clinicalresearch.io

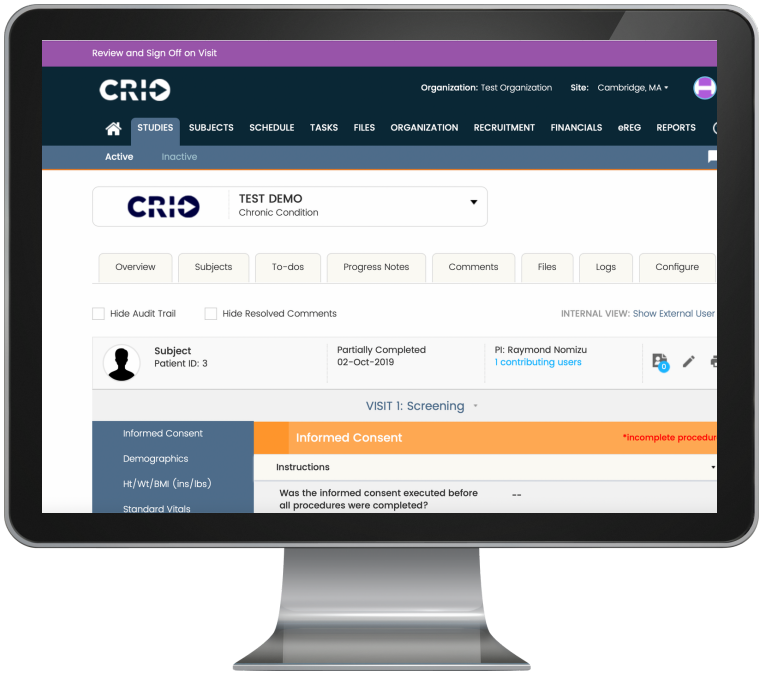
sales@clinicalresearch.io
www.clinicalresearch.io
(617) 302-9845

ENTERPRISE GRADE

When selecting a software vendor, you need to know you're working with a partner capable of meeting your enterprise requirements and regulatory obligations. This guide describes, at a high level, some of CRIO's best practices that differentiate us from other vendors you may be considering. Additional information such as policies, procedures and artifacts are beyond the scope of this document, and can be made available through our Corporate Quality department.

CRIO is entrusted by over 2,000 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 ICH E6, 21 CFR Part 11, Annex 11, HIPAA, CCPA and GDPR.

EXPERIENCE AS THE *LEADING* ESOURCE PROVIDER



2,000 +
Clinical Research Sites

350,000+
Subjects

17
Countries

800+
Sponsors

6,000+
Protocols

03

ENTERPRISE GRADE SECURITY & COMPLIANCE

- IISO 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)

CRIO complies with the major global regulatory standards governing clinical research:

GDPR

HIPAA

FDA 21 CFR Part 11

EU Annex 11

China's Personal Information Security Specification

SECURE & 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 is encrypted at rest and in transit (256-bit AES). CRIO conducts regular penetration tests with third party vendors to validate its security policies and measures.

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) options are also available.

Data Backup & Assurance

CRIO's backup and recovery process has been updated so that we can ensure that in the unlikely event our servers experience an outage, we can restore data to the second - i.e., essentially at zero data loss. This "point in time" recovery capability extends to any server outages that occurred in the trailing 7 days. This point-in-time recovery provides CRIO customers with a Recovery Point Objective (RPO) of 0 hours out to 7 days. After day 7, CRIO maintains incremental backups every 6 hours out to 60 days, and then full backups every 24 hours out to 1 year. In addition to this, CRIO ensures a Recovery Time Objective (RTO) of no greater than 6 hours.

EMBRACED BY SITES WORLDWIDE

NORTH AMERICA

United States
Canada
Dominican Republic
Mexico

CENTRAL/ SOUTH AMERICA

Brazil
Chile
Costa Rica

APAC

Australia

EUROPE

Germany
Hungary
Ireland
Spain
United Kingston
Ukraine

AFRICA

Kenya
South Africa
Uganda

Global Infrastructure

Customers can host their data on a server located within their region, ensuring that data does not move across national or regional jurisdictions – through this, CRIO complies with international data protection laws that restrict data from being stored in other countries. This level of privacy allows sites to store extensive personal information such as addresses, social security information, phone numbers and sensitive medical information. CRIO currently has servers in the United States, Canada, Germany, and Australia. Importantly, only anonymized study level data is sent to our Reviewer application, which is the application used by sponsors, CROs and other personnel who need to review, query, lock and/or extract data. This dual-database architecture is unique in the industry and ensures sites have direct control over their own source data.

Seamless Deployment, Product Stability & Monitoring

CRIO has implemented session serialization to enable seamless product deployments. 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.

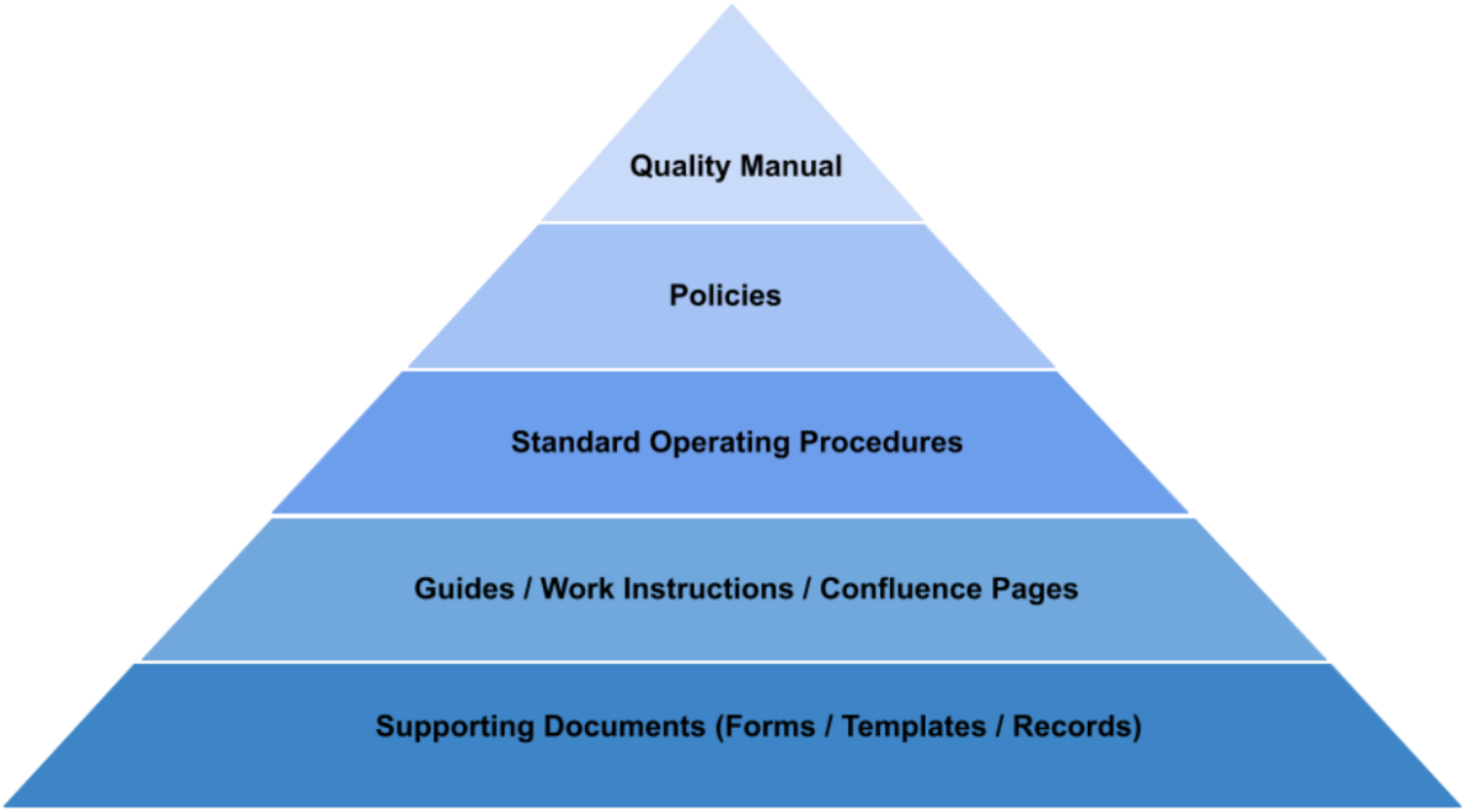
Because of this, CRIO is able to implement phased releases. Instead of releasing a major enhancement across the board, CRIO can introduce the enhancement to a subset of users, monitor impact, then either move toward full release or pull back. Any adversely affected users can simply refresh their browser to access the prior codebase, thus mitigating impact. This is known in the software development industry as blue-green deployment.

CRIO has implemented 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 Corporate QA and Compliance Director, 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 and GDPR. Our system is internally validated and externally certified, and we provide you with all necessary documents to evidence this.

Further, CRIO has adopted a fully realized quality management system (QMS), vendor qualification program and product readiness approach. Through CRIO's QMS, we assure that all aspects of our business our 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 suggested test scripts and draft SOPs built around our unique processes. All of our critical validation documents, compliance matrices and other documents are downloadable in our Document Download Center. If your site is getting audited by the FDA, we can share best practice suggestions and learnings from our extensive - and clean - FDA 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 has implemented 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 ready for the release.

Release readiness gets everyone on the same page and aims to make each software release smooth and painless. Release readiness is baked into the overall process of developing and deploying software – it's effectively an extension of the software development process. The use of release readiness plans is aimed at delighting customers, preparing CRIO's customer-facing team, and avoiding major product release incidents. Readiness does not stop with CRIO and can include CRIO's customers through Beta Testing and other forms of prerelease assessment.

Data Analytics

We utilize third party business intelligence software (Looker) to provide customized reporting to our clients. We also have APIs in place for third party patient recruitment apps and CRM systems to send patient leads in, schedule appointments, and manage study and patient data. We've built out APIs for feasibility management, MSO365 Outlook scheduling, EDC and IRT integration and EHR integration, and 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 access to core system validation documentation for our customers. In the event of a regulatory inspection, having access to this documentation is important in order to demonstrate that the system has been validated and demonstrates that it functions as purported. Beyond CRIO's core system validation, CRIO has developed example standard operating procedures/processes that can be used, modified specifically to the site and then adopted for managing clinical trials using CRIO's application. These procedures and processes are available through CRIO's site facing academy and make available, as needed, these documents for our customers to use as appropriate.

Certifications (External)

CRIO is focused on providing our customers with computing environments that have been tested and proven to meet exacting standards in and around physical and logical security, access to redundant internet protocols, backup methodologies which ensure safeguarded

data, redundant power sources managed through uninterrupted power supplies (UPS), generators and other capabilities which are world class. CRIO has selected a provider (Google Cloud Platform - GCP) that ensures that their hosting environment meets the expectations of standards established for world-class organizations. GCP meets the Systems and Organizations Control (SOC) II and ISO 27001 standards for cloud based hosting. SOC II ensures that GCP securely manages data to protect the interests of our organization and the privacy of its customers. ISO 27001 demonstrates and shows that GCP is serious about protecting their customers' data and that an independent certifying body has confirmed that the organization is in 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

Enterprise Grade Vendor Checklist

When running any trial – decentralized, virtual, hybrid, or site-based – be sure to choose an organization and a system that is confident and positioned for long term support and growth. Using the checklist below will help you discover the application and organizational must-haves when searching for the right tools to use for your trial needs.

Organizational & System Capabilities

☐ Session Serialization to enable more performant and up to date environments, with rapid releases of system fixes without interrupting user sessions	☐ ISO 27001 and SOC 2 Compliant Hosting Infrastructure
☐ Multi-Factor Authentication	☐ Robust and extensible APIs to allow for incorporation of 3rd party data (EMR, Lab, IRT, etc.)
☐ Ease of Configuration - Can your organization be self-sufficient in building out and maintaining their own studies? CRIO enables this.	☐ 24x7x365 Technical Support Help Desk
☐ Remote Monitoring - Access to source data to allow for monitors to ensure ALCOA+ is being followed	☐ Well-Defined Product Readiness to ensure that our internal team and clients are knowledgeable and ready to accept upcoming product releases
☐ Overnight EDC Data Entry Services	☐ Overflow study design and development support
☐ Regionally based data storage to ensure sites have continuous control over their source and all PHI stays resident in that geography	☐ Dedicated Implementation and Customer Success Personnel
☐ Reporting - Looker or BigQuery (direct data access) Options	☐ Ability to support telehealth
☐ Ability to support home based clinical trial research (mobile research nurse)	☐ Ability to support electronic patient reported outcomes (ePRO)
☐ Remote and site-based eConsent	