Assertion of Management of QHR Technologies

We are responsible for designing, implementing, operating, and maintaining effective controls within the QHR Technologies (QHR) Accuro EMR System (the “System” or “Accuro”) throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that QHR’s service commitments and system requirements for the System relevant to security and availability were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that QHR's service commitments and system requirements for the System were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). QHR's objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements for the System relevant to the applicable trust services criteria. The principal service commitments and system requirements for the System related to the applicable trust services criteria are also presented in attachment A.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that QHR's service commitments and system requirements were achieved based on the applicable trust services criteria.

QHR Technologies

Alan McNaughton
Director of Technology Operations
QHR Technologies
Kelowna, BC
February 28, 2022

GrantThornton

Grant Thornton LLP
Suite 1600, 333 Seymour Street
Vancouver, BC
V6B 0A4
T +1 780 401 8240
F +1 780 422-7114
www.GrantThornton.ca

Independent Service Auditors

To: QHR Technologies

Scope

We have examined QHR Technologies' (QHR's) accompanying assertion titled "Assertion of Management of QHR Technologies" (the "Assertion") that the, controls within QHR Accuro EMR System (the "System" or "Accuro") were effective, throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that QHR's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service organization's responsibilities

QHR is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that QHR's service commitments and system requirements were achieved. QHR has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, QHR is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient to provide a reasonable basis for our opinion.

Our examination included:

1. obtaining an understanding of the system and the service organization's service commitments and system requirements.

2. Assessing the risks that controls were not effective to achieve QHR's service commitments and system requirements based on the applicable trust services criteria

3. Performing procedures to obtain evidence about whether controls within the system were effective to achieve QHR's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within QHR's Accuro EMR System were effective throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

GRANT THORNTON LLP

Grant Thornton LLP

Chartered Professional Accountants

Vancouver, BC

February 28, 2022

Attachment A:

QHR Technologies' Description of Its Accuro EMR System

1. Services Provided

QHR offers Accuro, which is an electronic medical records (EMR) software as a service (SaaS). This service allows clients to store Personal Health Information about their patients electronically and communicate electronically with other entities such as Lab Vendors or Specialists. Accuro can be implemented locally on a client's site, or through the hosted solution Accuro Hosted (Accuro ASP or Accuro Cloud). Accuro Hosted is hosted at third-party data centres across Canada and is available through the Citrix gateway. It requires a web connection to access it and is offered on a subscription basis.

QHR provides installation, onboarding and training services to get its clients onboard. QHR also provides client support for its clients by email, phone, or in-person. We respond in real-time to client inquiries.

QHR also offers other products and services which follow best practices and processes as laid out in the control descriptions. However, they are not in scope for this report.

2. Principal Service Commitments and System Requirements

QHR designs controls to meet service and system objectives for Accuro. All processes used to support Accuro work together to achieve service commitments made to user entities.

Principle service commitments include, but are not limited to, the following:

- Implement information security standards to ensure data remains secure, including restricting access to applicable roles
- Monitored uptime targets for Accuro Hosted (the hosted Accuro solution)
- Provide regular software updates that have gone through the software development life cycle, including rigorous testing and approval prior to release
- 24/7/365 Client Support
- Abide by all applicable laws and regulations for the use, disclosure, retention, and destruction of data under QHR's control

QHR's Privacy Policies are available to all user entities on the external QHR website. These policies in combination with the License Service Agreement (LSA), the Information Manager Agreement (IMA), internal policies and procedures, and system design documentation establish QHR's security and availability commitments.

Documented policies define system requirements needed to meet service commitments for security and availability. These include policies around how the product is designed and developed, how the system operates, how the internal business systems and networks are managed and how employees are hired and trained. Procedures and work instructions have also been documented for specific processes related to security and availability. All staff have access to internal documentation required to perform their role and receive applicable training.

3. Components of the System Used to Provide the Services

3.1 Infrastructure

QHR's Accuro EMR services are provided using third-party operated data centers located in Canada at several locations: Kelowna, BC, Toronto, ON and Montreal, QC. The data centers are operated by TeraGo and eStruxture

Client data that is entered into the Accuro EMR platform is stored at one of the secure data centres and is not stored at QHR's office locations.

3.1.1 Physical Security

All locations housing QHR's production systems are hardened and require two-factor authentication for access. All personnel are required to wear badges in a visible location and any guest to the third-party data centers is required to show valid, picture ID prior to access. Mantraps are in place to act as additional security mitigation strategies.

3.1.2 Data Center

Data Center Power – the third-party data centers are equipped with an Uninterruptible Power Supply (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The UPS power provides instantaneous failover in the event of a primary UPS failure. The UPS systems are inspected on a regular basis. Stand-by power generators are in place to mitigate the risk of long-term utility power failures.

Generators are tested periodically and maintained to provide assurance of appropriate operability in the event of an emergency.

Data Center Cooling – the third-party data center and UPS rooms are equipped with cooling units that provide consistent temperature and humidity within the areas. The cooling units are inspected regularly, and air filters are changed as needed.

Data Center Fire Detection and Suppression – smoke and heat detection sensors are installed in the ceiling of the third-party data centers areas. Fire detection equipment is monitored remotely 24/7/365. Suppression devices include handheld extinguishers and a fixed sprinkler system. Fire detection and suppression features include:

3.1.3 Network Perimeter Security

The following are complementary types of network security perimeter devices used by QHR on its network to defend Internet-accessible systems:

- Router
- Firewall
- Demilitarized Zone (DMZ)
- Intrusion Detection and Prevention System (IDS/IPS)

3.1.4 Network Equipment

Switches and firewalls are essential components of the network and control much of QHR's communications. The devices are utilized to divide the network into segments and control traffic flow from one segment to another. Segmenting the network in this manner adds additional levels of security due to the application of traffic flow rules configured on each of the devices. All network equipment is located in secure, locked rooms to prevent tampering. Logical access to the devices is protected by unique usernames and passwords and can only be utilized by authorized personnel. Additionally, QHR utilizes network monitoring tools to proactively monitor its network for outages.

3.1.5 Firewall

QHR incorporates a firewall at the perimeter of its network to protect against threats from the Internet.

The firewall device provides user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of security and networking services in a unified threat management platform including:

- Application-aware firewall services
- Site-to-site and remote access Internet Protocol Security (IPSec)
- Intelligent networking services
- Flexible management solutions

3.1.6 DMZ

Network computers exposed to the Internet can subject the entire network to hacker attacks. This can lead to compromised data, viruses, and other types of malicious acts that could damage QHR's credibility and operations.

A DMZ has been established to isolate QHR's computers from the Internet. A DMZ is a small network of computers exposed to the external world (Internet). Identifiable security incidents occurring on the DMZ are evaluated, and steps are taken to mitigate those issues and further reduce the risk of breaches of the DMZ.

3.1.7 Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)

QHR utilizes firewalls to monitor its network perimeters for threats using an IDS/IPS. Alerting is configured to notify QHR administrators if predefined thresholds are met or exceeded.

An IDS detects unwanted manipulations to computer systems, mainly through the Internet. The manipulations may take the form of attacks by hackers.

3.2 Software

The Accuro EMR platform consists of:

- Software created and maintained by QHR that is either accessed through Citrix from the client's workstation, or locally on a client's site
- Third party software that is installed and operates on the Accuro Servers
- The operating system used on Accuro Server

3.3 People

QHR is divided into several departments:

- Product Development is responsible for the design and development of Accuro EMR and works with the various teams within that department that are responsible for leading the design and refinement of user interface features and elements and working with the Software Development team to successfully implement these designs within the Accuro software. The Privacy office resides within the Product Development department.
- The Finance department manages the daily administrative activities of Accuro, including accounting, and financial analysis functions.
- The Sales & Marketing department promotes Accuro EMR to prospective clients and manages these organizations throughout the sales cycle. Product Development is responsible for the design and development of Accuro EMR and works with the various teams within that department that are responsible for leading the design and refinement of user interface features and elements and working with the Software Development team to successfully implement these designs within the Accuro software.
- The Implementations department works with new clients to get them integrated and started on Accuro.
- The Client Services departments work with clients to ensure that they are optimizing their Accuro usage and are responsible for providing a helpdesk that supports clients with using the Accuro software and troubleshooting issues.

- Technology includes the Technical operations, Infrastructure, and employee support for the equipment (hardware and software) required for employees to perform their defined roles within the organization. Technical operations builds and maintains the infrastructure on which Accuro EMR software and services are delivered. The Information Security team resides within the Technology department. The GRC team resides within the Technology department.
- The Administration and Employee Support Services teams are responsible for maintaining physical security at all QHR office locations.

3.4 Procedures

The Security and GRC Teams are responsible for developing and implementing the procedures required to maintain the security of the data center servers in line with QHR's Policies. The teams have implemented procedures for:

- Hardware Decommissioning
- Change Management
- Data Centres
- Data Retention
- Employee Onboarding, Disabling and Termination
- Firewall Management
- Incident Management
- Password Security
- Penetration Testing
- Secure Data Transfer
- Vulnerability Management

Documentation is reviewed, updated, and approved by management on a regular basis.

3.4.1 Human Resources

QHR's hiring practices include a definition of roles and responsibilities, use of various recruiting methods to find the best candidates, and a multi-step process of interviews, orientations and ongoing training.

All staff have regular reviews with their direct reporting manager that includes reviewing skills requirements and evaluation of performance. As well, all staff attend training on policies and procedures, including security and availability processes and obligations.

3.4.2 Change Management

QHR uses structured change management processes for software and infrastructure changes. These processes include change implementation, review, testing and deployment stages, with division of roles and responsibilities.

3.4.3 System Access and Data Confidentiality

QHR has established procedures defining how client data should be securely transferred, maintained, and ultimately destroyed should the organization cease to be a client. They also have procedures in place to ensure that client data is only used in ways that are compliant with client agreements and regulatory requirements.

3.4.4 Incident Management

QHR follows a structured approach to assessing, categorizing, monitoring and managing risk. It also has specific procedures that employees are trained in the use of for handling incidents.

3.4.5 Backup

QHR has implemented various backup methods as part of its production operations. The company has a multi-layered strategy for protecting critical data files to meet business requirements. This strategy includes using onsite backups, and backups and transaction logs stored at separate physical sites to the primary data. Using an automated process, backup jobs run using a backup utility whereby the target files are identified in predefined backup jobs (both local and remote based backups). The Technology Department continuously monitors the backup system. Restore testing is performed through the course of normal operations and as part of periodic testing.

3.5 Data

Accuro is used by clients to manage, store, and access Personal Health Information (PHI) for which they are the direct custodian or authorized agent. QHR acts as the agent of this data by providing the service used to manage it. If a client utilizes the Accuro Hosted solution, all data is stored securely at third-party data centres. If the client implements a local install of Accuro, they store their data on their own site and are responsible for all privacy and security requirements for necessary hardware.

QHR allows clients to import or export their data to their database using a secure file transfer method. The QHR Data team assists with all data transfers to ensure data integrity is preserved.

User accounts within each client's database are created by QHR and managed by the client's designated administrator(s). QHR assigns role permissions for user accounts based on communication from the administrator. All access to client data must be approved by the data custodian.

QHR employees must sign an agreement which dictates their responsibilities as agents of client data. Access to client data is granted on the rules of need to know and least privilege. There are strict policies in place around access, use, disclosure, retention and destruction of client data.

4. Relevant Aspects of the Overall Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning controls and the emphasis given to controls, as expressed by the Company's policies, procedures, methods, and organizational structure. The following is a description of the components of internal control pertaining to the Company's systems.

4.1 Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Management

QHR's senior leadership sets the tone for all activities necessary for meeting Security and Availability commitments. They ensure that policies and procedures are understood and followed by all employees. There is an organizational structure which encourages information to flow from the top down.

Formal job descriptions and regular departmental/divisional meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under QHR's policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring client base for trends, changes, and anomalies.

Employee Responsibilities

All employees must sign the QHR employee IMA, Confidentiality Agreement and Code of Conduct prior to their start date. All employees are also subject to criminal background and reference checks prior to hire. During the onboarding process, training on policies and procedures is provided. Training records are kept for each employee and follow-up is done in their annual review to ensure full compliance.

4.2 Risk Management

QHR identifies and manages risk throughout all processes. QHR Directors meet regularly to discuss progress towards Objectives and Key Results (OKRs) of the organization. OKRs are defined for each department and include risk mitigation targets when deemed appropriate. The Privacy and Security

Offices review risks and approve mitigation plans.

4.3 Information and Communication

QHR uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner, and that staff understand their role and responsibility over service and controls. These methods include the following:

- new hire training,
- ongoing training,
- policy and process updates,
- use of email to communicate time sensitive information,
- documentation and storage of historical data in internal repositories for business and support activities.

Communication is encouraged at all levels to promote the operating accuracy of QHR. For communicating with clients, QHR utilizes a number of methods to provide and request information. There are release notes sent out about every software update; advisory notices are sent out to alert clients to any major issues; marketing emails are sent out to promote awareness of availably products and services.

4.4 Control Activities

QHR has designed and implemented controls over computer operations, access, and systems development and maintenance. These provide a secure and productive environment for the development and processing of applications. QHR has also documented policies and procedures to support the implementation of controls.

4.5 Monitoring

4.5.1 Computer Operations

Systems Monitoring

QHR regularly monitors our systems for capacity, performance, and hardware failure. Overall database health and capacity planning are monitored to ensure the system will meet the needs of QHR and its clients. Technology monitors security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem.

Patch Deployment

QHR takes a proactive approach to patch management. Company administrators regularly monitor various websites, messages boards, and mailing lists where timely notification of bug and related patches is often disclosed. This allows QHR to plan for upcoming patches.

4.5.2 Service Operations

Third-party Services

Prior to the use of third-party services, an assessment is conducted to determine that services will not significantly impact Security or Availability commitments. Where possible, attestation reports (e.g., SOC 2 reports), are obtained and evaluated.

Client Services

Client contacts are tracked in QHR's CRM tool and evaluated for trends or possible nonconformities. Service Level targets are also evaluated at regular intervals to ensure clients get assisted in a timely manner.

5. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the subservice organizations described below. The examination by the Independent Service Auditors did not extend to the policies and procedures at the subservice organizations.

6. User Control Considerations Provided by QHR Technologies

The processes of the Company were designed with the assumption that certain controls would be implemented by users. In certain situations, the application of specific controls at user organizations is necessary to achieve the control objectives included in this report.

This section highlights those internal control responsibilities that the Company believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for users to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place. Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for the assertions underlying the financial statements and control environments for the Company's user organizations.

For a local Accuro set-up, the client is responsible for certain controls necessary to achieve control objectives included in this report. The client is responsible for all of the following as per the LSA:

- A dedicated server that meets minimum technical requirements

- A Windows PC workstation to handle faxing and billing submissions
- IT services required to support all local hardware
- Data backups (although QHR does offer this service for an additional monthly fee)
- Adhering to security and privacy best practices for protecting the integrity of data for which they are the custodian
- In addition, there are controls that all clients regardless of whether they are ASP or local, should implement to complement controls at QHR. User auditors should consider whether or not the following controls have been placed in operations at client sites (user organizations):
- Controls are in place for user organizations to ensure compliance with contractual requirements
- Controls are in place to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and are required to be changed on a regular basis
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by QHR