MEDIDATA

WHITE PAPER

Data Integrity

Table of Contents

Background

Medidata is the leading provider of Software as a Service (SaaS) and data analytics solutions for the life sciences industry, specifically within the clinical trials sector. Medidata has a team of regulatory and quality subject matter experts and serves as a trusted advisor to the industry, offering critical insights into current and emerging regulatory policies, shaping strategies in alignment with governing bodies, and advocating for the needs of our clients.

The introduction of Rave, a flexible, robust, and scalable electronic system designed to manage clinical trial data digitally, transformed the landscape of clinical trial data collection. Rave EDC (electronic data capture) is now the world's most robust, sophisticated, and secure system for capturing and managing data from clinical trial sites, patients, and laboratories.

Medidata's leadership in the field is highlighted by our achievement of supporting over 36,000 clinical trials and engaging with more than ten million patients globally.[1]

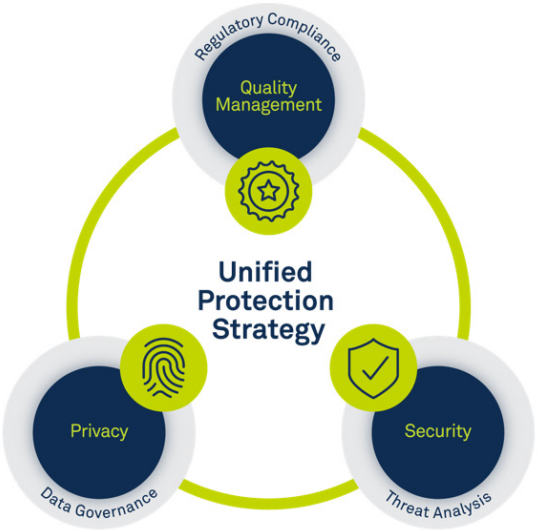
Recognizing that data integrity is a critical concern throughout the lifecycle of clinical and medical device trials, Medidata's systems are designed to ensure data integrity through integrated functionality and procedural controls. Foundational to data integrity are the ALCOA++ principles, which assert that data must be attributable, legible, contemporaneous, original, accurate, complete, available, consistent, enduring, and traceable.[2] Our commitment to data integrity is reinforced through various strategies such as stringent data security protocols, system validation processes, extensive user training, and well-defined contingency measures for system disruptions. Routine monitoring, audits, and quality control procedures are also implemented to validate the effectiveness of these safeguards.

Whilst not exhaustive, this whitepaper will focus on several key global regulatory positions, as outlined in Appendix 1. The following section will discuss our unified protection strategy and quality processes, which cover the data integrity principles outlined above.

Unified Protection Strategy:

Medidata's Unified Protection Strategy is a comprehensive approach that integrates a secure, stable, and scalable cloud platform, the Medidata Platform, with detailed data governance processes and an inspection-ready quality management system, key enablers of successful clinical trial management.

Our Information Security, Privacy, and Quality Management teams seamlessly collaborate to protect data and support regulatory compliance.



A fundamental element of our Unified Protection Strategy is transparency. Over the past 25 years, Medidata has built trust with its clients by offering clear insights into our business operations, bolstered by various third-party attestations and certifications. These endorsements confirm the integrity of our systems, software development life cycle, and our commitment to quality and security standards.

Each component of the Medidata Platform is developed, maintained, and operated in a validated state, supported by well-defined procedures within Medidata's Quality Management System (QMS). This ensures compliance with guidance and global standards underpinning regulatory, information security, and privacy requirements.

Medidata publishes a voluntary Service Organization Control report (SOC2+), conducted biannually by an external auditor. Our SOC 2+ outlines Quality Management, Security, IT Hosting Operations, Data Privacy, Software Development, and Data Integrity. Medidata customers can access this report via the **Trust and Transparency** resources.[3]

Selected Quality Processes:

Quality Policy

In ensuring data integrity, Medidata employs a robust QMS that emphasizes documentation, management accountability, and adherence to regulatory standards, as outlined in our company-wide Quality Policy. The Quality Policy defines elements of Medidata's QMS to demonstrate its commitment to developing, delivering, and maintaining quality software products and services in accordance with applicable regulatory requirements and industry best practices.

Medidata's QMS is governed by a set of controlled documents that outline our policies and procedures. These Quality System Documents (QSDs) describe the global processes for maintaining data standards and ensuring software products conform to specified requirements. QSDs are reviewed biennially to align with current practices and regulatory requirements as mentioned above. Senior management is committed to quality and data integrity by establishing clear responsibilities and regularly reviewing quality objectives. At the same time, the Global Compliance and Strategy (GCS) department conducts independent audits and risk-based reviews to verify compliance and provide regulatory counselling.

Risk management is central to our quality strategy, encompassing supplier evaluations, internal/external audits, and a thorough issue management process. Supplier evaluations are integral to the QMS, ensuring that external contributions meet Medidata's quality and data integrity standards. Internal and external audits monitor compliance, while our Quality Incident Management program addresses data integrity issues, ranging from system bugs and procedural deviations to data corruption, by rapidly enforcing corrective and preventative measures and reviewing the effectiveness of the Corrective Action/Preventive Actions (CAPA) through Effectiveness Checks.

Corporate Records Management

Medidata's Corporate Records Management Policy further details how we reinforce data integrity by setting clear guidelines for securely managing, storing, and disposing of records. A core component is the Records Retention Schedule, which mandates specific retention periods to ensure records remain accessible, accurate, and reliable as long as they are needed to support legal and regulatory needs. This structured approach minimizes the risk of duplicate data impacting data integrity and ensures obsolete records are disposed of consistently. The policy applies to all Medidata personnel and extends to contractors and third-party providers, who must follow the same retention and disposal requirements. The policy requires that records be stored on secure internal systems to support data integrity, reducing the risk of unauthorized access or data corruption. By discouraging personal storage on individual hard drives or removable media, the policy also limits data fragmentation and enhances system-wide data accuracy and integrity.

Management of Customer Data

Medidata's Data Management Standard Operating Procedure (SOP) establishes a structured approach to maintaining data confidentiality, integrity, and availability. This SOP outlines data backup, replication, restoration, and secure handling processes, including decommissioning and destroying data storage devices. It also covers procedures for managing data incidents and implementing continuity measures.

Data management processes are initiated by a range of requirements, such as regular backups and requests for data restoration, that could affect data integrity. Each situation is addressed by developing or updating a Data Management Plan customized to the hosting solution and sanctioned by IT Management. This plan outlines procedures for the frequency of data backups, the handling of restorations, incident response strategies, and data security standards, all of which can be accessed via Medidata's electronic document management system (eDMS).

The SOP mandates that data incidents, such as those involving data loss or security breaches, be escalated to management and addressed in accordance with the Continuity Management SOP. Security and access-related incidents must be directed to IT Management and the Information Security and Privacy Officer, while the Change Management process manages incidents requiring data restoration. Additionally, routine reviews and testing of data management practices, including annual disaster recovery testing, ensure reliability and responsiveness. This structured approach supports secure, reliable data management across our IT Hosting environments, aligning with best practices in data integrity.

Continuity Management

Medidata's Continuity Management SOP outlines an approach to document processes for managing high-risk issues that affect IT hosting services. This SOP is designed to ensure the continuity of critical operations by establishing and testing robust disaster recovery (DR) procedures.

As previously mentioned, the continuity management process is triggered by either an executive decision or the escalation of an incident requiring disaster recovery. Each hosting solution is covered by a DR Plan, which includes procedures for failover to recovery sites and returning operations to the primary environment. Detailed Service Recovery Scripts specify step-by-step actions for restoring services, safeguarding data integrity by ensuring consistent, repeatable recovery procedures. DR plans and scripts are stored in the eDMS to maintain accuracy, providing controlled access and versioning.

Annual testing of each DR Plan verifies the effectiveness of continuity measures, with test outcomes documented in DR Test Summary Reports. These reports highlight any issues encountered and provide recommendations, which, when addressed, enhance data integrity. This annual testing cycle supports continuous improvement and reinforces Medidata's commitment to data integrity by validating that recovery processes are reliable and that data remains secure and accessible in the event of an issue.

Access Management

Medidata's Access Management SOP aligns with data integrity standards by enforcing strict access control protocols across IT Hosting systems. This SOP highlights a structured process for granting, modifying, and revoking access to ensure only authorized users can access sensitive systems and data. Access requests are submitted via Medidata's Task Management System (TMS), which integrates with the Human Resources Information System (HRIS) to automate workflows for events like employee onboarding, offboarding, or leave, ensuring that access changes align promptly with personnel status.

A core aspect of data integrity in this SOP is the principle of least privilege. In this approach, user roles and permissions are limited to the minimum required for job responsibilities. Access is granted through security profiles rather than individual permissions, further supporting consistency and minimizing unauthorized access risks. Additionally, requests for production data access are reviewed carefully and granted only temporarily, reinforcing data security.

Quarterly reviews of all access by the Service Delivery Team ensure ongoing appropriateness, with results documented in summary reports. This review process is essential for data integrity, as it verifies that access privileges remain aligned with user roles and organizational needs. Access Management Plans, stored in Medidata's eDMS, specify protocols for each restricted system, contributing to a controlled environment where data integrity is consistently upheld through rigorous governance.

Software Development and Release

Medidata's Software Development and Release process establishes a framework to ensure data integrity throughout the software lifecycle, from development to release. This SOP, grounded in Agile principles, mandates that each software iteration undergoes comprehensive planning, development, testing, validation, and quality control checks. Testing covers a broad spectrum, including unit tests, functional tests, integration tests, regression tests, and end-to-end tests, which mitigate risks of errors or inconsistencies in data processing. Prioritizing Security and Privacy by Design (PbD) assessments and secure data mapping ensures that data flows within the software are secure and transparent. This supports robust data integrity and compliance with data protection regulations from the initial design phase to product release.

Data integrity is further reinforced through systematic validation procedures. These procedures ensure validated software resides on a qualified infrastructure, meets customer requirements and functions, and complies with applicable GCP, Data Protection/Data Privacy, and Electronic Records/Electronic Signatures regulations and guidance. Every new release, whether a feature, update, or urgent fix, is tested through operational qualification/performance qualification assessments, which verify that all functionalities meet specified requirements and performance benchmarks. All testing documentation, including test plans, test evidence, and test results, is documented within the Release Completion Forms and Validation Summaries and stored in Medidata's eDMS, ensuring traceability and controlled access.

Security vulnerability assessments and automated scans are also integral to each sprint, addressing potential data security risks early in development. Data-impacting defects are tracked and classified by severity, with critical or high-impact issues addressed immediately to safeguard data reliability. System actions and audit trail functionality are maintained as a part of the test evidence within the validation documentation, which is reviewed by Development Management, Test Management, Product Owner, and Release Engineering Management, further contributing to accountability within our processes. Process and Validation (P&V) further conducts an independent review of the Validation Packages within the Validation Portal. 'Validation Certificates' will then be issued confirming that the release is validated in accordance with our procedures and can be deployed to production.

These processes confirm that the final software meets Medidata's data accuracy, security, and regulatory compliance standards before production deployment.

Information Security

Medidata's Information Security Policy is foundational in preserving data integrity across all stages of its lifecycle: data handling, processing, storage, and communication. This policy, aligned with Appendix 1 standards, establishes stringent security protocols to protect data from unauthorized access, alteration, or loss.

Medidata prioritizes protecting its data by employing robust access control measures, such as multifactor authentication and unique user IDs, to ensure accountability and restrict data access to unauthorized personnel. Continuous monitoring and regular audits, including penetration tests and vulnerability assessments, further strengthen our ability to identify and address risks proactively, whilst encryption, using Advanced Encryption Standards algorithms, protects data during storage and transmission. Configuration and change management processes add another layer of protection to our systems by ensuring system security against incoming threats, with all changes reviewed and approved to maintain consistency.

Annual training programs help build awareness among personnel, verifying they understand their roles in preserving data integrity. Strong governance frameworks ensure that accountability is clearly assigned, with the Head of InfoSec overseeing implementation and department managers ensuring compliance within their domain. Incident response and business continuity measures are integrated into this policy, ensuring Medidata's resilience against data-related disruptions while keeping data accurate and intact during incidents. Together, these measures ensure that Medidata maintains the highest security standards, promoting trust and reliability across all aspects of our operations.

Training

Data integrity is embedded within Medidata culture by training personnel on ALCOA++ principles. Mandatory training is provided to all employees concerning the regulatory landscape in which we and our clients operate. Additional role-based training is provided to individuals and teams appropriate to their functional roles within Medidata, enabling them to fulfill their duties and responsibilities within Medidata's QMS. Policy-level training is mandated for all personnel. Training assignments and records of training execution for Medidata personnel are managed in Medidata's LMS. Managers periodically review the training history of each direct report stored in the LMS to ensure that training is up-to-date and complete. A procedure on Training Process & Documentation dictates employee training.

Change Management

Our Change Management SOP establishes a coordinated approach to preserving data integrity throughout the change management lifecycle. By mandating detailed planning, documentation, and oversight, the SOP minimizes risks of data corruption, unauthorized modifications, and service disruptions.

Changes are documented and categorized by criticality, with those affecting data security or system performance requiring leadership approval. Each change follows a detailed Change Management Plan that includes risk assessments, contingency plans, and testing procedures. This ensures potential risks are identified and mitigated before implementation, with protocols in place to roll back errors. Roles such as Change Author, Approver, and Tester ensure accountability, distributing responsibilities to prevent unchecked control.

For client-facing changes, pre-notification, approval, and post-notification requirements promote transparency and trust while protecting clinical data. Additionally, all activities are recorded in a centralized system, providing a complete audit trail and validating compliance with internal and regulatory standards. By integrating thorough risk controls, accountability, and transparency, the change management SOP maintains data integrity as a core priority, ensuring changes are implemented securely and consistently.

Global Customer Data Governance Framework

Medidata's Data Governance Framework ensures accountability for data protection by regulating access, privacy, security, and confidentiality of 'covered data,' defined as: any data received from, or on behalf of a Medidata customer, for which Medidata has data protection responsibilities. It applies to all personnel, activities, and third parties handling such data. Central to this policy is a structured approval process that governs all non-production use of covered data, enforcing strict compliance with privacy and security standards. Implementing this policy includes IT security controls, designated personnel oversight, quarterly executive reporting, mandatory training, and continuous risk assessments. All non-production data use requires a Covered Data Requisition Request (CDRR), documenting processing purposes and requiring approval from GCS, Legal, and InfoSec. Approved CDRRs are retained in accordance with QSD record retention policies, as previously mentioned. This policy ensures data integrity standards across our operations by enforcing strict access controls and ongoing risk assessments.

Conclusion

By embedding ALCOA++ principles into our QMS, we establish a foundation for reliable and secure data management. Our processes are intentionally designed to incorporate data integrity safeguards at every stage, from system validation and access management to audit trails and disaster recovery protocols. Each policy, standard operating procedure, and quality control measure is tailored to meet and exceed regulatory requirements, ensuring data is managed precisely and transparently. Further, the Medidata Platform is built with core functionality that supports ALCOA++ principles, and allows for electronic records in the platform to be audited, capturing creations, additions, and deletions to such records. The platform records the user ID, date/time, and revision action each time an electronic record is created, modified, or deleted. These audit trails can be readily available to clients, further contributing to availability and transparency. This strategy strengthens our platform's reliability and instills confidence in our clients while advancing the broader clinical research goals by delivering secure data solutions.

Appendix: Global Regulatory Standards/Guidance:

Global:

- ICH GCP E6 R3 (adopted by the US, EU, Canada, Japan, Nordic Countries, Australia, etc)[4]
- GAMP 5 (Good Automated Manufacturing Practice): Risk-based validation for automated systems in pharma manufacturing, focusing on quality and system reliability. (cannot access document online without paying)[5]
- WHO Guidelines on Good Data and Record Management Practices: Annex 4: Provides a global framework for data governance and quality in pharmaceuticals, reinforcing ALCOA+ principles.[6]

USA:

- Guidance for Industry - Computerised Systems used in Clinical Trials | FDA [7]
- Guidance for Industry - Electronic Source Data in Clinical Investigations | FDA [8]
- 21 CFR Part 11, Electronic Records; Electronic Signatures - Scope and Application | FDA : Ensures electronic records and signatures are trustworthy and equivalent to paper records through audit trails, access control, and system validation.[9]

UK:

- Guidance for Industry: Guidance on GxP Data Integrity | MHRA[10]

EU:

- EMA Guideline on Computerised Systems and Electronic Data in Clinical Trials[11]
- EU Annex 1: Requires secure, validated computerized systems in GMP environments, emphasizing audit trails, data security, and accuracy.[12]

Japan:

- MHLW Guideline for Electronic Record & Electronic Signatures | PMDA[13]

China:

- Guidance for Industry: Good Clinical Practice for Drugs | NMPA[14]

International Organisation for Standardization (ISO) Standards:

- ISO 27001 - Information Security Management Systems.
- ISO 27002 - Establish, implement, and improve an Information Security Management system focused on cybersecurity.
- ISO 27017 - Information security controls within the cloud.
- ISO 27018 - Protecting Personally Identifiable Information (PII) in the cloud.
- ISO 27701- Privacy Information Management.

Quality System Documents:

Reference	Title
POL-CORP-007	Quality Policy
POL-CORP-005	Corporate Records Management
SOP-ITH-012	Data Management
SOP-ITH-001	Continuity Management
SOP-ITH-003	Access Management
SOP-CORP-013	Training Process and Documentation
SOP-SDLC-013	Develop and Release Software Product
POL-InfoSec-001	Information Security Policy
SOP-CORP-010-007	Operations Change Management
POL-MPO-002	Global Customer Data Governance Framework

References

1 https://www.medidata.com/en/

2 https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

3 https://www.medidata.com/en/

4 https://database.ich.org/sites/default/files/ICH_E6%28R3%29_DraftGuideline_2023_0519.pdf

5 https://ispe.org/pharmaceutical-engineering/january-february-2023/what-you-need-know-about-gampr-5-guide-2nd-edition#:~:text=GAMP%C2%AE%205%20Guide%2C%202nd%20Edition%2C%20seeks%20to%20meet%20and,the%20patient%20and%20the%20public.

6 https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/inspections/trs1033-annex4-guideline-on-data-integrity.pdf?sfvrsn=6218a4e6_4&download=true

7 https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/fda-bioresearch-monitoring-information/guidance-industry-computerized-systems-used-clinical-trials

8 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/electronic-source-data-clinical-investigations

9 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

10 https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity

11 https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf

12 https://health.ec.europa.eu/system/files/2022-08/20220825_gmp-an1_en_0.pdf

13 https://www.pmda.go.jp/files/000263504.pdf

14 https://clinregs.niaid.nih.gov/sites/default/files/documents/china/NMPA-GCP-No57-2020_Google-Translation.pdf