White Paper

Ingenuity® Variant Analysis™ Hosted Infrastructure Security, HIPAA and Safe Harbor Compliance, and Data Privacy

This white paper describes the hosting capabilities and infrastructure used by QIAGEN®, to assure high availability, security and data privacy, and HIPAA Compliance for Variant Analysis and customer data.

Summary

QIAGEN applications are hosted in a Tier 1 data center strategically located to assure world-class performance, continuous availability, and highest levels of securityfor our customers. The data center is SAS 70 type II / SSAE 16 Type II compliant, certified annually by external auditors (SSAE 16 Type II audit report available upon request).

Exceed industry standards

QIAGEN provides capabilities intended to exceed industry standards. The data center footprint extends worldwide, with a presence in 17 key markets in North America, Europe, and Asia. The infrastructure has been architected for built-in redundancy with a second location for disaster recovery that is quarterly tested for failover capabilities. The disaster recovery site is a replicated and mirrored instance of the production environment and geographically located to sustain catastrophic failure.

Full redundancy

The hosting environment provides fully redundant Internet connections and network infrastructure and is designed to support QIAGEN's rapid growth and expanding need for hosting options. The data center facility provides N+1 minimum redundancy with an uninterruptable power source (UPS) as well as additional power generation, cooling, and humidity control.

Advanced physical security

The highly secure facility provides 24x7 guarded physical security 365 days a year for the complex, which is monitored by closed circuit recorded video. Access to the facility is protected with hand geometry biometric controls, retina scans, and multi-level background checks for physical access to onsite visitors. All visitors are required to log in and out of the data center and are also granted card key access only to designated areas of the facility.

HIPAA Compliance

QIAGEN is focused on securing customer data (Patient Health Information) and assuring all privacy and compliance measures are enforced. All data is 256 bit AES encrypted in-transit and at-rest. The Ingenuity Variant Analysis Application, the QIAGEN Clinical Insight Application, and hosted infrastructure are HIPAA certified and in compliance with the Code of Federal Regulation (CFR 45). Our Policies, Corrective Action Plans (CAPS), and Remediation requirements have been certified by an external audit firm that will conduct quarterly audits to ensure adherence to all compliance requirements and policy updates. The QIAGEN audit emphasizes the strict adherence to the Administrative, Technical, and Physical Safeguards of the HIPAA policy mandates.

Safe Harbor Compliance

QIAGEN is a certified member of the Safe Harbor initiative and in compliance with the US-EU and US-Swiss Safe Harbor Principles. QIAGEN has certified its privacy practices as consistent and compliant with the US-EU Safe Harbor Framework and US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.

QIAGEN has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view our certification page, please visit **http://www.export.gov/safeharbor/.** Data is managed with respect and integrity and is only accessible by those with required business justification. QIAGEN supports and maintains internal and external policies that enforce the primary components of the Safe Harbor Framework.

For more information on QIAGEN's Privacy policy, please visit **http://www.ingenuity.com/company/privacy.html**.

Meshed Architecture

The hosted environment is built on a full-meshed network architecture based on multiple redundant enterprise class routers, switches, firewalls, and load balancers. Servers and enterprise storage have been deployed in a multi-node capacity to withstand failures and deliver seamless uptime. Multiple carriers provide Internet services with redundant routes into the data center. Acceleration services are also used for caching and SSL of all QIAGEN content and customer data. All administration services are logged and originate from individual user accounts that have defined access controls and credentials based on data privacy and business justification. Logs are recorded and monitored, and all access follows a strict change management process and best practices. The environment is monitored 24x7 from multiple end points internally and externally by third-party services.

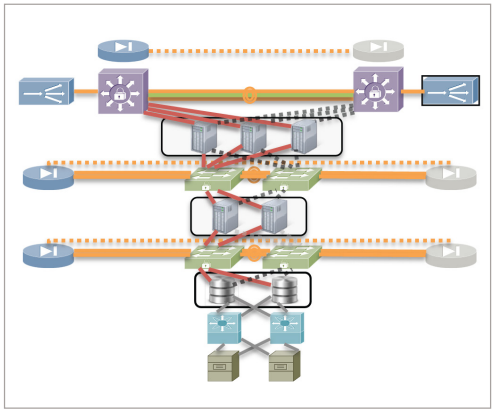

Figure 2. Full-meshed network architecture.

QIAGEN Operations Management Solutions

QIAGEN leverages various industry-leading solutions for systems management, monitoring, and automation as shown in the table below.

Services	Solutions
Single sign-on and user management	Ingenuity SSO
Database monitoring and management services	Oracle® Enterprise Manager / Data Guard
Server monitoring and reporting	Nagios®, GroundWork, Dotcom
Storage area network and storage management	EMC Navisphere and Snapview

QIAGEN Data Protection Practices

In order to secure customer data (Patient Health Information), QIAGEN has put in placethe following data protection practices.

- **Physical security.** Servers reside at a high-security facility utilizing 24-hour guards, picture ID access, proximity cards, video surveillance, and a locked dedicated cage with restricted access.
- **Perimeter defense.** QIAGEN protects its network perimeter with firewalls and monitors the system with intrusion detection systems. Logs are proactively monitored to identify security threats.

- **Internal security.** All data is protected against compromise from server-toserver communication with multiple internal firewall layers, network address translation, port redirection, IP masquerading, and non-routable addressing.
- **Data encryption.** To shield in-transit data sessions from eavesdropping attacks, QIAGEN employs 256-bit AES SSL encryption with VeriSign web server digital SSL certificates. All PHI data is 256-bit AES encrypted at-rest while stored on QIAGEN infrastructure. QIAGEN enforces strong data retention policies and ensures all customer data can and will be permanently deleted from the environment.
- **User authentication.** User authentication requires username and password for application login. Password creation requirements: (8 character minimum, at least 1 number and letter, no dollar sign $) User is also provided a "password strength meter" when selecting password. Accounts are locked following (5) failed login attempts.
- **Data and database security.** QIAGEN deploys redundant disk arrays to protect the Ingenuity Variant Analysis and QIAGEN Clinical Insight systems from disk failure and delayed data replication for protection from data corruption and disasters. QIAGEN's proprietary database security model prevents cross-account data leakage.
- **Server operating system security.** QIAGEN hardens all servers by removing unnecessary accounts, services, protocols, and processes. Patch levels are maintained according to recommendations of its vendors.
- **Data backups.** The QIAGEN hosting system replicates data to local and remote disks. Multiple copies of all (PHI) data are encrypted with 256-bit AES standards. Rotational incremental and full backups take place multiple times per day.

Delivering High Availability and Backup/Disaster Recovery

The QIAGEN hosted environment delivers its services with more than 50 redundant, load-balanced servers. The system provides failover for all applications with multi-node redundancy to protect against software and hardware failure. It also includes hot database backup and replication with Oracle Cluster and Data Guard sync technologies. Enterprise class arrays provide redundant, high-availability data storage. Backup and disaster recovery are provided by the following processes, which assure data can be immediately restored in case of failure:

- Clone to array and backup to array
- Continuous asynchronous local replication to provide multiple onsite copies
- Two copies of all data stored onsite for immediate access