# Use of Cleanrooms for Privacy-Safe Measurement of User-Based Randomized Control Trials

Varun Chivukula

Varunvenkatesh88@berkeley.edu

## Abstract

The increasing need for user privacy in the digital age has challenged conventional approaches to measuring the effectiveness of user-based Randomized Control Trials (RCTs). Cleanrooms, designed to ensure data security and privacy, offer an innovative solution for conducting RCTs while adhering to stringent privacy standards. This paper explores the role of cleanrooms in privacy-safe measurement of RCTs, discussing their architecture, implementation, and the implications for research and business practices. It articulates the technical guardrails necessary for cleanroom functionality and effectiveness while addressing challenges and proposing recommendations for optimizing their use in diverse settings. The discussion is substantiated by references to the latest advancements in cleanroom technology and privacy-preserving analytics.

**Keywords:** Cleanrooms, CCPA, GDPR, Randomized control trial(RCT)

## 1. Introduction

Randomized Control Trials (RCTs) are a gold standard for evaluating causal relationships in various fields, including medicine, marketing, and behavioral science. However, the rise in data privacy regulations—such as the General Data Protection Regulation (GDPR) [2] and the California Consumer Privacy Act (CCPA) [3]—has imposed significant constraints on the traditional methods of conducting RCTs. Cleanrooms, secure environments designed for data processing, have emerged as a potential solution, enabling privacy-preserving analysis without compromising data integrity. This paper delves into the technical guardrails that ensure cleanrooms achieve their intended privacy objectives while maintaining analytical rigor.

## 2. Cleanrooms: An Overview

A cleanroom is a secure environment where data from multiple sources can be aggregated and analyzed without exposing identifiable information. Cleanrooms typically use advanced privacy-preserving technologies, such as encryption [6], differential privacy [1], and federated learning [7], to ensure compliance with privacy standards. Companies like Google, Facebook, and Amazon have pioneered cleanroom solutions to facilitate privacy-compliant data sharing and analysis.

### 2.1 Key Features of Cleanrooms

- **Data Anonymization:** Cleanrooms employ techniques to anonymize datasets by removing or masking identifiable attributes.
- **Secure Access Protocols:** Robust access controls ensure that only authorized users can interact with the data.

- **Audit Trails:** Comprehensive logging mechanisms track all activities within the cleanroom, ensuring accountability [9].
- **Predefined Query Libraries:** Analysts are restricted to using preapproved queries to prevent the extraction of sensitive data.
- **Noise Injection:** Statistical noise is added to outputs to mitigate the risk of re-identification through results [1].

## 3. Privacy-Safe RCTs in Cleanrooms

### 3.1 **Designing RCTs in a Cleanroom Environment**

Cleanrooms allow researchers to implement RCTs by providing anonymized and aggregated datasets. The following components are critical for designing privacy-safe RCTs:

- **Data Ingestion:** Secure transfer and storage of data from participating entities using encryption protocols such as TLS 1.3 [6].
- **Randomization:** Assigning participants to control or treatment groups through deterministic or cryptographically secure methods [4].
- **Analysis:** Conducting statistical analysis using pre-approved algorithms to evaluate outcomes, ensuring compliance with privacy regulations [9].

### 3.2 **Privacy Mechanisms in Cleanrooms**

Cleanrooms employ several mechanisms to protect privacy, including:

- **Encryption:** Ensuring data is encrypted both at rest and in transit using standards like AES-256 [6].
- **Differential Privacy:** Adding calibrated noise to datasets to prevent re-identification of individuals while preserving statistical utility [1].
- **Federated Learning:** Distributed machine learning allows models to be trained on decentralized data, avoiding direct data sharing [7].
- **Access Controls:** Implementing role-based access and multi-factor authentication to restrict data access [9].
- **Query Rate Limiting:** Limiting the frequency and scope of queries to mitigate risks of reverse engineering sensitive data [4].

## 4. Technical Guardrails for Cleanroom Implementation

### 4.1 **Infrastructure Security**

- **Zero Trust Architecture:** Cleanrooms operate under a zero-trust model, ensuring that no component is inherently trusted without verification.
- **Data Segmentation:** Separation of data sources and storage reduces the risk of cross-contamination or unauthorized access.

- **Containerization:** Using containerized environments, such as Docker, ensures isolated and consistent runtime environments [9].

### 4.2 **Data Governance**

- **Metadata Management:** Metadata about the datasets—including provenance and access logs—is maintained for auditing and compliance [10].
- **Consent Management:** Cleanrooms integrate mechanisms for managing user consent, ensuring compliance with GDPR and other privacy laws [2].
- **Automated Policy Enforcement:** Policies governing data access and use are automatically enforced through policy-as-code frameworks [4].

### 4.3 **Statistical Safeguards**

- **Threshold Analysis:** Cleanrooms impose minimum thresholds for the size of groups in statistical analyses to reduce the risk of re-identification [1].
- **Synthetic Data Generation:** Where appropriate, synthetic data mimicking the statistical properties of the original dataset is used to preserve privacy [8].

### 4.4 **Audit and Monitoring**

- **Real-Time Monitoring:** Continuous monitoring detects anomalies or unauthorized activities in real-time [9].
- **Independent Audits:** Third-party audits validate the integrity and compliance of the cleanroom environment [4].

## 5. Applications of Cleanrooms in RCTs

Cleanrooms are increasingly being adopted in various industries to measure the impact of interventions through RCTs:

- **Healthcare:** Evaluating the effectiveness of treatments or interventions while complying with HIPAA regulations [10].
- **Marketing:** Measuring ad campaign performance without exposing consumer data [5].
- **Technology:** Assessing user behavior in A/B tests for product development [4].
- **Finance:** Ensuring compliance while analyzing transaction patterns to detect fraud or assess marketing interventions [6].
- **Public Policy:** Evaluating the effectiveness of government programs without compromising citizen privacy [8].

## 6. Challenges in Implementing Cleanrooms

Despite their advantages, cleanrooms face several challenges:

- **Complexity:** High technical and operational complexity in setting up and maintaining cleanroom infrastructure [9].
- **Data Loss:** Aggregation and anonymization may lead to loss of granularity, impacting the precision of results [1].
- **Cost:** Implementing cleanroom technology can be expensive, particularly for small organizations [4].
- **Interoperability:** Ensuring seamless integration between diverse data sources and formats remains a challenge [7].
- **Regulatory Uncertainty:** Emerging regulations may evolve faster than cleanroom implementations can adapt [3].

## 7. Recommendations and Best Practices

To optimize the use of cleanrooms for RCTs, we recommend the following:

- **Standardization:** Develop industry-wide standards for cleanroom architecture and protocols [9].
- **Collaboration:** Encourage collaboration between stakeholders to share best practices and reduce costs [5].
- **Education:** Train researchers and analysts in privacy-preserving techniques and cleanroom technologies [8].
- **Open-Source Frameworks:** Promote open-source tools for building and managing cleanrooms, reducing costs and fostering innovation [7].
- **Adaptive Systems:** Design cleanrooms to adapt dynamically to evolving regulatory and technical landscapes [4].

## 8. Conclusion

Cleanrooms represent a transformative approach to conducting privacy-safe RCTs, balancing the need for rigorous evaluation with stringent privacy requirements. By addressing the challenges and adopting best practices, organizations can leverage cleanrooms to generate actionable insights while maintaining user trust and compliance with regulatory frameworks.

## References

[1] Dwork, C., & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science.*

[2] European Union. (2018). General Data Protection Regulation (GDPR).

[3] California Consumer Privacy Act (CCPA). (2018).

[4] Google Ads Data Hub Documentation. (2023).

[5] Facebook Advanced Analytics Cleanroom Guide. (2023).

[6] Abadi, M., et al. (2016). Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference.*

[7] Google AI Blog. (2021). Federated Learning: Collaborative Machine Learning without Centralized Training Data.

[8] Nissim, K., et al. (2018). Differential Privacy: A Primer for a Non-technical Audience. *Vanderbilt Journal of Entertainment & Technology Law.*

[9] OpenMined. (2022). An Overview of Privacy-Preserving Technologies.

[10] HIPAA Privacy Rule. (2013). U.S. Department of Health & Human Services.