AQuity Solutions Security Whitepaper

This security whitepaper describes the overall security controls in place for AQuity Solutions products and services. It should be read in conjunction with the product-specific and/or service-specific white papers for the AQuity Solutions products and services that you may use, which include additional details specific to those products and services.

Company Background

AQuity Solutions was founded on February 1, 2019, as a dedicated outsourced clinical documentation labor service. Initially created with the production service workforce portion and supporting functions (HR, Finance, Sales, IT, Support) of the former M*Modal business when the technology assets were acquired by 3M. AQuity Solutions's legacy traces back to 1984 with the formation of MedQuist as a consolidation of small regional transcription labor services in the Northeast.

In more than 45 years of continuous operations serving the U.S., Canada, Australia, and U.K. healthcare marketplace, AQuity Solutions has evolved through a balance of strong organic growth as well as mergers and acquisitions to become the premier supplier of medical records business process outsourcing, as evidenced by top rankings with both KLAS and Black Book.

Through the roll-up of legacy technology leaders such as Lanier, Digital Voice, Inc., and SpeechMachines, along with premier labor businesses such as CBay, Spheris, and scores of smaller, highly respected regional players, MedQuist, then M*Modal and now AQuity Solutions became a dominant force in the U.S. healthcare market.

AQuity Solutions provides Transcription, Records Management, Coding and Medical Scribing services to its customers utilizing the 3M/MModal Fluency suite of products and AQuity Solutions FutureNet suite of products.

Needs and Expectations of Interested Parties

PHI/PID originating in the USA is only processed in Microsoft Azure environments inside the USA.

Data originating from customers in Canada is processed in Canada. That location is compliant with British Columbia Privacy Act, Canada PIPEDA, Ontario PHIPA and FIPPA, and Nunavut ATIPP.

Data originating from customers in Australia is processed in the AQuity Solutions-managed Azure Australia facility and compliant with the Australian Privacy Act and National Privacy Principles, as well as state regulations and laws.

AQuity Solutions is regulated by HIPAA, HITECH, and various state and international data protection laws. AQuity Solutions has determined that the ISO 27001 standard and consequent AQuity Solutions Information Security Management System (ISMS) address the combined requirements of all applicable data protection laws. AQuity Solutions has been audited for SSAE 18 SOC 2 compliance and was found to have security and privacy controls, which are working effectively.

Physical and Environmental Security

AQuity Solutions manages Microsoft Azure environments in Australia and the USA. The Azure environments undergo annual audits. AQuity Solutions is provided with space, power, and network connectivity. Azure environments are setup in the following Azure areas:

- US East
- US West
- Australia Southeast

AQuity Solutions also uses 3M/M*Modal as a cloud service provider. 3M/M*Modal environments are in the following countries:

- US
- Australia
- Canada
- United Kingdom

AQuity Solutions annually reviews physical and environmental security with its vendors.

These reviews take the form of:

- Responses to a questionnaire, including perimeter security, entry controls, room security, external and environmental threats.
- A review of the certificate's and/or report of the standards-based security review already completed by the vendors (e.g., SSAE-18, ISO 27001).

Microsoft Azure environment access is controlled through the use of secure VPN to access Internal Systems. VPN Access uses Microsoft Azure Active Directory with MFA for Authentication. No physical access is allowed.

- Azure environments are highly secure environments. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the environment resources. Azure environments managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

- **Facility's perimeter.** When you arrive at the Azure datacenter, you are required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team always monitoring their videos.
- **Building entrance.** The Azure datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter and always monitor the videos of cameras inside the datacenter.
- **Inside the building.** After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the Azure datacenter. If your identity is validated, you can enter only the portion of the environment that you have approved access to. You can stay there only for the duration of the time approved.
- **Environment floor.** You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you are required to pass through an additional security scan.

AQuity Solutions Microsoft Azure environments have Intrusion Detection/Intrusion Prevention Systems and robust network security, including firewalls, segmented networks, web application vulnerability scanning, monthly network vulnerability scanning, AV on all servers, and geo-IP filtering.

Physical security controls are also in place at all AQuity Solutions offices. Customized badges or biometrics are required to unlock exterior doors. Visitors to offices are required to sign in using a programmed iPad, identify which AQuity Solutions employee based in the office is to be visited, accept or reject retention of their names for a period of time, and are issued a temporary photo ID badge. This includes AQuity Solutions personnel visiting other AQuity Solutions offices. AQuity Solutions visitors, which are not employees of the company, are always escorted while in the office. All visitors must sign out upon exiting the office.

Workstation Security

All AQuity Solutions corporate and production workstations include the following security standards:

- Antivirus Control: Enterprise Antivirus & Up-to-date Antivirus signatures
- Enterprise Patch Management
- Complete Hard Drive Enterprise Encryption
- Centralized System Inventory of all hardware
- VPN connection between AQuity Solutions production and customer environments
- Multi Factor Authentication is used when accessing customer networks / systems

- All PHI is encrypted in transit
- Password-protected screen savers are configured to apply after a set period of inactivity
- Whitelisting is restricted to only required websites
- Real time monitoring on all workstations
- Controls to block external storage (USB/Thumb Drives) and print media

Operational Security

Backups

In AQuity Solutions Microsoft Azure environments, full database backups are done each evening. All backups are encrypted. A restoration test is performed at least annually. All backups are routinely checked for their data integrity. Tapes and other removable media currently are not used in backups. More information on disaster recovery is provided later in this document.

Event Logging

Access to AQuity Solutions services is logged and audited, with attention paid to attempts to sign in and out and attempts to view and alter PHI. Some audit data is available for customers to review, while other data is intended for internal use. Please refer to other whitepapers for details of the audits available to you for the products and services that you use.

Deployment

Deployments are only performed by trained and approved employees, after successful testing, with management approval, and a rollback strategy in place.

Network Security

AQuity Solutions-managed Microsoft Azure environments have Intrusion Detection/Prevention Systems and robust network security, including firewalls, segmented networks, geo-IP filtering, web application vulnerability scanning, monthly network vulnerability scanning, and encryption protocols.

AQuity Solutions restricts or forbids transferring PHI/PID by removable media, printing, faxing, voice mail, email, message boards, file sharing, unsecure instant messages, or verbal conversations with or near unauthorized personnel. This functionality has been disabled on production PCs.

AQuity Solutions has implemented Geo-IP blocking for all countries in which we do not do business, as well as email blacklisting of countries in which we do not do business.

AQuity Solutions has implemented multi-factor authentication for privileged user access to servers and data.

Multi-factor authentication is utilized for VPN and all Microsoft Azure environment access.

International data transfer

PHI originating in the USA is processed and stored in Azure environments located inside the continental United States.

AQuity Solutions adheres to the European Union General Data Protection Regulation (GDPR), Canadian PIPEDA and other provincial privacy laws, Australian Commonwealth Principles for the Fair Handling of Personal Information and other Commonwealth privacy laws, and any relevant country privacy regulations or laws related to transborder data flow. PHI/PID/PII is not transferred from the country in which the data resides to another country.

Remote access to Azure environments

AQuity Solutions personnel access AQuity Solutions Azure environments via a secure VPN tunnel and uses Microsoft Azure AD with MFA for Authentication.

Network security testing

In addition to weekly and monthly internal vulnerability scanning, AQuity Solutions undergoes third party penetration testing on an annual basis.

Cryptography

AQuity Solutions uses cryptographic controls to protect the most sensitive classifications of information: Protected Health Information, Personally Identifiable Information, Passwords, and other Authentication Information. Cryptographic controls are used to ensure that data is not improperly viewed (confidentiality), not improperly modified without detection (integrity), and to authenticate users and other system entities (authentication).

Cryptographic algorithms for cryptographic transitions, symmetric key encryption, asymmetric key encryption, secure hashing, secure random number generation, and message authentication use algorithms from the list of approved security algorithms in *FIPS 140-2*. This includes use of *FIPS 180-4* for secure hashing. Minimum key sizes are as described by NIST guidance, such as *FIPS 140-2* and *NIST Special Publication 800-57 5.6*. AQuity Solutions uses the following secure cryptographic algorithms: AES-128, AES-256, TDEA (also known as Triple DES), RSA-2048, DSA-2048, ECDSA-256, Hash_DRBG, HMAC_DRBG, CTR_DRBG, PBKDF2, SHA-2, SHA-3 and DSS. Storage encryption technologies on end user devices are consistent with *NIST Special Publication 800-111*.

Please refer to other white papers for details of the cryptography implemented for specific AQuity Solutions products and services.

Data Transfer

For information transfer, approved secured connection types are TLS (including HTTPS and FTPS), SSH (including SFTP), and secure VPN (including IPsec and SSL). Cryptography is done using third party cryptographic modules. AQuity Solutions does not create its own implementations of cryptographic algorithms. AQuity Solutions HTTPS data transfer supports Perfect Forward Secrecy and HTTP Strict Transport Security. AQuity Solutions TLS data transfer complies with *NIST Special Publication 800-52* (Guidelines for Selection and Use of Transport Layer Security (TLS) Implementations). AQuity Solutions VPN data transfer complies with *NIST Special Publications 800-77* and *800-113* (Guides to IPSec VPNs and SSL VPNs).

AQuity Solutions requires the use of cryptographic controls on all PID/PHI transfer over the internet, public networks, and wireless networks, to or from AQuity Solutions systems, and on all transfer of authentication information.

Encryption at Rest

Hashes of user-created passwords are stored with PBKDF2, as described in *NIST Special Publication 800-132*. Hashes are preferred to reversible encryption where technically feasible.

AQuity Solutions encrypts PHI/PII/PID when it is stored at rest. PHI/PII/PID is not to be stored on any mobile devices, workstations (including laptops), and removable media.

AQuity Solutions protects data at rest in our highly secure Microsoft Azure environments using Network, Physical and Operational security measures mentioned above. Data at rest is encrypted at the applications and appliance level.

Human Resources

AQuity Solutions screens all potential employees, which may include:

- Criminal background checks (misdemeanor and felony;
- Social Security Number Address check; Office of Inspector General (OIG) List of Excluded Individuals/Entities (LEIE);
- Government Services Administration (GSA) Excluded Parties List System (EPLS);
- Employment verification.

A structured disciplinary process is followed in the event of a violation of AQuity Solutions privacy or security policies. After employee or contractor exit, access to corporate and customer resources are promptly disabled.

Privacy and Security Training

All AQuity Solutions personnel are required to undergo annual online HIPAA, CMS Fraud, Waste and Abuse, ISO 27001/2 and GDPR training, including testing their comprehension of each training. All privacy and security training are electronically tracked and documentation retained in accordance with HIPAA.

All employees and contractors are required to sign a confidentiality agreement, which contains responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee. Employees and contractors also execute a separate PHI confidentiality policy, which survives any termination of employment by AQuity Solutions.

User authentication and authorization

Access to PHI/PID is reviewed at least annually. This includes reviewing recently terminated employees since the last review, access grant requests for appropriate authorization, and role-based access to sensitive system or areas, including specific environments.

All logins require a unique individual login and secret authentication information. The secret authentication information may either take the form of a secret password (x character minimum) or a 1024-bit (minimum) DSA or RSA private key. Password complexity is enforced. Passwords must not be written down and may not be emailed unencrypted. Initial or temporary passwords expire upon initial access by the end user, forcing the user to choose another password before the logon process is completed.

Systems are configured in such a manner that system identifiers are not displayed until the log-on procedure has been successfully completed. The log-on procedure protects against brute force log-on attempts. For example, after a specified number of unsuccessful log-on attempts, action may be taken. Log-on procedures trace login and logout events for each user ID. This allows the detection of simultaneous login sessions that may be the result of shared user IDs. Each system can be configured to terminate or lock electronic sessions after a predetermined time of inactivity.

Each system can be configured to restrict the access of user IDs and/or user groups to information and application system functions, including:

- Controlling which data can be accessed by a particular user
- Controlling the access rights of users, e.g., read, write, delete and execute

Regular user activities are not performed from privileged accounts.

AQuity Solutions has implemented multi-factor authentication for all users accessing Azure environments.

Risk Assessment and Treatment

AQuity Solutions conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI/PID that it holds and impact on the Business, as well as other assets including hardware, software, configuration files and settings, customer profiles, job processing information, billing information, passwords, and other factors of authentication.

The risk assessment process is continuous and includes a yearly review. A risk treatment plan is created and executed to add compensating controls where reasonable and appropriate and to remediate any found deficiencies. Senior management reviews and approves all risk assessment and risk treatment plans and determines whether to remediate, transfer, accept, avoid risk. HIPAA and GDPR are mapped to AQuity Solutions risk assessment and treatment.

Security Audits

AQuity Solutions undergoes an annual internal ISO 27001 audit by the Steering Committee for Information Security and an internal audit by an external party, an annual external ISO 27001 audit, an annual SSAE-18 audit, annual penetration testing, and SOC2 certification audits. Non-conformities are promptly reviewed by the Chief Security Officer and appropriate corrective action is taken.

HIPAA, GDPR, SOC 2 are mapped to ISO 27001/2 ISMS requirements and controls.

Business Continuance

AQuity Solutions has a proprietary system architecture and corresponding recovery plan in place to ensure business continuity that has been proven to meet every customer's contractual service level. AQuity Solutions has a formal, documented Business Continuity Procedure and Plan, which are formally tested at least annually.

Disaster Recovery

To maximize the resiliency of systems in the event of local disaster, AQuity Solutions has server and storage that is diversified to ensure that in the event of a failure at one Azure environment AQuity Solutions could recover services at another Azure region.

For all systems, disaster controls include:

- All mission-critical equipment is placed inside the hardened environments, which have tight security procedures, backup environmental and communication systems, and state-of-the-art fire suppression systems.
- Installed proactive monitoring tools on all applications that identify potential failure points before they affect operations.
- Virtualize all servers.
- A call tracking system to monitor all trouble tickets.
- Call center operating 24x7 with technicians always available.
- An alert system should an event be identified as potentially catastrophic.
- Documented business continuity management plan, incident management plan, and an Incident Response Team to immediately implement disaster protocol.

Catastrophic Failure

Although the probability of destruction of a facility is extremely low, AQuity Solutions has selected Microsoft Azure as its Cloud Service Provider and has production platforms operating in Azure Regional environments. An Azure Region is a set of datacenters that is interconnected via a massive and resilient network. The network includes content distribution, load balancing, redundancy, and data-link layer encryption by default for all Azure traffic within a region or travelling between regions.

The primary objective is to restore services as quickly as possible, with little or no data loss. AQuity Solutions has an internal call escalation/recovery plan with on-call personnel and target recovery timeframes to address office / cloud infrastructure and production platforms before, during, and after a catastrophic event. As part of our requirement to maintain the highest levels of security and to preclude targeted malicious attacks on our infrastructure, details of the systems architecture, call escalation and recovery plans are not presented in this white paper.

Additional privacy and security policies

AQuity Solutions has HIPAA, ISO 27001, SOC2 and GDPR compliant policies to address numerous business functions that have privacy and security implications including, but not limited to, use of mobile devices, teleworking, use of removable media and media transfer, media disposal, emailing of PHI/PID, faxing PID, business continuity, capacity management, privacy and security incident reporting and response, system change control, system monitoring, malware protection, data retention and data destruction.

© 2022 AQuity Solutions IP LLC, all rights reserved