Using MongoDB Atlas in GxP Systems

Achieving Compliance and Implementing Best Practices

December 2024

MongoDB.

Table of Contents

Abstract

The primary purpose of this white paper is to provide a comprehensive guide on best practices for using MongoDB Atlas as a database in GxP (Good Practice) regulated environments. GxP regulations, which encompass Good Manufacturing Practice (GMP), Good Clinical Practice (GCP), and Good Laboratory Practice (GLP), among others, are critical for ensuring the safety, quality, and efficacy of products. These regulations are applied across various industries, including pharmaceuticals, biotechnology, medical devices, food, cosmetics, and veterinary products. This white paper aims to help organizations understand how to leverage MongoDB while maintaining compliance with these stringent regulatory standards.

Additionally, this document seeks to address the unique challenges and considerations involved in using a non-relational database like MongoDB in GxP environments. By providing detailed recommendations, case studies, and practical examples, this white paper will serve as a valuable resource for IT professionals, compliance officers, and quality assurance teams. It will guide them in implementing and managing MongoDB in a manner that ensures regulatory compliance, enhances data integrity, and supports overall operational efficiency.

When using MongoDB Atlas for GxP activities, it is crucial to ensure that the system is developed, validated, and operated according to its intended use.

Disclaimer

Introduction

The life sciences and healthcare industries have experienced tremendous change in recent years, with significant data and workload migrations to the cloud. This shift accelerated in 2020 as organizations adopted new policies for remote work, virtual engagement, remote patient care, and decentralized clinical research.

By 2026, it's projected that 70% of hospitals will have adopted a cloud-based approach to supply chain management, highlighting the growing reliance on cloud technologies in healthcare. Furthermore, a McKinsey report suggests that cloud capabilities could generate substantial value for healthcare companies, with an estimated $100 billion to $170 billion by 2030.

MongoDB Atlas, a leading cloud-based data platform, has emerged as a preferred choice for regulated IT systems in the life sciences and healthcare sectors. Its agility, automation capabilities, and robust security features align with the stringent requirements of these industries. MongoDB Atlas enables organizations to scale their data infrastructure seamlessly, automate routine tasks, and maintain comprehensive security controls. While MongoDB Atlas supports the implementation of GxP (Good Practice) regulations, compliance is ultimately achieved through proper configuration and management by the user organization.

This document serves as a comprehensive guide for deploying MongoDB Atlas effectively in GxP-related processes. It draws upon insights gained from collaborations with pharmaceutical and medical device companies and outlines key considerations for audit strategies, IT frameworks, and operational protocols specific to MongoDB Atlas.

About MongoDB Atlas

MongoDB was founded in 2007 to address the challenges of managing and processing large volumes of diverse data. The company's founders aimed to create a database that leverages the flexibility and scalability of distributed systems, overcoming the limitations of

traditional relational databases in handling varied and rapidly changing data types. This vision led to the development of MongoDB, a document-oriented database designed to store, process, and manage large sets of data efficiently, enabling developers to build applications faster and more flexibly.

MongoDB's impact has been significant, with millions of developers across various industries using the platform to build applications, from simple to highly complex systems. As cloud computing capabilities grew, MongoDB evolved into MongoDB Atlas, a comprehensive cloud-hosted database platform launched in 2016. MongoDB Atlas provides businesses with a scalable, secure, and easy-to-use database solution, supporting data storage, indexing, and security features.

Designed for businesses of all sizes, MongoDB Atlas offers flexible pricing options and supports a wide range of use cases, including web and mobile applications, real-time analytics, and microservices. It delivers high availability and dependability, ensuring that customer data is always secure and accessible. With MongoDB Atlas, businesses can focus on their core competencies, leaving the database management to MongoDB.

MongoDB Atlas adheres to a range of compliance standards, including ISO 27001, ISO 27017, ISO 27018, ISO 9001, SOC 2, PCI DSS, HIPAA, HDS, and TISAX, providing a foundation for GxP compliance. Additionally, MongoDB has engaged an independent auditor to author a report on the information security and privacy program of MongoDB Atlas related to HIPAA and HITECH.

MongoDB Atlas for healthcare and life sciences

MongoDB Atlas is a leading data platform addressing the complex data needs of healthcare providers, payers, and related entities, as well as life sciences companies. Its foundational use of the document model enables the accommodation of diverse and complex data types, crucial for healthcare and life sciences, to describe the intricate complexity of the human body and biological processes.

It supports organizations achieving healthcare interoperability in both healthcare and life sciences. MongoDB Atlas serves as the persistence layer for key healthcare data standards like HL7 FHIR, and can be integrated with existing applications and APIs, enhancing patient care and data utilization efficiency.

MongoDB Atlas empowers healthcare providers with real-time access to complete patient information, overcoming data silos and fragmentation, while allowing life sciences companies to streamline research and development processes, manage clinical trial data efficiently, and ensure regulatory compliance.

Leading healthcare organizations like GE Healthcare and Humana leverage MongoDB Atlas to drive innovation and improve patient outcomes through advanced data management and analytics. Similarly, leading life sciences companies utilize MongoDB Atlas to handle large-scale genomic data, enhance drug discovery and development processes, and manage complex datasets necessary for advanced research and innovation.

Overall, MongoDB Atlas's scalable and flexible platform is engineered to meet the stringent requirements of both the healthcare and life sciences sectors, promoting better patient care, operational efficiency, and scientific advancement.

Some customer case studies can be found at https://mongodb.com/library/customer-case-studies?industries=healthcare

For additional information around specific case studies and solutions, visit our webpage on MongoDB, the Healthcare Database.

Examples of use cases in the life sciences sector

MongoDB Atlas offers robust solutions for various critical applications in the life sciences sector. Below are some specific examples highlighting how MongoDB Atlas can be leveraged to enhance operations, ensure regulatory compliance, and drive innovation in this field.

Clinical trials management

- **Data collection and analysis:** MongoDB Atlas can be used to collect and analyze data from clinical trials. Its ability to handle large volumes of diverse data types makes it ideal for aggregating patient data, treatment outcomes, and other critical metrics. Compliance features ensure that all data handling meets regulatory requirements.
- **Patient monitoring:** Real-time data synchronization and analytics capabilities enable continuous monitoring of patients participating in clinical trials, helping researchers quickly identify and respond to adverse events.

Electronic health records (EHRs)

- **Secure and scalable data storage:** MongoDB Atlas provides a secure, scalable platform for storing EHRs, ensuring that patient data is protected and easily accessible by authorized healthcare providers.
- **Interoperability:** MongoDB's flexible schema design allows for seamless integration with other healthcare systems, facilitating the exchange of information between different healthcare providers and systems while maintaining compliance with regulations like HIPAA.

Pharmacovigilance

- **Adverse event reporting:** MongoDB Atlas can be used to collect and analyze adverse event reports, helping pharmaceutical companies identify and respond to potential safety issues with their products. The platform's auditing and compliance.

Why choose MongoDB for GxP environments?

Choosing MongoDB for GxP environments offers numerous advantages in terms of reducing the complexity, flexibility and performance at scale, and, crucial for managing complex data in regulated industries. With the rise of AI and generative AI, the ability to handle large volumes of diverse data efficiently is more important than ever.

Its robust security features and comprehensive support for automation and high availability make it an ideal choice for regulated industries aiming to integrate AI and generative AI into their workflows while maintaining compliance.

Overview of GxP regulations

GxP regulations encompass a set of guidelines and requirements intended to ensure that products in regulated industries, such as pharmaceuticals and biotechnology, are safe, meet their intended use, and adhere to quality standards. The term “GxP ″ stands for “Good Practice” and the “x” represents the various fields, such as Good Manufacturing Practice (GMP), Good Clinical Practice (GCP), and Good Laboratory Practice (GLP). These regulations cover a wide range of activities from manufacturing processes to clinical trials and laboratory testing, ensuring that each step of the product life cycle maintains a high standard of quality and compliance.

Definition and importance

The importance of GxP regulations cannot be overstated. These guidelines help prevent errors, inconsistencies, and risks associated with the production and testing of medical products. This involves rigorous processes, documentation, and oversight to safeguard the health and safety of patients and consumers. Additionally, following GxP guidelines, organizations can minimize risks of contamination, mix-ups, and errors during manufacturing and handling processes.

Compliance with GxP standards ensures that companies maintain a systematic approach to quality management, which is essential for patient safety and product efficacy. Non-compliance can lead to severe consequences, including product recalls, legal penalties, and loss of consumer trust. GxP compliance also facilitates transparency and traceability, allowing for effective auditing and review. This not only helps in maintaining regulatory compliance but also enhances the overall credibility and reliability of the products in the eyes of regulatory bodies and the public.

Therefore, adherence to GxP regulations is not just a legal obligation but a **critical** aspect of ethical business practices in the life sciences industry.

GxP computerized systems

Today, all processes are digitized, and therefore all IT infrastructure and applications involved in these processes need to comply with GxP regulations. A GxP computerized system, also referred to as a GxP system or GxP application, is subject to these regulations. A key component of this digital landscape is the database, which plays a crucial role in storing, managing, and retrieving data throughout the product life cycle.

Implications of database management in GxP compliance

The implications of a database as part of GxP compliance are significant. Databases must ensure data integrity, accuracy, and security to meet regulatory requirements. This includes maintaining comprehensive audit trails, enabling traceability of data changes, and ensuring restricted access to sensitive information. Failure to implement robust database management practices can lead to data breaches, loss of data integrity, and non-compliance with GxP standards, which can have severe legal and financial repercussions. Therefore, integrating GxP principles into database management is essential to support the overall quality management system, ensuring that all data handled is reliable, secure, and compliant with regulatory expectations.

Data integrity

Data integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. In GxP-regulated environments, data integrity is not just a regulatory requirement; it is a cornerstone of ensuring that products are safe, effective, and meet quality standards. For organizations in the life sciences sector, maintaining data integrity is critical for patient safety, product efficacy, and overall compliance with regulatory standards such as FDA's 21 CFR Part 11 and EMA's Annex 11.

Organizations must implement stringent controls to protect data from unauthorized access, modification, or deletion, and to ensure that all data is recorded accurately and in a timely manner.

Core principles of data integrity

- **Attributability:** Every piece of data should be traceable to a specific individual or system action. This ensures accountability and allows for the identification of who performed a particular action, such as data entry, modification, or deletion.
- **Legibility:** Data must be easily readable and understandable by humans. This ensures that records can be reviewed and interpreted during audits or investigations.
- **Contemporaneity:** Data should be recorded at the time the event occurs. This principle is vital for ensuring that records accurately reflect the events they describe.
- **Originality:** Original data, or its true copy, must be preserved.
- **Accuracy:** Data must be free from errors and accurately reflect the process or action it records.

Technological measures supporting data integrity

MongoDB Atlas offers several features and technologies that help organizations maintain data integrity in compliance with GxP regulations:

- **Immutable audit logs:** MongoDB Atlas provides immutable audit logs, ensuring that once data is recorded, it cannot be altered or deleted. These logs record all database activities, including data access, modifications, and deletions, creating a reliable audit trail that supports compliance with regulatory requirements.
- **Encryption and access controls:** Data integrity is closely tied to data security. MongoDB Atlas encrypts data both at rest and in transit, ensuring that data remains secure from unauthorized access. Role-based access control (RBAC) further ensures that only authorized users can view or modify critical data, thereby reducing the risk of data tampering.
- **Automated backups and disaster recovery:** MongoDB Atlas provides automated backups and point-in-time recovery options. This ensures that data can be restored

to its original state in case of corruption, loss, or accidental modification, thus maintaining data integrity over time.

- **Validation and error detection:** MongoDB Atlas includes schema validation mechanism to ensure that data entered into the system meets predefined criteria, reducing the likelihood of errors.
- **Data retention policies:** Configurable data retention policies in MongoDB Atlas allow organizations to manage the lifecycle of their data in accordance with regulatory requirements. These policies ensure that data is retained for the required period and is securely deleted when it is no longer needed, preventing unauthorized access to obsolete data.

Best practices for ensuring data integrity with MongoDB Atlas

To fully leverage MongoDB Atlas in maintaining data integrity, organizations should implement the following best practices:

- **Regular audits and reviews:** Conduct regular audits of MongoDB Atlas audit logs and data access records to identify and address any potential integrity issues. This proactive approach helps in maintaining continuous compliance.
- **User training and awareness:** Ensure that all users are trained on the importance of data integrity and how to use MongoDB Atlas features effectively to protect data. Awareness programs should emphasize the critical role of accurate data entry, timely recording, and adherence to access controls.
- **Data validation procedures:** Implement robust data validation procedures to check the accuracy and consistency of data as it is entered into the system. MongoDB Atlas's validation tools should be configured to enforce these checks automatically.
- **Documentation and recordkeeping:** Maintain thorough documentation of all data management processes, including data retention policies, backup procedures, and validation protocols. This documentation is essential for demonstrating compliance during regulatory audits.
- **Change management controls:** Implement strict change management controls to document, review, and approve any changes to the MongoDB Atlas

configuration or data handling procedures. This ensures that all changes are carefully considered and do not compromise data integrity.

Data integrity is a fundamental requirement in GxP environments, and MongoDB Atlas provides the necessary tools and features to help organizations maintain it effectively. By implementing the right technological measures, adhering to best practices, and continuously monitoring data handling processes, organizations can ensure that their data remains accurate, reliable, and compliant with regulatory standards.

Customer and platform definitions

Within the context of this document, the customer refers to any person or organization using or managing a GxP computerized system hosted on a cloud platform such as MongoDB Atlas. The platform encompasses a collection of integrated cloud services, including personnel, processes, technology, software, and physical infrastructure, which together deliver the complete service offering.
This version integrates the key points about the importance of databases in GxP compliance and incorporates definitions and concepts similar to those found in MongoDB Atlas documentation. It also maintains clarity and relevance for the target audience.

Relevant regulatory bodies (e.g., FDA, EMA)

The enforcement of GxP regulations is overseen by various national and international regulatory bodies, each with its own set of guidelines and standards. In the United States, the Food and Drug Administration (FDA) is the primary regulatory authority responsible for ensuring compliance with GxP standards in the pharmaceutical, biotechnology, and medical device industries. The FDA's regulations, such as 21 CFR Part 11, specify requirements for electronic records and electronic signatures, ensuring the integrity and authenticity of data.

In Europe, the European Medicines Agency (EMA) plays a similar role, providing comprehensive guidelines and regulations to ensure product safety and efficacy across member states. The EMA's GxP guidelines include requirements for Good Manufacturing Practice (GMP), Good Clinical Practice (GCP), and Good Laboratory Practice (GLP), among others. Both the FDA and EMA collaborate with other international regulatory bodies to harmonize standards and facilitate global trade and regulatory compliance. Understanding the requirements of these regulatory bodies is crucial for companies operating in the life

sciences sector, as it ensures their products meet the highest standards of quality and safety.

Key GxP principles

Key GxP principles are the foundation upon which all GxP regulations are built. These principles include consistency, traceability, accountability, and transparency. Consistency ensures that processes are performed the same way every time, which is critical for maintaining product quality. Traceability involves maintaining comprehensive records that allow every step of the process to be traced back to its origin, which is vital for audits and investigations. Accountability ensures that every action is attributable to a responsible individual, which promotes responsible behavior and decision-making.

Transparency is another crucial GxP principle, requiring clear and accessible documentation of all processes, decisions, and actions. This openness is essential for regulatory audits and helps build trust with regulatory authorities and the public. These principles ensure that organizations can reliably produce safe and effective products, maintain compliance with regulatory requirements, and quickly identify and address any issues that arise.

Good documentation practices (GDP)

Good documentation practices (GDP) are a set of standardized procedures for creating, managing, and storing documents in a compliant manner. GDP ensures that all records are accurate, complete, legible, and traceable, which is essential for maintaining data integrity and facilitating regulatory audits. Proper documentation includes recording data at the time of the activity, ensuring that entries are signed and dated, and preventing unauthorized changes or deletions.

The importance of GDP lies in its role in maintaining the integrity of data throughout the product life cycle. Accurate and reliable documentation is critical for verifying that processes are performed correctly and consistently. It also provides a traceable history of all activities, which is essential for identifying the root cause of any issues and implementing corrective actions. By adhering to GDP, organizations can ensure that their

documentation meets regulatory requirements and supports the overall quality management system.

Good automated manufacturing practice (GAMP)

Good automated manufacturing practice (GAMP) guidelines provide a framework for validating automated systems used in the manufacturing of regulated products. GAMP emphasizes a risk-based approach to validation, ensuring that critical systems and processes are thoroughly tested and documented. This includes the validation of software, hardware, and processes to confirm that they operate as intended and meet all regulatory requirements.

The implementation of GAMP guidelines helps organizations ensure the reliability and integrity of their automated systems. This is particularly important in GxP environments where the quality and safety of products depend on the accuracy and consistency of automated processes. By following GAMP principles, companies can reduce the risk of system failures, improve efficiency, and maintain compliance with regulatory standards. GAMP also promotes continuous improvement and innovation, helping organizations stay competitive in the rapidly evolving life sciences industry.

MongoDB Atlas offering

Its robust security features and comprehensive support for automation and high availability make it an ideal choice for regulated industries aiming to integrate AI and generative AI into their workflows while maintaining compliance.

MongoDB Atlas offers a highly scalable cloud database platform with high availability and dependability, providing the tools necessary to run a wide range of applications. Ensuring the confidentiality, integrity, and availability of our customers' systems and data is paramount to MongoDB, as is maintaining customer trust and confidence.

Similar to other general-purpose IT products such as operating systems and database engines, MongoDB Atlas offers commercial off-the-shelf (COTS) IT services according to IT

quality and security standards such as ISO, NIST, SOC, and many others. For the purposes of this document, we will use the definition of COTS in accordance with the definition established by FedRAMP, a United States government-wide program for procurement and security assessment. FedRAMP references the US Federal Acquisition Regulation (FAR) for its definition of COTS, which outlines COTS items as:

- Products or services that are offered and sold competitively in substantial quantities in the commercial marketplace based on an established catalog.
- Offered without modification or customization.
- Offered under standard commercial terms and conditions.

MongoDB Atlas's products and services provide the necessary tools and infrastructure to support GxP compliance by ensuring data integrity, security, and traceability. The platform's built-in security features and compliance certifications help life sciences organizations meet regulatory requirements for electronic records and electronic signatures (e.g., 21 CFR Part 11). Additionally, MongoDB Atlas's high availability and disaster recovery capabilities ensure continuous operation and data protection, which are critical for maintaining compliance in regulated environments.

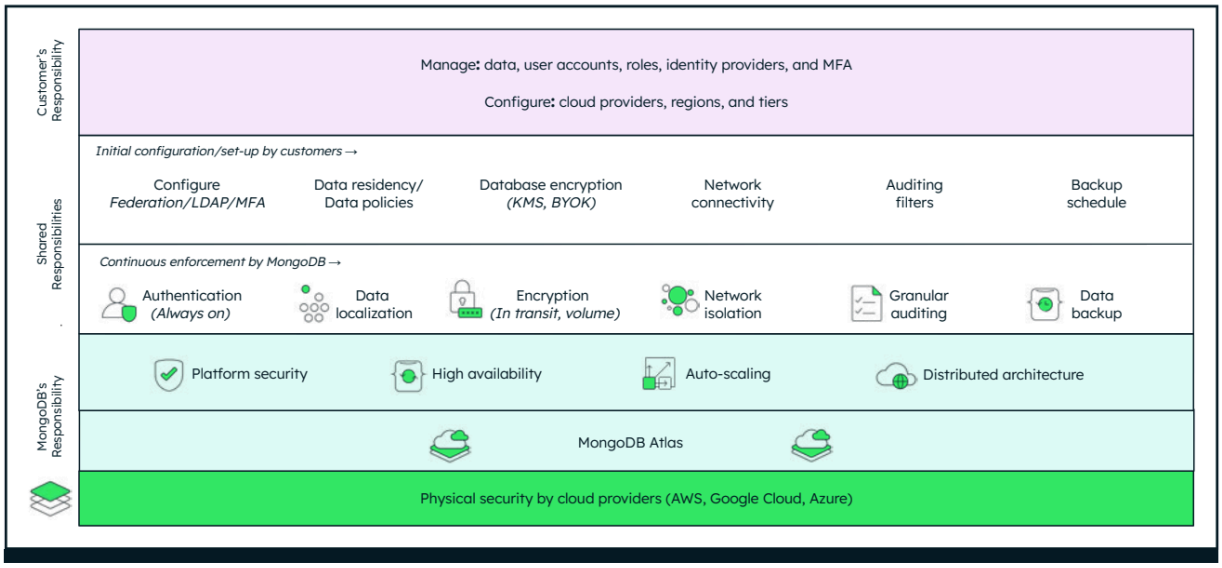
By leveraging MongoDB Atlas, organizations can focus on innovation and efficiency while ensuring that their data management practices adhere to stringent GxP standards, ultimately supporting the development, manufacturing, and distribution of safe and effective products.

Under GAMP guidelines (such as GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems), organizations implementing GxP-compliant environments will need to categorize MongoDB Atlas services using respective GAMP software categories. Under GAMP guidelines, MongoDB Atlas is **categorized as Software Category 1**—Infrastructure Software, which includes database managers and security software. This categorization reflects its role as a general-purpose, commercial off-the-shelf (COTS) solution that provides foundational services for GxP-compliant environments.

Shared responsibility model

As with any cloud service, the provider and customers share responsibility for securely using the service. MongoDB Atlas has been designed with strong security defaults in mind so that the burden of securely using the service is minimized for the customer. These defaults include always-on authentication, authorization, encryption in-transit, encryption at-rest, and no database access from the internet by default. MongoDB Atlas is architected to provide automated database resilience and mitigate the downtime risks associated with hardware failures or unintended actions

While this document provides information on using MongoDB Atlas services in GxP environments, it is important to consult with your own legal advisors to ensure that your GxP policies and procedures are in compliance with regulatory requirements.



Customer responsibilities

- **Managing data:** Customers are responsible for managing their data, including user accounts, roles, identity providers, and multi-factor authentication (MFA).
- **Initial configurations:** Customers need to set up the cloud providers, regions, and service tiers they want to use, along with configuring federation/LDAP/MFA, data residency/policies, database encryption (using either MongoDB's Key Management

System (KMS) or their own keys (BYOK)), network connectivity, auditing filters, and backup schedules.

Shared responsibilities

- **Configuration:** Both MongoDB and customers share the responsibility for configuring specific aspects of the service. Customers initially set up configurations like federation, data residency, encryption, network connectivity, auditing, and backups. MongoDB ensures the continuous enforcement of these configurations.
- **Data security:** Customers are responsible for defining data residency and data policies. MongoDB enforces these policies and ensures data localization as per requirements. MongoDB also handles encryption of data both in transit and at rest (volume encryption).
- **Auditing:** While customers define the auditing filters initially, MongoDB provides granular auditing capabilities and ensures continuous enforcement.
- **Backups:** Customers define the backup schedule, while MongoDB is responsible for carrying out the actual data backup process.

MongoDB's responsibilities

- **Platform security:** MongoDB takes on the responsibility for the security of the underlying platform, including physical security (provided by cloud providers like AWS, Google Cloud, and Azure).
- **Authentication:** MongoDB ensures continuous authentication and authorization of users and processes.
- **Network isolation:** MongoDB isolates customer networks to enhance security.
- **Core service management:** MongoDB manages the core aspects of the Atlas service, such as platform security, high availability, auto-scaling, and maintaining the distributed architecture of MongoDB Atlas.

For a detailed explanation of the MongoDB Atlas Shared Responsibility Model, we strongly recommend referring to the "Who Owns Security in the Cloud?" white paper.

Features for enhancing GxP compliance

MongoDB Atlas offers specific controls and features that enhance GxP compliance, making it an ideal database solution for organizations in the healthcare and life sciences

sectors. By leveraging these features, organizations can maintain high standards of data integrity, security, and regulatory adherence.

Security and compliance features

- **Encryption at rest and in transit:** MongoDB Atlas ensures data is encrypted both at rest and in transit, safeguarding sensitive healthcare data from unauthorized access and breaches.
- **Role-based access control (RBAC):** MongoDB Atlas provides fine-grained access control, allowing administrators to define roles and permissions to ensure that only authorized personnel can access or modify critical data.
- **Auditing:** Comprehensive auditing capabilities allow tracking of all access and modifications to data. This is crucial for maintaining an audit trail and ensuring accountability and transparency, as required by GxP regulations.
- **Multi-Factor authentication (MFA):** Enhances security by requiring multiple forms of verification before access is granted, ensuring that only authorized users can access the system.
- **Automated backups and point-in-time recovery:** Automated backups and the ability to perform point-in-time recovery ensure that data can be restored accurately and quickly in case of an incident, which is critical for maintaining data integrity and availability.
- **Compliance certifications:** MongoDB Atlas adheres to a range of compliance standards, including ISO 27001, SOC 2, PCI DSS, HIPAA, and HITRUST, providing a foundation for GxP compliance.

Data Integrity and validation

- **Immutable audit logs:** Ensuring that audit logs cannot be altered once written, which helps in maintaining data integrity and complying with regulatory requirements.
- **Time-based data retention policies:** Configurable data retention policies ensure that data is retained for the required period and then securely deleted, aiding in compliance with data lifecycle management regulations.
- **Zero-downtime maintenance:** Maintenance and upgrades are performed without downtime, ensuring continuous compliance and availability of the system.

Operational controls

- **Change management:** MongoDB Atlas supports robust change management practices, ensuring that any changes to the system are properly documented, tested, and approved before implementation.

- **Disaster recovery:** Built-in disaster recovery capabilities ensure data can be quickly restored in the event of a catastrophic failure, ensuring business continuity and compliance with data availability requirements.

Monitoring and reporting

- **Comprehensive monitoring:** MongoDB Atlas provides comprehensive monitoring tools to track database performance and health, enabling proactive identification and resolution of issues.
- **Custom alerts:** Customizable alerts can be set up to notify administrators of any unusual activity or potential compliance breaches, allowing for immediate action to be taken.

Compliance and trust

MongoDB is dedicated to protecting customer data and has a robust compliance and trust program for its cloud offerings. This program includes continuous monitoring, comprehensive documentation, dedicated customer support, and training to ensure the highest levels of security and privacy standards. MongoDB is committed to meeting the most stringent regulatory requirements and providing customers with the resources they need to maintain compliance.

> You can find detailed white papers on MongoDB products, privacy, and data protection considerations at MongoDB Trust Center

MongoDB Atlas compliance

MongoDB is consistently broadening our range of security and compliance reports in response to customer requests. Below is the current list of reports accessible to all customers and prospects under an NDA. For copies of reports relevant to your organization or to inquire about upcoming certifications, please contact us.

The scope of services under compliance and trust includes Atlas Database, Atlas Search, Charts, Cloud Manager, and MongoDB Serverless.

Quality management

MongoDB adheres to industry standards for the design, development, release, maintenance, and support of its services, ensuring alignment with quality management (QM) principles and requirements. MongoDB holds the ISO 9001:2015 certification, among others related to QM. Learn more.

HITRUST and HIPAA compliance

HITRUST

The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) provides a guide to regulatory compliance and risk management for the healthcare industry. MongoDB maintains a SOC 2 + HITRUST certification report, which maps SOC 2 Type II controls to the 75 required HITRUST controls. Although MongoDB's cloud services are not HITRUST CSF certified, this report covers all applicable HITRUST CSF controls, a recommended approach by both AICPA and HITRUST.

HIPAA

For customers subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), MongoDB Atlas supports HIPAA compliance. It enables covered entities and their business associates to use a secure MongoDB Atlas environment to process, maintain, and store protected health information (PHI). MongoDB, Inc. will enter into Business Associate Agreements (BAAs) with customers as necessary to ensure compliance under HIPAA.

Learn more about MongoDB's compliance with HITRUST and HIPAA.

Global security and compliance standards

MongoDB meets a range of global security and compliance standards, ensuring the protection of sensitive data and adherence to industry regulations. Certifications include:

- **GDPR:** Complies with data protection laws across the EU.
- **ISO/IEC 27001:** Certified for information security management systems (ISMS).
- **ISO/IEC 27017:** Provides cloud-specific security controls.
- **ISO/IEC 27018:** Focuses on protecting personal data in the cloud.
- **SOC 2:** Audited for safeguarding data confidentiality and privacy.

- **PCI DSS:** Validated as a PCI-compliant service provider.
- **CSA STAR:** Achieved Level 2 for security and privacy controls.
- **VPAT:** Accessibility Conformance Reports for MongoDB products.

Additional market & industry specific certifications:

- **IRAP:** Australian government security compliance.
- **TISAX:** Automotive industry information security.
- **HDS:** French certification for health data hosting.
- **QC2**: From the Italian Agenzia per la Cybersicurezza Nazionale (ACN).

MongoDB Atlas for government compliance

MongoDB Atlas for Government (US) is a FedRAMP® authorized and dedicated environment of MongoDB Atlas for the US public sector as well as ISVs looking to build offerings for the US public sector.

- **FedRAMP® Moderate Authorized:** The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. MongoDB Atlas for Government is FedRAMP Moderate authorized. This authorization ensures that MongoDB Atlas meets the stringent security requirements necessary for use by U.S. government agencies.
- **Criminal Justice Information Solutions (CJIS):** CJIS compliance ensures that MongoDB Atlas can securely handle and store criminal justice information. This is crucial for government agencies and organizations that deal with law enforcement data.
- **TX-RAMP:** The Texas Risk and Authorization Management Program (TX-RAMP) is a state-specific framework for cloud services security. TX-RAMP compliance enables MongoDB Atlas to be used by Texas state agencies and their contractors.

NIST AI Safety Institute Consortium

MongoDB is collaborating with the National Institute of Standards and Technology (NIST) in the AI Safety Institute Consortium to develop measurement science for identifying proven, scalable, and interoperable AI methodologies. NIST does not evaluate or endorse any commercial products in this Consortium. More information can be found here.

For more detailed information about our security and compliance practices, please, check the MongoDB Atlas Trust Center and the MongoDB Atlas Security White Paper for more information about the security controls in MongoDB Atlas.

Electronic records / controls for closed systems

Ensuring compliance with Title 21 CFR Part 11 is crucial for organizations in the healthcare and life sciences sectors, as it governs the management of electronic records and electronic signatures. MongoDB Atlas provides several features designed to support compliance with these regulations, ensuring data integrity, security, and accountability.

Importance of compliance with Title 21 CFR Part 11

Overview of Title 21 CFR Part 11

Title 21 CFR Part 11 is a regulation established by the U.S. Food and Drug Administration (FDA) that sets the criteria for the acceptance of electronic records and electronic signatures by the FDA. This regulation applies to electronic records used in FDA-regulated environments, such as pharmaceutical manufacturing, biotechnology, and medical device production. Compliance with this regulation is critical for ensuring that electronic records are trustworthy, reliable, and equivalent to paper records.

Key requirements

- **Validation:** Systems must be validated to ensure accuracy, reliability, and consistent performance.
- **Audit trails:** Secure, computer-generated audit trails must be in place to record the date and time of operator entries and actions that create, modify, or delete electronic records.
- **Record retention:** Records must be maintained for the required retention period and be readily retrievable.
- **User access controls:** Systems must limit access to authorized individuals and ensure that electronic signatures are unique to each user.
- **Electronic signatures:** Electronic signatures must be legally binding, unique to the individual, and verifiable.

Importance of compliance

- **Regulatory approval:** Compliance with Title 21 CFR Part 11 is necessary for obtaining and maintaining FDA approval for products and processes.
- **Data integrity:** Ensuring the integrity of electronic records is vital for patient safety, product efficacy, and regulatory compliance.

- **Operational efficiency:** Implementing compliant systems can streamline processes, reduce the need for paper records, and enhance data management capabilities.

Features of MongoDB Atlas that Support Compliance with Electronic Records and Electronic Signatures

MongoDB Atlas provides several features designed to help organizations comply with Title 21 CFR Part 11, ensuring the secure and reliable management of electronic records and electronic signatures.

Title 21 CFR Part 11- Subpart B - Electronic Records

Data integrity and validation

Validation: MongoDB Atlas supports system validation by providing robust tools and documentation to help customers validate their deployment. This includes guidelines for installation qualification (IQ), operational qualification (OQ), and performance qualification (PQ).

Data integrity controls: MongoDB Atlas ensures data integrity through features such as immutable audit logs, time-based data retention policies, and rigorous access controls.

Compliance support	Description
Regulatory adherence	The comprehensive auditing features of MongoDB Atlas help organizations adhere to regulatory requirements by providing a complete and accurate record of all database activities
Audit readiness	Detailed and immutable audit trails ensure that organizations are always prepared for regulatory audits, providing clear and traceable records of all interactions with the database.

Data integrity	Description
Accountability	By maintaining detailed logs of who accessed the data and what changes were made, MongoDB Atlas ensures that all actions are attributable to specific users, promoting

	accountability.
Anomaly detection	Regular review of audit logs can help detect unauthorized or suspicious activities, allowing for timely intervention and corrective actions.

Operational efficiency	**Description**
Streamlined investigations	In the event of data discrepancies or incidents, comprehensive audit logs facilitate quick and effective investigations, helping to identify the root cause and implement corrective measures.

Audit trails

- **Comprehensive auditing:** MongoDB Atlas includes comprehensive auditing capabilities that allow organizations to track access and modifications to data. This includes detailed logs of who accessed what data and when, as well as what changes were made.
- **Immutable logs:** Audit logs in MongoDB Atlas are immutable, meaning they cannot be altered once written. This helps maintain the integrity of audit trails and ensures compliance with regulatory requirements.

MongoDB Atlas provides robust auditing capabilities that are essential for maintaining compliance with regulatory requirements, including Title 21 CFR Part 11. These auditing features help organizations track and monitor access to data and any changes made, ensuring accountability and data integrity. Customers can enable comprehensive database auditing to

Key auditing features	**Description**
Access history	MongoDB Atlas maintains detailed logs of all user access to the database. This includes who accessed the data, what data was accessed, and the time of access
Query history	The platform logs all queries executed on the database, providing a record of what operations were performed, by

	whom, and when
Configuration changes	Audit logs capture any changes to the database configuration, including schema changes, user roles, and permissions adjustments.
Data modifications	MongoDB Atlas tracks all modifications to data, including insertions, updates, and deletions, ensuring that any changes are fully documented.

Immutable logs	**Description**
Tamper-evident	MongoDB Atlas provides logs for Atlas user activity and audit logs that can then be downloaded by an Atlas customer and stored in their security monitoring tools (SIEM). These logs record the activity of the users in Atlas and Atlas clusters.
Storage and retention	Audit logs are securely stored and can be retained according to configurable retention policies, ensuring they are available for the required duration for compliance purposes

Record retention and retrieval

- **Automated backups:** MongoDB Atlas provides automated backups and point-in-time recovery, ensuring that electronic records are securely stored and can be readily retrieved when needed.
- **Data retention policies:** Configurable data retention policies help organizations maintain records for the required retention period and securely delete them when no longer needed.

Access controls

- **Role-based access control (RBAC):** MongoDB Atlas provides fine-grained access control through RBAC, allowing administrators to define roles and permissions for users. This ensures that only authorized individuals can access or modify electronic records.
- **Multi-factor authentication (MFA):** MongoDB Atlas supports MFA, adding an extra layer of security by requiring multiple forms of verification before granting access to the system.

Title 21 CFR Part 11 - Subpart C - Electronic signatures

- **Unique electronic signatures:** MongoDB Atlas supports the creation and management of unique electronic signatures for each user. This includes mechanisms to ensure that electronic signatures are verifiable and legally binding.
- **Signature verification:** Electronic signatures in MongoDB Atlas are designed to be tamper-evident and verifiable, ensuring that they cannot be easily repudiated.

Electronic signatures

MongoDB Atlas supports various authentication mechanisms contributing to the implementation of electronic signatures, including:

- **User ID and Password Combinations:** SCRAM-SHA-256 and SCRAM-SHA-1.
- **LDAP Integration:** Centralized user authentication.
- **X.509 Certificates:** Cryptographic authentication.
- **OAuth 2.0:** Social logins.
- **Custom JWT:** JSON Web Tokens signed by an external system.
- **AWS IAM:** Integration with AWS IAM roles to simplify authentication and secret management.
- **OIDC:** Support for OpenID Connect (OIDC) for user authentication and authorization.

By leveraging these features, organizations can ensure that their use of MongoDB Atlas complies with Title 21 CFR Part 11, supporting the secure, reliable, and compliant management of electronic records and electronic signatures. This compliance not only helps meet regulatory requirements but also enhances overall data integrity, security, and operational efficiency.

For a detailed **matrix of responsibilities for Title 21 CFR Part 11** compliance, please **refer to Appendix.** This matrix outlines the specific requirements of the regulation and maps them to the respective responsibilities of the customer and MongoDB Atlas, providing a clear guide to ensure full compliance.

Conclusion

It is imperative for organizations in the life sciences and healthcare sectors to recognize their responsibility in maintaining compliance with GxP guidelines when utilizing MongoDB Atlas for managing sensitive electronic records. While MongoDB Atlas provides the tools and features to support compliance, it is ultimately the customer's duty to implement and manage these within their quality management and regulatory compliance frameworks.

Further reading

For additional information, see:

- MongoDB Trust Center
- MongoDB, the Healthcare Database

Appendix: 21 CFR Part 11 Responsibility Matrix

Subpart B—Electronic Records

11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Requirement	MongoDB Responsibility	Customer Responsibility

11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	• MongoDB Atlas is designed and tested to meet key IT industry standards, such as SOC, ISO, PCI, among others
	• https://www.mongodb.com/products/platform/trust#compliance.
	• MongoDB Atlas provides advanced monitoring tools to ensure consistent availability and performance of GxP systems.
	  ◦ MongoDB Atlas Performance Advisor: Analyzes slow queries and suggests indexes to improve performance.
	  ◦ Real-Time Performance Panel: Offers live metrics on database operations, CPU, memory, and I/O utilization.
		• It is the customer's duty to setup, and operate MongoDB Atlas to fulfill their specific requirements, including GxP software validation and GxP infrastructure qualification. This responsibility also extends to validation processes needed to comply with 21 CFR Part 11 standards.
		• The customer is accountable for performing the necessary operational and performance qualifications (IQ/OQ/PQ) and for carrying out the validation activities that ensure systems handling GxP workloads and electronic records are fit for their intended purposes and meet all relevant regulatory criteria.

	• Automated Backup and Restore: Ensures data availability and reliability with automated backup processes. • Atlas Triggers: Allows real-time notifications and automated workflows based on database events. • Atlas Charts: Provides data visualization for performance monitoring and analytics. • Alerts and Monitoring: Configurable alerts and monitoring dashboards to track the health and performance of the database.	
11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	• Data Export and Backup: MongoDB Atlas provides tools for exporting and backing up data, ensuring that records are complete and accurate. Automated backups are enabled for M10+ clusters, with full-copy snapshots and localized snapshot storage. • Automated Backup and Restore: Ensures data availability and reliability through continuous cloud backups, incremental snapshots, and the ability to restore from scheduled or on-demand snapshots. Backup compliance policies can be enabled to meet strict data protection requirements. • Data Integrity and Compliance: Maintains compliance with industry standards (SOC, ISO, PCI) to facilitate accurate record-keeping and data integrity. MongoDB Atlas also supports multi-region snapshot distribution for enhanced data redundancy and availability. • Supports exporting data in JSON, which is suitable for inspection,	• Configure and Use Backup Tools: Regularly use MongoDB Atlas's backup and export tools to ensure records are complete, accurate, and up-to-date. This includes configuring backups according to organizational policies and regulatory requirements. • Maintain Records: Ensure that records are stored and maintained in a manner that allows for easy retrieval and inspection by regulatory agencies. This involves regular validation and testing of backup and restore procedures. • Agency Interaction: Contact the relevant regulatory agency if there are any questions or concerns regarding the agency's ability to review and copy electronic records. Ensure that the necessary documentation and records are available for inspection. • Verify Records: Verify that the generated records meet all regulatory requirements for accuracy and completeness. This includes regular audits and reviews

	review, and copying by regulatory agencies. • Provides documentation and support to help users meet regulatory requirements, including generating accurate and complete copies of records. Specific compliance assets available in the Atlas Trust Center include: SOC 2 , ISO 27001, PCI DSS, HIPAA, GDPR, CCPA.	of data integrity and compliance with MongoDB Atlas's provided tools and guidelines.
11.10(c) Protection of Records to Enable Their Accurate and Ready Retrieval Throughout the Records Retention Period	• Maintain security controls to protect MongoDB Atlas services and infrastructure, in accordance with industry standards such as SOC 2, ISO 27001, and PCI DSS. • Implement controls to ensure data is stored and maintained completely, accurately, and in a timely manner for its specified lifespan. • Provide service level agreements (SLAs) for data and service availability and ensure these terms are monitored and met, guaranteeing a high level of uptime and reliability. • Oversee the service of data backup and recovery, ensuring automated backups are performed and maintained across multiple geographic locations to safeguard data against loss. • Provide tools such as MongoDB Atlas Performance Advisor, Real-Time Performance Panel, and Atlas Alerts for continuous monitoring and proactive risk mitigation to ensure system performance and availability. • Facilitate disaster recovery with automated failover and high availability configurations, including multi-region cluster setups to maintain service continuity in the event of failures.	• Follow MongoDB Atlas Data Security and Encryption Best Practices, including using built-in TLS encryption for data in-transit and AES-256 encryption for data at-rest to secure and protect data stored within the GxP systems hosted in MongoDB Atlas. • Implement appropriate security controls, such as role-based access control (RBAC) and identity management through LDAP/SAML, governing access to MongoDB Atlas services and GxP systems, including permissions to regulated data. • Regularly test backup processes using MongoDB Atlas's automated backup features to ensure data integrity and restore capabilities. • Define and enforce record retention policies for regulated data. • Ensure disaster recovery and business continuity processes are in place and regularly tested. • Properly configure and utilize MongoDB Atlas features, including automated backups, Performance Advisor, real-time monitoring tools, and encryption technologies, to maintain the security and availability of your data. • Architect your MongoDB Atlas usage to leverage high availability configurations, including distributing data across multiple

		geographic regions and clusters for enhanced resilience and disaster recovery capabilities.
11.10(d) Limiting System Access to Authorized Individuals	• Physical and Logical Security Policies: Maintain physical and logical security policies to restrict access to authorized individuals. This includes implementing industry-standard security controls. • Role-Based Access Control (RBAC): Use RBAC to manage permissions and ensure that access to MongoDB Atlas services is restricted to authorized users only. • Encryption: Ensure that all data in-transit and at-rest is encrypted using TLS and AES-256, respectively. • User Authentication and Authorization: Supports various methods for user authentication and authorization, including LDAP, OIDC, AWS IAM, and X.509 certificates. • IP Whitelisting and VPC Network Peering: Utilize IP whitelisting and network peering to isolate traffic from public networks for added security. Atlas supports network peering for clusters hosted on AWS, Google Cloud, and Azure. • Private Endpoints: Configure private endpoints to establish secure, private connections between your cloud provider and MongoDB Atlas, avoiding public network exposure. • Periodic Security Reviews: Continuously update security policies to address new threats and conduct periodic reviews of access rights. • Monitoring and Auditing: Use MongoDB Atlas's built-in monitoring and auditing tools,	• Access Controls: Implement and enforce appropriate access controls governing who can access MongoDB Atlas services. This includes defining user roles and permissions based on the principle of least privilege. • User Authentication Configuration: Configure and manage user authentication methods, such as LDAP, OIDC, AWS IAM, and X.509, to ensure secure and authorized access to the database. • IP Whitelisting and VPC Peering Configuration: Set up and manage IP whitelisting and network peering connections to restrict access to authorized networks and enhance security. • Regular Audits: Regularly audit access logs and user permissions to detect and address any unauthorized access attempts. • Security Best Practices: Follow MongoDB Atlas security best practices to ensure robust protection of data and access controls within GxP systems.

	such as authentication logs and database auditing, to track access and detect unauthorized attempts.	
11.10 (e) Use of secure, computer-generated time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	• Audit Trail Generation and Maintenance: MongoDB Atlas provides tools for generating and maintaining time-stamped audit trails that capture all changes to data without obscuring previous records. This includes the use of database auditing and logs. • Security and Access Control: Ensure that audit logs are secure and accessible only to authorized individuals. • Data Protection: Offer features such as automated backups and data encryption to protect the integrity and availability of audit trail data. • Offer features such as automated backups and data encryption to protect the integrity and availability of audit trail data. • Retention and Accessibility: Ensure that audit trail documentation is retained for the required period and is available for agency review and copying. MongoDB Atlas supports configurable retention policies and easy retrieval of audit logs. • Compliance and Updates: Support compliance with industry standards (SOC 2, ISO 27001, PCI DSS) by maintaining robust security controls and regular updates to address new threats and vulnerabilities.	• Audit Trail Implementation: Ensure GxP systems generate secure, immutable audit trails for all regulated electronic records. Configure and monitor these systems to capture necessary audit data. • Access Control: Implement security controls to restrict access to audit trail data and prevent disabling of audit trail functionality. This includes setting up and managing RBAC and IP whitelisting. • Backup and Verification: Test and verify data backup processes for audit trail data to ensure their integrity and availability. Regularly review backup logs and restore processes. • Record Retention Policies: Establish and enforce record retention policies that include audit trail data, ensuring they meet or exceed regulatory requirements. Use MongoDB Atlas's features to manage and retain these records appropriately.
11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.	Not applicable – this requirement applies exclusively to the regulated use of the GxP application.	• Verify that the GxP system using MongoDB Atlas enforces the permitted sequencing of steps and events according to the business process requirements.

		• Ensure the system configuration aligns with regulatory and operational requirements to prevent unauthorized actions or sequence deviations. • Regularly audit and test the system to confirm that operational checks are functioning as intended and are compliant with regulatory standards.
11.10 (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	• Not applicable – this requirement pertains solely to the regulated use of the GxP application.	• Authority Check Implementation: Implement authority checks within the GxP system to ensure that only authorized individuals can use the system, electronically sign records, access the operation or computer system input or output devices, alter records, or perform specific operations. • Access Control Configuration: Ensure the system configuration restricts access based on user roles and permissions to meet regulatory and operational requirements. • Regular Audits and Testing: Regularly audit and test the system to confirm that operational checks are functioning as intended and are compliant with regulatory standards.
11.10 (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	• Not applicable – this requirement pertains exclusively to the regulated use of the GxP application.	• Device Check Implementation: Ensure that the GxP system incorporates device checks to verify the validity of data input sources and operational instructions, as required by business process needs. • Regular Review and Validation: Regularly review and validate that device checks are functioning correctly to maintain data integrity and compliance. • Device Authentication Configuration: Configure the GxP system to recognize and authenticate valid devices or

		terminals involved in data entry or operational activities.
11.10 (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	• Offer training and certification programs to help users and administrators gain proficiency in MongoDB Atlas. • Ensure MongoDB Atlas staff are trained and certified according to industry standards, maintaining a high level of expertise and competency. This includes continuous education to keep up with new developments and best practices in database management and security.	• Implement and document comprehensive training programs for users, developers, and administrators to ensure they have the necessary skills and knowledge. • Verify that all personnel involved with electronic record/electronic signature systems possess adequate qualifications, training, and experience to perform their roles effectively. • Maintain detailed records of personnel training, qualifications, and relevant experience, including training records, job descriptions, and CVs.
11.10 (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	• Not applicable – this requirement pertains exclusively to the regulated use of the GxP application.	• Establish and document policies that hold individuals accountable for actions taken under their electronic signatures to deter record and signature falsification. • Ensure that appropriate training policies are in place, and maintain documentation of training and personnel qualifications, including training records and CVs.
11.10 (k) Use of appropriate controls over systems documentation including:	• Maintain and manage system descriptions, procedures, and technical specifications as part of systems documentation.	• Ensure that documentation such as procedures, requirements, specifications, and validation documents are properly managed and controlled under these requirements.
11.10(k)(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	• Maintain procedural controls to appropriately manage the distribution, access, and use of system documentation produced for MongoDB Atlas operations and maintenance, adhering to relevant industry standards.	• Implement procedural controls to manage the distribution, access, and use of system documentation for GxP systems hosted within MongoDB Atlas.
11.10(k)(2) Revision and Change Control Procedures to Maintain an Audit Trail that Documents Time-Sequenced Development and	• Implement and maintain documentation and change management controls to ensure an audit trail that documents the	• Ensure that documentation and change management procedures are in place, including controls to maintain an audit trail that

Modification of Systems Documentation	development and modification of systems documentation according to industry standards.	documents time-sequenced development and modification of systems documentation.

11.30 Controls for open systems

Requirement	MongoDB Responsibility	Customer Responsibility
11.30 Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	• Implement Controls: Follows SOC 2 and CCM criteria for data protection to ensure the security and confidentiality of electronic records. • Secure Communication: Uses TLS for secure internal data transmission, with all network traffic to MongoDB clusters encrypted by default. TLS cannot be disabled and the default version is TLS v1.2. • Encryption: Provides encryption at-rest using AES-256 by default to secure all volume data. Additionally, supports customer-provided encryption keys for database-level encryption using AWS KMS, Google Cloud KMS, or Azure Key Vault. • System Assessment: Assesses GxP systems to determine if they are open or closed.	• Configure Security: While MongoDB Atlas provides encryption by default, customers who wish to bring their own encryption keys must configure this according to their specific security policies. • Assess Systems: Determine if hosted GxP systems within MongoDB Atlas are open or closed based on regulatory definitions and ensure compliance. • Ensure Compliance: Verify that the use and specification of electronic signatures and encryption align with GxP requirements, utilizing the tools and features provided by MongoDB Atlas.

11.50 Signature manifestations

Requirement	MongoDB Responsibility	Customer Responsibility
11.50 (a) Signed electronic records shall contain information associated with	• Not applicable – this requirement pertains solely to the regulated use of the GxP application.	• Ensure that any GxP system supporting electronic signatures complies with the specified

the signing that clearly indicates all of the following: 11.50 (a) (1) The printed name of the signer; 11.50 (a) (2) The date and time when the signature was executed; and 11.50 (a) (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. 11.50 (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).		regulatory requirements, including capturing the printed name of the signer, the date and time of the signature, and the meaning associated with the signature. • Verify that these items are subject to the same controls as other electronic records and are included in any human-readable form of the electronic record.

11.70 Signature/record linking

Requirement	MongoDB Responsibility	Customer Responsibility
11.70 Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	• Not Applicable: This requirement applies exclusively to the regulated use of the GxP application and does not apply to MongoDB Atlas directly. Customers must ensure their GxP applications using MongoDB Atlas meet these requirements.	• Verify Compliance: Ensure that any GxP system supporting electronic signatures conforms to the specified regulatory requirements. • Define Procedures: Establish and document procedures or policies that define the use and elucidation of electronic signatures to maintain compliance.

Subpart C—Electronic Signatures

11.100 General requirements

Requirement	MongoDB Responsibility	Customer Responsibility
11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	• Unique Electronic Signatures: Ensures mechanisms are in place so that electronic signatures are unique and not reused or reassigned. MongoDB Atlas uses role-based access controls (RBAC) and unique user identifiers to maintain this uniqueness. • Identity Verification: Supports integration with identity verification services (such as LDAP and SAML) to help organizations verify individual identities before establishing electronic signatures. • Compliance Support: Provides tools and documentation to help users certify their electronic signatures as legally binding equivalents of handwritten signatures, in compliance with regulatory requirements. This includes compliance with SOC 2, ISO 27001, PCI DSS, and other relevant standards as detailed in the MongoDB Trust Center.	• Enforce Unique Signatures: Implement policies to ensure each electronic signature is unique and not reassigned, utilizing MongoDB Atlas's RBAC and user management features. • Verify Identity: Verify the identity of individuals before establishing electronic signatures, using, when necessary, the integration capabilities of MongoDB Atlas with identity verification services. • Certify Legality: Certify to the relevant agency that electronic signatures are legally binding and equivalent to handwritten signatures, using provided tools and documentation. • Submit Certifications: Submit required certifications in paper form with handwritten signatures to the appropriate agency. • Provide Additional Certification: Be prepared to provide additional certification or testimony if requested by the agency, with support from MongoDB Atlas's compliance documentation.
11.100 (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.		
11.100 (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.		
11.100 (c) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to: The Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.		
11.100 (c)(2) Persons using electronic signatures shall, upon agency request, provide additional certification		

or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.		

11.200 Electronic signature components and controls

Requirement	MongoDB Responsibility	Customer Responsibility
11.200 (a) Electronic signatures that are not based upon biometrics shall:	• Two-Factor Authentication (2FA): Supports two-factor authentication, employing at least two distinct identification components such as an identification code and password. MongoDB Atlas provides built-in support for 2FA through integrations with identity providers. • Controlled Access Management: Provides mechanisms to enforce initial signings with full components and subsequent signings with partial components during continuous access periods. This can be managed through session controls and role-based access controls (RBAC). • Authentication Management: Supports identity and access management (IAM) systems, including LDAP, OIDC, and SAML, to ensure electronic signatures are only used by their genuine owners. MongoDB Atlas also supports integration with external identity providers for robust IAM. • Access Controls: Implements strict access controls to prevent unauthorized use of electronic signatures, including IP whitelisting, VPC peering, and private endpoints. These controls ensure that only authorized users	• Configure 2FA: Ensure the configuration of two-factor authentication within MongoDB Atlas for all users, using supported identity providers and authentication methods. • Enforce Signing Protocols: Implement policies to ensure the use of all electronic signature components for initial signings and appropriate components for subsequent signings during continuous access periods. • Restrict Signature Use: Ensure that electronic signatures are used only by their genuine owners and that access control measures, such as RBAC, are in place. • Prevent Unauthorized Use: Establish procedures requiring collaboration for any unauthorized attempt to use an individual's electronic signature, leveraging MongoDB Atlas's access controls and monitoring features.
11.200 (a)(1) Employ at least two distinct identification components such as an identification code and password.		
11.200 (a)(1)(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.		
11.200 (a)(1)(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.		
11.50 (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be		

included as part of any human readable form of the electronic record (such as electronic display or printout).	can access the MongoDB Atlas clusters.	
11.200 (a)(2) Be used only by their genuine owners; and		
11.200 (a)(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.		
11.200 (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.		

11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

Requirement	MongoDB Responsibility	Customer Responsibility
11.300 (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	• Unique Credentials: Ensures mechanisms are in place to maintain the uniqueness of each identification code and password combination. MongoDB Atlas uses unique user identifiers and RBAC to enforce this uniqueness. • Periodic Review: Provides tools and supports policies for the	• Enforce Unique Credentials: Implement and enforce policies to ensure the uniqueness of each identification code and password combination, utilizing MongoDB Atlas's RBAC and user management features. • Periodic Credential Management: Regularly check, recall, or revise identification codes and
11.300 (b) Ensuring that identification code and password issuances are periodically checked, recalled, or		

revised (e.g., to cover such events as password aging). 11.300 (c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. 11.300 (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. 11.300 (3) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	periodic checking, recalling, and revising of identification codes and passwords, aligning with best practices for security management. Atlas supports pre-built and custom roles, as well as temporary user permissions. • Loss Management: Implements procedures to electronically deauthorize compromised tokens or devices and supports issuing replacements with rigorous controls. Atlas provides tools for managing and revoking user access tokens. • Transaction Safeguards: Employs safeguards to prevent unauthorized use of credentials and ensures immediate reporting of any unauthorized attempts to system security. Atlas provides real-time monitoring and alerting for suspicious activities.	passwords. Implement password policies that include aging and rotation. • Manage Lost Credentials: Follow loss management procedures to deauthorize and replace compromised tokens or devices. Utilize MongoDB Atlas's tools to manage and revoke user access tokens as necessary. • Monitor and Report: Establish transaction safeguards to detect and report unauthorized use attempts promptly, utilizing MongoDB Atlas's monitoring and alerting tools. Ensure that any incidents are reported to the appropriate system security unit and organizational management. • Test Security Devices: Conduct initial and periodic testing of devices, such as tokens or cards, that bear or generate identification codes or passwords to ensure they function properly and have not been altered. Utilize integrated identity management systems to perform these tests and ensure they meet security requirements.

Resources

For more information, please visit mongodb.com or contact us at sales@mongodb.com.
Case Studies (mongodb.com/customers)
Presentations (mongodb.com/presentations)
Free Online Training (university.mongodb.com)
Webinars and Events (mongodb.com/events)
Documentation (docs.mongodb.com)
MongoDB Atlas database as a service for MongoDB (mongodb.com/cloud)
MongoDB Enterprise Download (mongodb.com/download)

Legal Notice

This document may include certain "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, or the Securities Act, and Section 21E of the Securities Exchange Act of 1934, as amended, including statements concerning our future growth and the potential of MongoDB Atlas; and our ability to transform the global database industry and to capitalize on our market opportunity. These forward-looking statements include, but are not limited to, plans, objectives, expectations and intentions and other statements contained in this document that are not historical facts and statements identified by words such as "anticipate," "believe," "continue," "could," "estimate," "expect," "intend," "may," "plan," "project," "will," "would" or the negative or plural of these words or similar expressions or variations. These forward-looking statements reflect our current views about our plans, intentions, expectations, strategies and prospects, which are based on the information currently available to us and on assumptions we have made. Although we believe that our plans, intentions, expectations, strategies and prospects as reflected in or suggested by those forward-looking statements are reasonable, we can give no assurance that the plans, intentions, expectations or strategies will be attained or achieved. Furthermore, actual results may differ materially from those described in the forward-looking statements and are subject to a variety of assumptions, uncertainties, risks and factors that are beyond our control including, without limitation: the effects of the ongoing military conflicts between Russia and Ukraine and Israel and Hamas on our business and future operating results; economic downturns and/or the effects of rising interest rates, inflation and volatility in the global economy and financial markets on our business and future operating results; our potential failure to meet publicly announced guidance or other expectations about our business and future operating results; our limited operating history; our history of losses; failure of our platform to satisfy customer demands; the effects of increased competition; our investments in new products and our ability to introduce new features, services or enhancements; social, ethical and security issues relating to the use of new and evolving technologies, such as artificial intelligence, in our offerings or partnerships; our ability to effectively expand our sales and marketing organization; our ability to continue to build and maintain credibility with the developer community; our ability to add new customers or increase sales to our existing customers; our ability to maintain, protect, enforce and enhance our intellectual property; the effects of social, ethical and regulatory issues relating to the use of new and evolving technologies, such as artificial intelligence, in our offerings or partnerships; the growth and expansion of the market for database products and our ability to penetrate that market; our ability to integrate acquired businesses and technologies successfully or achieve the expected benefits of such acquisitions; our ability to maintain the security of our software and adequately address privacy concerns; our ability to manage our growth effectively and successfully recruit and retain additional highly-qualified personnel; and the price volatility of our common stock. These and other risks and uncertainties are more fully described in our filings with the Securities and Exchange Commission ("SEC"), including under the caption "Risk Factors" in our Annual Report on Form 10-K for the year ended January 31, 2024, filed with the SEC on March 15, 2024, and other filings and reports that we may file from time to time with the SEC. Except as required by law, we undertake no duty or obligation to update any forward-looking statements contained in this release as a result of new information, future events, changes in expectations or otherwise.