White Paper

# Trust Without Compromise: Enterprise Security, Privacy, and Compliance

## 2025 Update

When selecting a software vendor, you need to know you're working with a partner capable of meeting your enterprise requirements and regulatory obligations. Quality-first principles are woven into the fabric of our organization and this paper outlines how CRIO meets and exceeds industry standards when it comes to data protection and security.

Additional information such as policies, procedures and artifacts are beyond the scope of this document, and can be made available through CRIO's Corporate QA & Compliance department.

CRIO is entrusted by over 2,500 sites worldwide with their mission-critical data. As a service provider, we go well beyond regulatory requirements to keep your data secure, private, redundant and accessible. We also partner with our clients to ensure they utilize our software in a manner that is compliant with applicable regulatory requirements, including Good Clinical Practice (ICH E6), FDA's Regulation on electronic records and electronic signatures (21 CFR Part 11), EU's guidelines on computerized systems (Annex 11), HIPAA, and the EU General Data Protection Regulation (GDPR).

### EXPERIENCE AS THE LEADING ESOURCE PROVIDER

- 2500 Sites
- 6000 Protocols
- 3000 Sponsors
- 5M Patients
- 30 Countries

### ENTERPRISE GRADE SECURITY & COMPLIANCE

- ISO 27001 and SOC 2 compliant Google Cloud Platform (GCP) data centers around the globe, keeping PHI local
- Continuous data back-up with point-in-time recovery and zero Recovery Point Objective (RPO) (i.e. zero data loss)
- Data encrypted in transit and at rest
- Over 99.9% Uptime recorded
- No scheduled downtime with seamless deployment
- Regularly scheduled third-party penetration testing
- Externally validated regulatory compliance audits
- 100% FDA audit track record
- Validation, test scripts, and controlled documents continuously available and downloadable from document center
- Multi-Factor Authentication (MFA) and Single Sign On (SSO)

## SECURE AND PRIVATE HOSTING AND INFRASTRUCTURE CONTROLS:

CRIO hosts its infrastructure within secure private networks via the Google Cloud Platform (GCP). Both physical and digital measures are in place to protect CRIO's infrastructure. Data centers are SOC 2 and ISO 27001 certified and utilize biometric authentication. Firewalls, access control policies, and security monitoring systems are enabled on each machine to protect against malicious activity. All data are encrypted at rest (256-bit AES) and in transit (via Transport Layer Security [TLS]). CRIO conducts regular penetration tests with third party vendors to verify its security measures.

## Next Level Security:

As part of our ongoing commitment to protecting sensitive data and ensuring the highest standards of security, CRIO has implemented the Google Security Command Center (SCC) Enterprise—Google Cloud's most advanced security platform. SCC Enterprise equips CRIO with enhanced tools to detect, investigate, and respond to security threats quickly and effectively.

With SCC Enterprise, CRIO has advanced **SIEM** and **SOAR** capabilities—tools that help us spot security threats faster and respond to them automatically. These systems continuously monitor activity across our cloud environment, looking for unusual behavior or risks such as unauthorized access or misconfigured systems.

- **SIEM** (Security Information and Event Management) collects and analyzes security data from across our systems in real time. It helps us connect the dots between different events—like a login from an unusual location and a sudden change in system permissions—to identify threats early.

- **SOAR** (Security Orchestration, Automation, and Response) takes that a step further by allowing us to automate the response. For example, if SCC detects suspicious activity, it can automatically limit access, alert our security team, and begin an investigation—often within seconds.

**What this means for CRIO customers**

CRIO customers trust us to handle sensitive research, patient, and partner data. Protecting this information is not just a priority—it's a responsibility. SCC Enterprise allows us to:

- Reduce risk through faster threat detection and automated responses.
- Meet and exceed compliance requirements by maintaining full visibility and audit trails.
- Build trust by demonstrating that our cloud environments are managed with enterprise-grade security.

This ensures we are not only staying ahead of evolving cyber threats, but also aligning with the security expectations of our customers, regulators, and partners. It's a major step forward in making sure our security practices are as advanced and reliable as the solutions we deliver.

## Multi-Factor Authentication:

From an authentication perspective, CRIO enables customers to utilize multi-factor authentication (MFA). Using MFA, the legitimacy of the user attempting access to the CRIO application is confirmed and provides a robust framework for further securing our customers' data. As a part of this process, the end user is prompted to provide a verification code that is provided by CRIO directly to the end user's mobile device. Once the verification code is entered into the CRIO application and confirmed, the user gains access.

## Single Sign-On (SSO):

Organizations can also take advantage of CRIO's SSO. SSO simplifies access for users by allowing them to log in once with a single set of credentials to access multiple applications and services. This significantly enhances the user experience by eliminating the need to remember numerous usernames and passwords, which in turn reduces password fatigue. By consolidating authentication, SSO also strengthens security by centralizing control and making it easier to enforce robust password policies and multi-factor authentication across all integrated systems.

## Data Backup and Assurance:

CRIO's backup and recovery mechanism can restore data to the second utilizing Google's point-in-time recovery. This recovery capability extends to any server outages that occurred in the trailing seven (7) days. A Recovery Point Objective (RPO) of zero (0) hours out can be achieved for up to seven days. After day seven, CRIO maintains incremental backups every six (6) hours out to 60 days, and then full backups every 24 hours out to one (1) year. In addition to this, CRIO ensures a Recovery Time Objective (RTO) of no greater than six (6) hours.

## Global Infrastructure:

By using servers located within a customer's specific region, CRIO ensures their data never crosses national or regional borders (where applicable). This approach helps customers comply with international data protection laws that require data to be stored locally.

The focus on regional data hosting provides a high level of privacy and security, allowing sites to safely store sensitive information such as addresses, Social Security numbers, phone numbers, and medical records.

## Dual-Database Structure and PHI Protection (CRIO Reviewer):

The dual database architecture in CRIO's eSource system separates site source data from sponsor-accessible data to enhance security and privacy. The site database contains the full source data, including personal identifiers, which only site users can access and control. The sponsor database holds de-identified or limited data extracted from the site database, allowing sponsors to perform monitoring and oversight without accessing protected health information (PHI). This separation ensures compliance with privacy regulations and maintains site ownership of source data while enabling sponsors to fulfill their regulatory responsibilities. Access controls and role-based permissions govern user rights within each database, minimizing the risk of unauthorized data exposure. The dual database design supports clear data ownership, privacy protection, and operational efficiency in clinical trials.

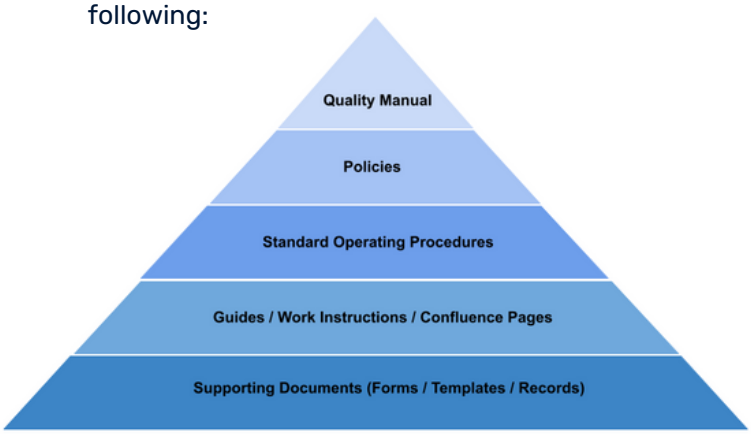
## Seamless Deployment, Product Stability & Monitoring:

CRIO has implemented session serialization to enable seamless product deployments and effectively remove the need for "maintenance windows". Session serialization means that individual users are no longer tied to a specific application server for the entirety of their session. CRIO can now deploy changes to the system without any downtime.
With this flexibility, CRIO can immediately deploy emergency patches and implement bug fixes more frequently - without requiring users to log off the system - enabling a truly seamless deployment. Thus, there is no need for CRIO to notify clients in advance of scheduled maintenance, or for our clients to have to plan around it.
Because of this, CRIO is able to implement phased releases. Instead of releasing a major enhancement across the board, CRIO can introduce the enhancement to a subset of users, monitor impact, then either move toward full release or pull back. Any adversely affected users can simply refresh their browser to access the prior codebase, thus mitigating impact. This is known in the software development industry as blue-green deployment.
Additionally, CRIO is leveraging Application Performance Monitoring (APM) software; APM software sits on top of our code and monitors performance. With APM software, CRIO can proactively monitor and remediate potential problems and more quickly identify and troubleshoot post-release issues. This shortens the time it takes to perform root cause diagnostics, thus expediting bug fixes.

## Compliant with Regulations:

CRIO's full time dedicated head of Corporate QA and Compliance, in consultation with leading external compliance experts, has developed a comprehensive series of SOPs and matrices to demonstrate compliance with ICH E6, 21 CFR Part 11, Annex 11, HIPAA, CCPA, GDPR and other relevant regulatory frameworks. Our system is internally validated and externally certified, and we provide our clients with all necessary documents to evidence this.

Further, CRIO has adopted a fully realized quality management system (QMS), in alignment with best practices found in organizations that have implemented ISO 9001.
Additionally, CRIO maintains a robust vendor qualification program and product readiness approach. Through CRIO's QMS, we assure that all aspects of our business are governed under a well-structured system that is comprised of the following:




Finally, we recognize that how our users validate and utilize our system is ultimately what is critical for compliance. To that end, we take a proactive approach, providing our clients with draft SOPs built around our unique processes. All of our critical validation documents, compliance matrices and other documents are available inside the Document Download Center. If CRIO clients are being notified of an upcoming audit / inspection by a regulatory agency, CRIO can share best practice suggestions and learnings from our extensive - and clean - regulatory audit history.

## Ensuring Quality Vendors

CRIO's vendor qualification program ensures a full accounting of CRIO's vendors and puts into place a qualification program to ensure that these vendors comply with regulatory requirements and CRIO's business requirements. Each appropriate vendor is assessed and a qualification assessment is carried out. As a result of this assessment, any needed remediation is identified and monitored to completion.

## Product Readiness

CRIO follows a product readiness approach for product releases. This readiness approach ensures that all aspects of the business are ready to support a successful rollout.

A detailed readiness checklist and planning approach is followed and monitored on a week-to-week basis to ensure that operations, technical support, information technology, and sales and marketing are in alignment and ready for the release.

Release readiness is part of the overall process of developing and deploying software – it's effectively an extension of the software development process. Release readiness plans prepare CRIO's customer-facing team and minimize the risk of encountering any major product release incidents. Readiness does not stop with CRIO and can include customers through CRIO's voluntary Beta Testing Program and other forms of pre-release assessments.

## Data Analytics

CRIO utilizes Google's business intelligence software (Looker) to provide customized reporting to our clients. APIs are in place for third party patient recruitment apps and CRM systems to send patient leads in, schedule appointments, and manage study & patient data. We've built out APIs for feasibility management, MS365 Outlook scheduling, EDC and IRT integration and EHR integration, and CRIO will continue to invest in our capacity to send and receive data across the eClinical landscape.

We recognize that many of our enterprise clients have their own business intelligence tools and want direct access to their data. To that end, we've created a replica reporting database, updated in real time, and managed through Bigquery - a database service managed by Google that is optimized for data querying. This option offers real-time, continuous and secure access to all of the client's data tables, along with the joinder relationships - an access level well above conventional reporting and/or API solutions.

## Validation & Process Documents for Sites

CRIO provides customers with access to core system validation documentation, which is essential for demonstrating system compliance during regulatory inspections. This documentation verifies that the system has been validated and performs as intended.

In addition to core validation materials, CRIO offers example standard operating procedures (SOPs) that can be tailored to a site's specific needs for managing clinical trials within the CRIO application. These resources are available through CRIO's site-facing academy and can be adapted by customers, as needed.

## Certifications (External)

CRIO utilizes Google Cloud Platform (GCP) as its hosting provider. GCP's infrastructure complies with internationally recognized security frameworks, including SOC 2 and ISO/IEC 27001. SOC 2 certification confirms that GCP securely manages data to protect organizational interests and customer privacy, while ISO/IEC 27001 certification demonstrates that GCP maintains a formal, independently verified information security management system (ISMS) to ensure ongoing protection and operational control.

## CRIO Management System

CRIO has implemented the CRIO Management System (CMS). The CMS is a framework of policies, procedures and processes used by CRIO to ensure that it can fulfill all the tasks required to achieve its strategic objectives. Its primary focus is on measuring what matters for the business and our customers and is aimed at continuous improvement.

Our CMS framework is built on best-in-class quality principles, and features monthly and quarterly KPI tracking, fact-based diagnostics, concrete improvement plans, and cross-functional governance.

In Summary, the CMS:

- Provides a strategy deployment framework that focuses and aligns activities to allow quick response
- Recognizes employees' individuality, provides clear responsibilities, and fosters a consultative environment
- Enables CRIO to determine episodic versus systemic issues and allows for appropriate response
- Measures key performance indicators (KPIs) that matter and ensures action plans are implemented and aimed at continuous improvement

CRIO management has appointed the head of the Corporate QA & Compliance department to oversee the CMS. This appointment ensures a dedicated focus on maintaining high standards of quality and compliance across CRIO, including a consistent effort to drive continuous improvement throughout the organization. The responsibility and authority of this role further ensures that CRIO senior leadership is kept informed at periodic intervals on the progress of initiatives and issues within the organization.

## Conclusion

The measures outlined in this paper have been scrutinized in client audits of CRIO and in regulatory inspections of our clients on a global scale. To date, no regulatory finding has been directly attributed to the design, use, or configuration of the CRIO system.

Our clients entrust us with their sensitive data, and we regard this as a fundamental responsibility. Every member of the CRIO team, along with our partner organizations, is accountable for maintaining the highest standards of data protection, security, and accessibility to ensure reliable service delivery.