational resources for cryptographic operations while maintaining strict isolation boundaries between participating organizations. Platform automation tools ensure that security configurations and privacy controls are consistently applied across all Clean Room instances, reducing the risk of configuration drift that could compromise privacy guarantees.

Data Segregation and Access Control

Sophisticated data isolation mechanisms guarantee that involved organizational data sets are logically and physically separate in Clean Room settings. Multi-tenant solutions employ rigorous boundary enforcement, avoiding cross-contamination of information while allowing synchronized analytical workflows. Cryptographic controls over access to data ensure that only legitimate computational activities can be executed on particular data sets. Resource management frameworks in virtualized settings become especially important for ensuring isolation guarantees while optimizing for computational efficiency (Nikolaidis, F. *et al.*, 2023).

Role-based access control systems define fine-grained permissions for various analytical operations, with audit trails recording all data interaction for compliance tracking. Control systems go beyond basic read-write privileges to include complex policy enforcement mechanisms that have the capability to restrict certain kinds of analytical operations according to data sensitivity levels. The application of effective SMPC protocols in the absence of authenticated channels opens up new avenues for efficient access control processes that can function effectively in dynamic multi-party scenarios (Vu, D. H. *et al.*, 2020). Innovative federated learning resource allocation frameworks ensure that computation resources are allocated optimally across engaged organizations with uncompromising data segregation requirements sustained throughout the analytical process (Nikolaidis, F. *et al.*, 2023).

Platform-level access control integrates with application-layer privacy controls to create defense-in-depth security architectures. Kubernetes namespace isolation provides additional segregation boundaries, while service mesh policies enforce communication restrictions between different organizational components. Identity and access management systems integrate across organizational boundaries through federated authentication mechanisms, enabling secure access control without requiring centralized identity stores that could create privacy risks.

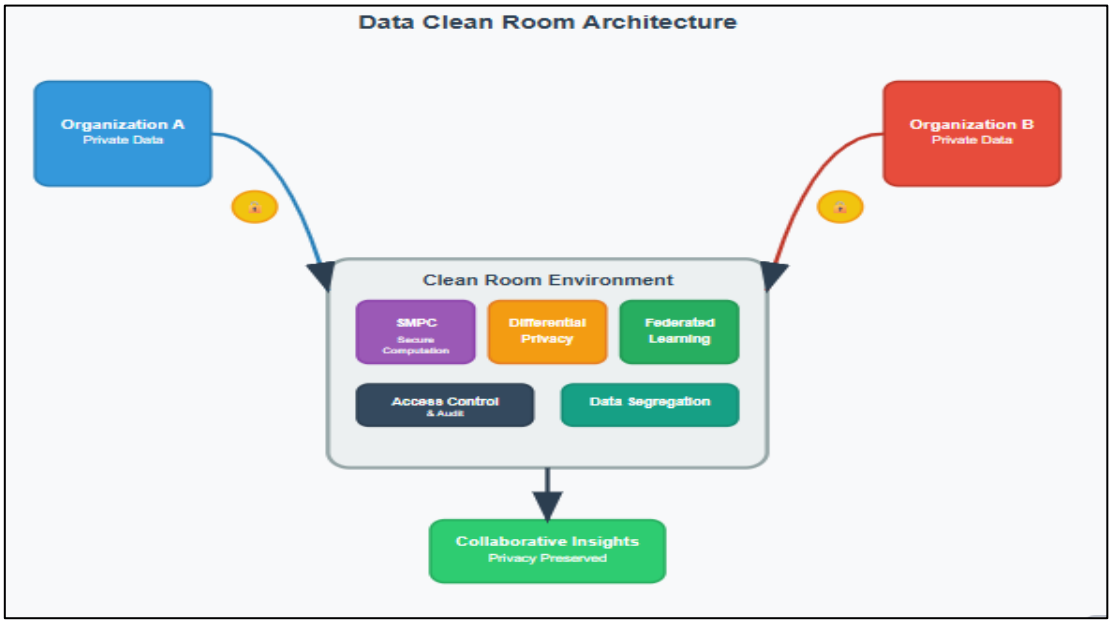

Fig 1. Data Clean Room Technical Architecture (Vu, D. H. *et al.*, 2020; Nikolaidis, F. *et al.*, 2023)

Publisher: SARC Publisher

REGULATORY COMPLIANCE FRAMEWORK

Multi-Jurisdictional Compliance Architecture

Data Clean Rooms need to support varied regulatory needs across geographies and industry sectors using rich architectural designs. The architecture implements compliance controls that simultaneously satisfy the requirements of the California Consumer Privacy Act for Californians, the General Data Protection Regulation for European citizens, and the Health Insurance Portability and Accountability Act for healthcare data. Privacy by design principles under GDPR set basic requirements for data protection measures to be incorporated from the initial phases of system development so that privacy aspects do not remain an afterthought but integral architectural components (Matuszewska, K. 2018).

Privacy by design principles are integrated into system architectures so that data protection measures are not grafted on but organically built into each component. Data minimization procedures restrict the collection and processing of personal data to what is necessary for stated analytical goals, and purpose limitation controls require that data usage be aligned only with pre-established legitimate business purposes. The GDPR model requires privacy by design deployment to be proactive and not reactive, with the requirement that organizations prove conformity through technical and organizational measures that safeguard data subjects during the complete data processing cycle (Matuszewska, K. 2018).

Multi-jurisdictional compliance implementation necessitates advanced technical designs that can address different regulatory demands in multiple legal contexts. In the context of GDPR, privacy by design establishes seven fundamental principles that must be integrated into Clean Room designs, including proactive rather than reactive safeguards, default privacy, and preserving complete functioning in addition to privacy protection (Matuszewska, K. 2018). These principles give rise to technical specifications that affect all Clean Room design and deployment aspects.

Platform engineering approaches enable automated compliance validation through policy-as-code implementations that continuously assess Clean Room deployments against regulatory requirements. Infrastructure automation tools integrate compliance checks into deployment pipelines, ensuring that new Clean Room instances automatically inherit appropriate regulatory controls based on data jurisdiction and industry context. This approach reduces manual compliance overhead while providing auditable evidence of regulatory adherence.

Consent Management and Rights Enforcement

Advanced consent management systems monitor individual privacy choices among multiple participating organizations to ensure analytical processes honor fine-grained consent choices. These systems need to support intricate situations where individuals can hold distinct consent choices with various organizations, necessitating dynamic policy reconciliation processes. Federated learning environments introduce singular privacy and security issues that need thorough survey analysis to comprehend the entire range of privacy-preserving methods and corresponding security implications (Gosselin, R. *et al.*, 2022).

Data subject rights enforcement mechanisms allow the individual to enforce rights to access, rectification, erasure, and portability by all participating organizations at once. The synchronized strategy avoids compliance loopholes through decentralized management of rights by multiple institutions. Privacy and security aspects in federated learning systems involve several dimensions, such as data privacy, model privacy, and communication security, each of which must have specialized technical safeguards and enforcement mechanisms (Gosselin, R. *et al.*, 2022). Higher-level federated learning deployments need to deal with privacy issues at both the level of individual data point privacy as well as aggregate model parameter security without forgoing the distributed compute advantage that federated methods provide to make cross-organization collaboration worth the effort.

Platform-level rights enforcement mechanisms integrate with Clean Room governance systems to provide automated data subject rights fulfillment across organizational boundaries. API-driven architectures enable real-time rights enforcement, allowing individuals to exercise their privacy rights through standardized interfaces that propagate changes across all participating Clean Room instances. Container orchestration platforms facilitate rapid deployment of rights fulfillment workloads, ensuring timely compliance with regulatory requirements for data subject requests.

Publisher: SARC Publisher

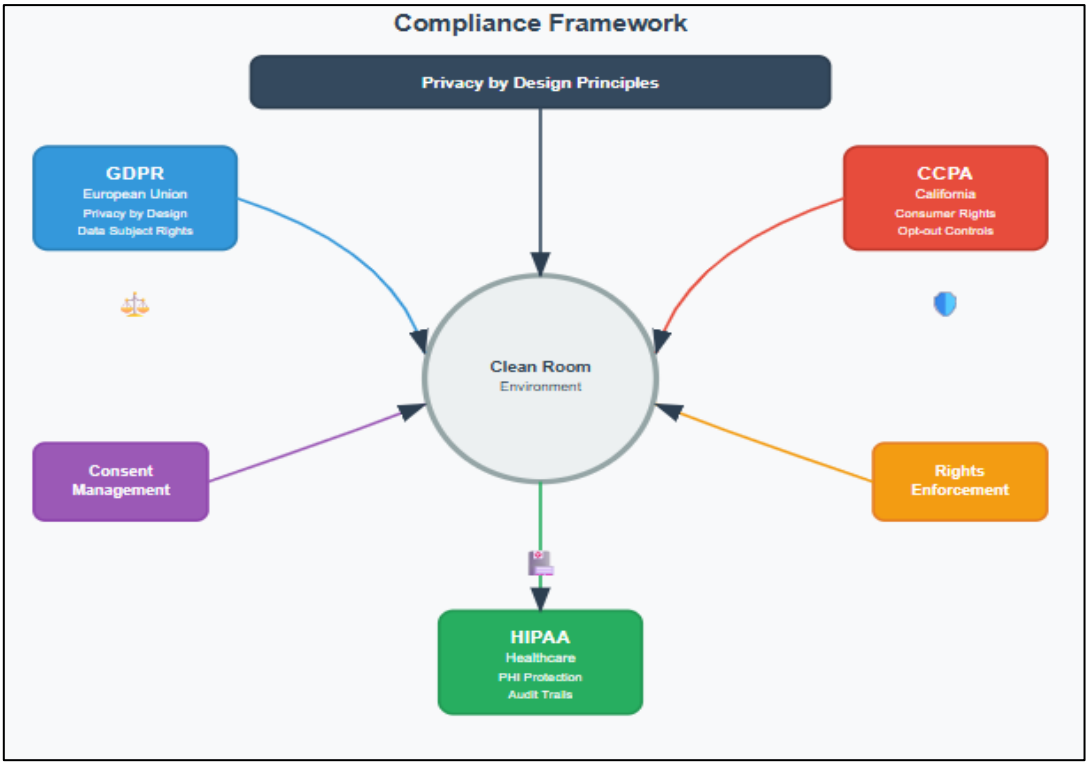

Fig 2. Multi-Jurisdictional Compliance Framework (Matuszewska, K. 2018; Gosselin, R. *et al.*, 2022)

INDUSTRY-SPECIFIC USE CASES AND APPLICATIONS

Financial Services Risk Analytics

Clean Rooms in the financial industry allow for cooperative fraud detection efforts where banks and payment processors can detect complex fraud patterns without having to share customer transaction information. Anti-money laundering investigations have the advantage of cross-institutional pattern detection without violating customer confidentiality and competitive secrecy. Machine learning use cases in assessing financial risk have disruptive potential to improve conventional risk assessment methods, with algorithmic solutions supporting more advanced pattern recognition and forecasting capabilities across a wide variety of financial data sets (Kuna, A. 2025). The application of advanced analytics in banking and other financial institutions opens up possibilities for more detailed risk assessment methodologies that are sensitive to changing market conditions and new patterns of threats.

Credit risk modeling strengthens when several financial institutions can contribute to model training while keeping individual customer profiles out of the public sphere. The collaborative strategy enhances model performance while sharing risk assessment capabilities across the industry. Financial risk analysis by using machine learning methods provides major advances compared to standard statistical techniques, especially in identifying intricate interactions between several risk factors and forecasting likely default situations (Kuna, A. 2025). Algorithmically sophisticated methods allow financial institutions to handle huge amounts of transactional data while finding subtle patterns that may reflect fraudulent behavior or exposure to credit risk, providing more elaborate and accurate risk assessment frameworks.

Platform engineering considerations for financial services Clean Rooms include implementing high-availability architectures that can handle real-time fraud detection workloads while maintaining sub-second response times. Multi-cloud deployment strategies enable financial institutions to meet data sovereignty requirements while leveraging specialized compute resources for different analytical workloads. Automated scaling mechanisms ensure that fraud detection models can process transaction spikes during high-volume periods without compromising accuracy or privacy protections.

Healthcare Analytics and Research

Healthcare applications utilize Clean Rooms for population health research, where several healthcare providers submit patient data for epidemiological studies without compromising patient confidentiality. Pharmaceutical firms can partner with health systems to optimize clinical trials while keeping tight patient privacy

Publisher: SARC Publisher

safeguards in place. Privacy-protecting federated learning methods in medical studies show great promise for multi-institutional data mining collaboration, which can facilitate researchers to build more thorough analytical models while ensuring strict patient confidentiality standards (Haripriya, R. *et al.*, 2025). The allied literacy system enables health institutions to contribute to large-scale studies without infringing on case-position sequestration or violating nonsupervisory compliance norms.

Insurance companies and healthcare providers can develop more accurate threat scoring models by combining claims data with clinical issues, enabling better decoration pricing and care operation strategies without compromising sensitive health information. Cooperative medical data mining through sequestration-conserving allied literacy enables healthcare institutions to share multi-institutional exploration enterprise while maintaining complete control over patient data and ensuring compliance with healthcare sequestration regulations (Haripriya, R. *et al.*, 2025). The allied system opens the door to erecting further flexible prophetic models that take advantage of miscellaneous case populations and clinical data from several different healthcare systems, eventually enhancing the delicacy of opinion and treatment issues while maintaining the obscurity and integrity of sensitive medical data along the course of cooperative exploration.

Healthcare clean room deployments require specialised platform configurations to address big-scale genomic statistics processing and longitudinal affected person record evaluation. Container orchestration enables dynamic allocation of specialized compute resources, including GPU clusters for deep learning workloads and high-memory instances for genomic sequence analysis. Platform automation ensures that healthcare Clean Rooms maintain HIPAA compliance throughout their operational lifecycle while providing researchers with scalable analytical capabilities.

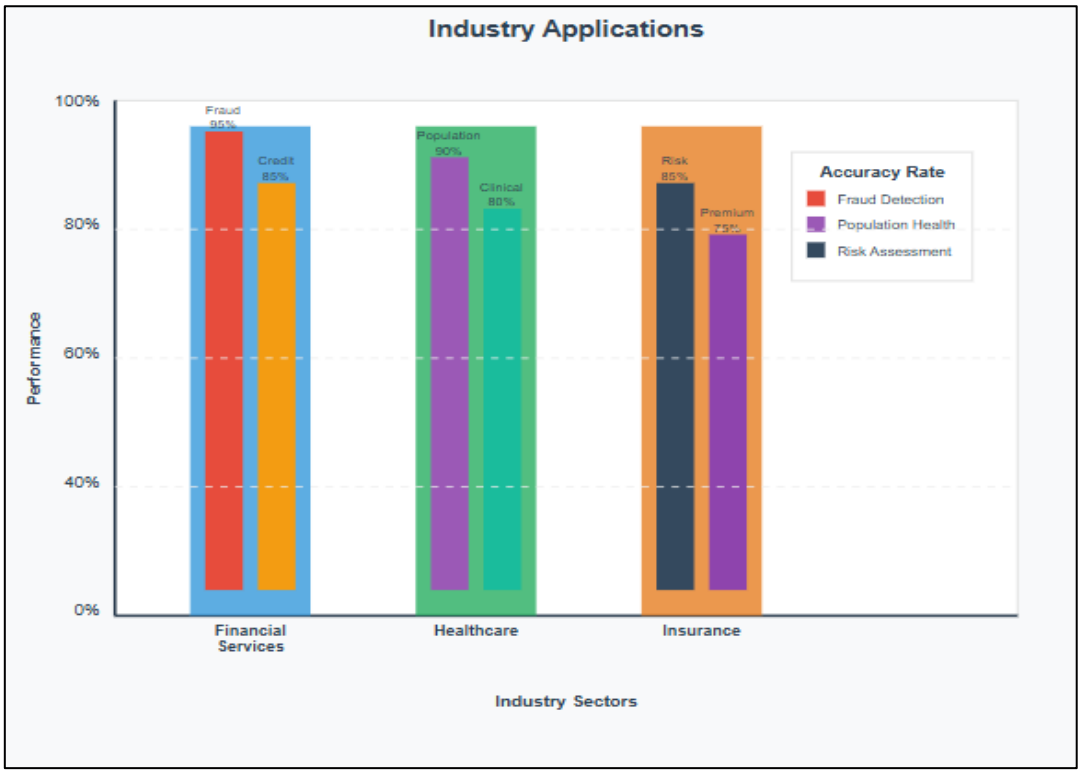

Fig 3. Industry Applications Performance Chart (Kuna, A. 2025; Haripriya, R. *et al.*, 2025)

DATAOPS AND PLATFORM ENGINEERING EXCELLENCE

Workflow Management and Governance

Dataops practices guarantee that clean room logical workflows are auditable, unremarkable, and scalable via give up-to-cease practical fabrics. Interpretation control systems cover updates to data processing channels and logical models, allowing associations to have detailed inspection trails for nonsupervisory purposes. Automated test frameworks ensure that privacy controls continue to be effective as analytical processes change. Contemporary DataOps deployments highlight the urgent need to have strong data governance

Publisher: SARC Publisher

structures that can manage the complexity of collaborative analytics while preserving operational efficiency (Novogroder, I. 2025). The adoption of stylish practices for DataOps allows companies to produce a scalable data structure that can handle adding logical conditions while maintaining harmonious quality and compliance in varied operating environments.

Platform engineering integration transforms DataOps practices through Infrastructure as Code (IaC) implementations that enable version-controlled Clean Room infrastructure management. GitOps workflows provide automated deployment pipelines for privacy-preserving analytical workflows, ensuring that infrastructure changes maintain strict security controls and compliance validation at each deployment stage. Continuous integration and deployment (CI/CD) systems specifically designed for Clean Room environments incorporate privacy impact assessments and regulatory compliance checks as integral parts of the deployment process, preventing privacy violations before they reach production systems.

Observability platforms allow real-time monitoring of Clean Room operations, relating to anomalies that may suggest sequestration violations or compliance issues. These systems create rich logs supporting forensic analysis and regulatory reporting requirements. Higher-level DataOps concepts emphasize building end-to-end monitoring and alerting systems that deliver insight into data pipeline behavior and data quality measures across the analytical life cycle (Novogroder, I. 2025). Observability of distributed analytical processes in real-time guarantees that stakeholders within organizations can have visibility into complicated multi-party computations without compromising confidentiality and security requirements unique to Clean Room environments.

Platform-specific observability solutions implement privacy-preserving telemetry collection that maintains operational visibility without exposing sensitive analytical processes or data patterns. Distributed tracing systems track computation flows across organizational boundaries while maintaining zero-knowledge properties about the underlying data being processed. Sophisticated alerting mechanisms detect potential privacy violations or compliance issues while respecting the confidentiality requirements of multi-party computations, enabling rapid incident response without compromising the fundamental privacy guarantees of Clean Room environments.

Quality Assurance and Validation

Ongoing validation protocols ensure analytical results remain high in fidelity despite privacy-preserving transformations made at all stages throughout Clean Room workflows. Statistical validation models contrast Clean Room outputs with reference analyses to measure accuracy trade-offs that privacy mechanisms impose. Validation procedures guarantee that business choices based on Clean Room analytics have suitable confidence levels. Quality-focused methods in federated learning systems illustrate the importance of in-depth quality assessment frameworks capable of measuring model performance across distributed systems while ensuring privacy restrictions Usman, M. *et al.,* 2025). Sophisticated validation methods allow organizations to determine analytical accuracy and reliability throughout collaborative processes without undermining the basic privacy protections that Clean Room environments are established to offer.

Extensive quality assurance models integrate several validation phases throughout the analytical life cycle, ranging from initial data ingestion to final result creation. Statistical validation methods allow organizations to measure privacy-preserving transformation effects on analytical accuracy to ensure collaborative insights are sufficiently precise for decision-making in the business domain. Quality-oriented federated learning methods place significant emphasis on having systematic quality evaluation methods that are capable of assessing model performance and reliability across various participating organizations Usman, M. *et al.,* 2025). Sophisticated validation frameworks ensure ongoing monitoring of analytical quality through the collaborative process, allowing stakeholders to have confidence in Clean Room analytical findings while preventing privacy-preserving mechanisms from introducing unacceptable uncertainty into collaborative processes.

Platform engineering approaches enable automated quality assurance through continuous validation pipelines that assess analytical accuracy and privacy preservation simultaneously. Container-based testing environments provide isolated spaces for validation workflows, ensuring that quality assessment processes do not compromise the security or privacy of production Clean Room

Publisher: SARC Publisher

operations. Infrastructure automation facilitates rapid deployment of validation environments that mirror production configurations, enabling comprehensive testing of privacy-preserving analytical workflows before deployment to collaborative environments.

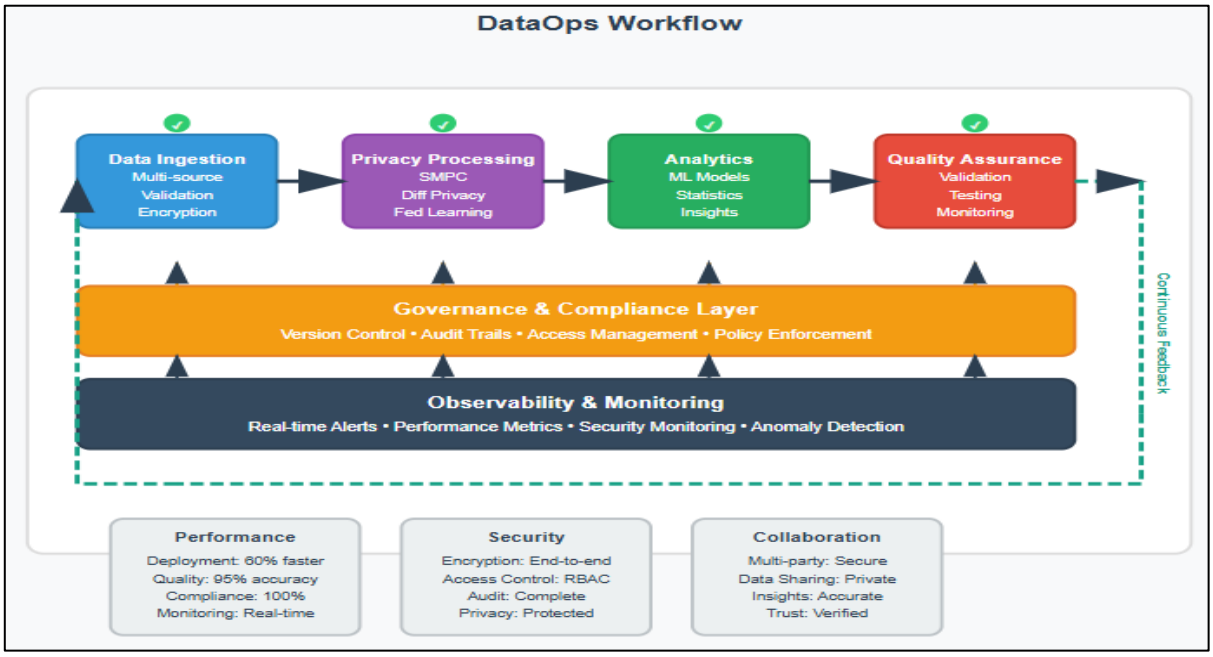

Fig 4. DataOps Workflow Management Chart (Novogroder, I. 2025; Usman, M. *et al.*, 2025)

CONCLUSION

The adoption of Data Clean Rooms transforms how organizations approach collaborative analytics in privacy-sensitive environments, enabling new opportunities for secure data collaboration across industry boundaries. The specialized architecture successfully addresses longstanding challenges in cross-organizational data sharing by combining advanced cryptographic methods with robust governance frameworks and modern platform engineering practices, enabling high-fidelity analytics while maintaining strict privacy protections. Platform engineering foundations provide the critical infrastructure orchestration capabilities that enable Clean Room technologies to operate reliably at enterprise scale, with container orchestration, service mesh architectures, and Infrastructure as Code practices ensuring consistent, secure, and scalable deployments across diverse organizational environments.

Fiscal services associations profit from enhanced fraud discovery capabilities and further robust credit threat modeling through cooperative approaches that save competitive confidentiality, while healthcare institutions can share in large-scale population studies and clinical trial optimization without compromising patient sequestration. The integration of platform engineering principles with privacy-preserving technologies enables these industry applications to scale effectively while maintaining operational excellence and regulatory compliance across multiple jurisdictions. The multi-jurisdictional compliance frame ensures that Clean Room executions can contemporaneously satisfy different nonsupervisory conditions across different legal fabrics, creating scalable results for global associations operating in multiple jurisdictions.

DataOps integration combined with platform engineering practices provides essential functional excellence through automated workflow operation, infrastructure provisioning, and nonstop quality assurance, ensuring that cooperative analytics maintains applicable confidence situations for business decision-making. The sophisticated concurrence operation and rights enforcement mechanisms produce coordinated approaches that cover individual sequestration preferences across multiple sharing associations, with platform-level automation ensuring consistent policy enforcement and rapid response to data subject rights requests.

As non-supervisory surroundings continue evolving toward stricter sequestration conditions, Clean Room technologies combined with modern platform engineering approaches give unborn evidence foundations for sequestration-conserving analytics that can acclimate to changing

Publisher: SARC Publisher

compliance demands while maintaining logical effectiveness. The strategic relinquishment of these integrated technologies will eventually determine organizational success in navigating the complex geography of cooperative invention while meeting increasingly strict sequestration protection conditions across regulated diligence. Platform engineering excellence ensures that these sophisticated privacy-preserving systems can operate with the reliability, scalability, and operational efficiency required for enterprise-scale collaborative analytics initiatives.

REFERENCES

1. Cataligent, "Reduce Compliance Costs Through Industry Collaboration." (2025).
2. Shalabi, E., Khedr, W., Rushdy, E., & Salah, A. "A comparative study of privacy-preserving techniques in federated learning: A performance and security analysis." *Information* 16.3 (2025): 244.
3. Vu, D. H., Luong, T. D., & Ho, T. B. "An efficient approach for secure multi-party computation without authenticated channel." *Information Sciences* 527 (2020): 356-368.
4. Nikolaidis, F., Symeonides, M., & Trihinas, D. "Towards efficient resource allocation for federated learning in virtualized managed environments." *Future Internet* 15.8 (2023): 261.
5. Matuszewska, K. "Privacy by design under the GDPR." *PIWIK*, (2018).
6. Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. "Privacy and security in federated learning: A survey." *Applied Sciences* 12.19 (2022): 9901.
7. Kuna, A. "AI-Driven Behavioral Risk Profiling in Digital Lending Platforms: A Cross-Disciplinary Framework for Dynamic Risk Assessment." *Journal of Computer Science and Technology Studies* 7.6 (2025): 746-751.
8. Haripriya, R., Khare, N., & Pandey, M. "Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings." *Scientific Reports* 15.1 (2025): 12482.
9. Novogroder, I. "DataOps Best Practices and Top Tools for 2025." *lakeFS*, (2025).
10. Usman, M., Bernardi, M. L., & Cimitile, M. "Introducing a Quality-Driven Approach for Federated Learning." *Sensors* 25.10 (2025): 3083.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Pandurangan, S. K. "Privacy-Preserving Risk Analytics Through Data Clean Rooms: An Integrated Platform Engineering and Privacy Technology Framework for Regulated Industries." *Sarcouncil Journal of Engineering and Computer Sciences* 4.9 (2025): pp 31-39.

Publisher: SARC Publisher