QMENTA®

Data Security and Quality Framework at QMENTA

Security Whitepaper

Data Security & Quality Framework at QMENTA

Introduction

The QMENTA platform and its database has helped hospitals, specialists, research organizations, biopharmaceutical companies and Clinical Research Organizations (CRO's) in learning more about the human and animal brain, following the industry's comprehensive security framework.

The platform manages protected health information (PHI) in a secure, segregated network and uses encrypted data transmission. Security is a critical core aspect of running a business and conducting research in this highly sensitive and life affecting industry.

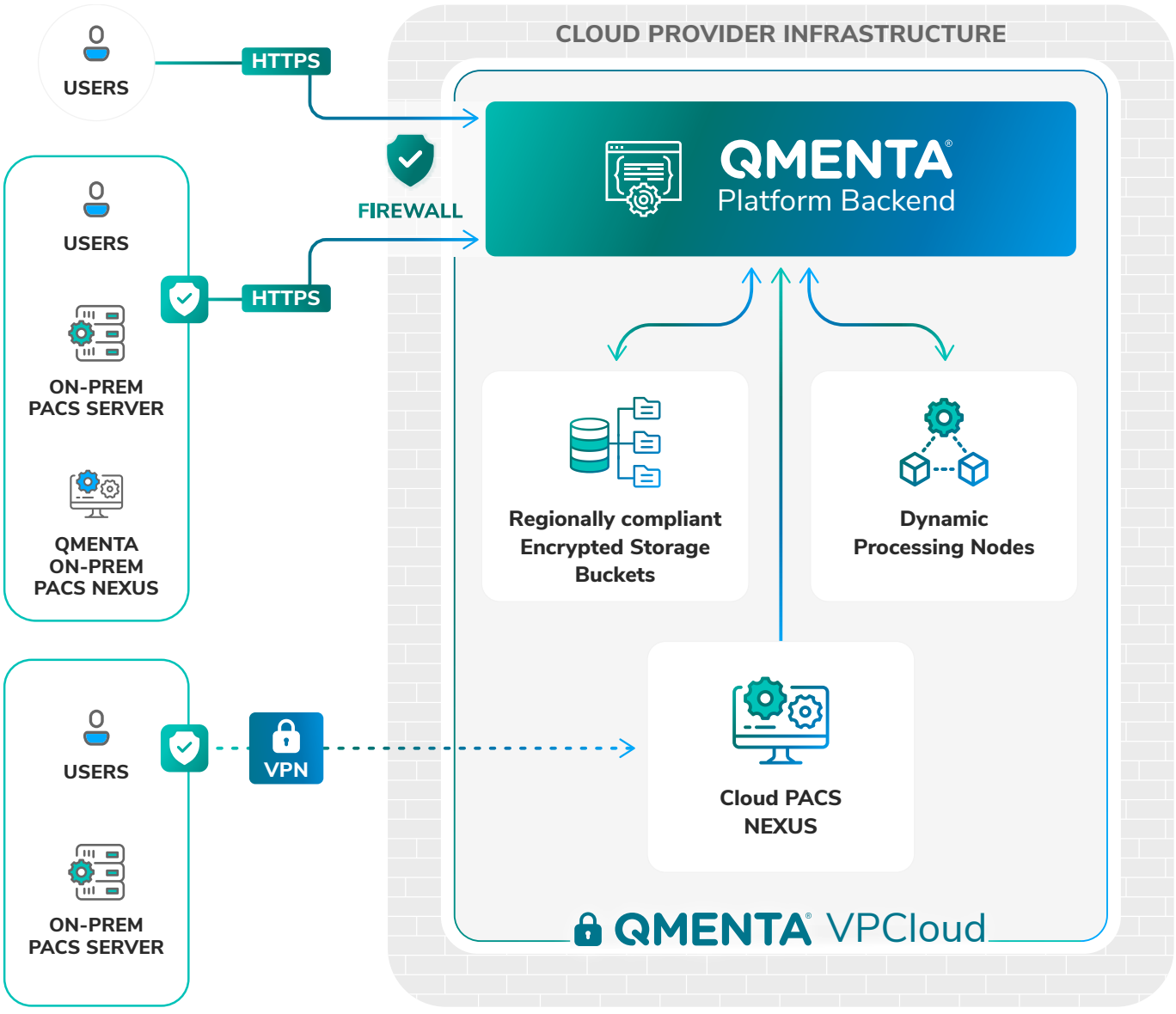
QMENTA understands the security requirements and aspects of the cloud architecture, and the platform is designed to deliver superior security than traditional on-premises data-archiving systems. Our comprehensive security strategy includes planning, technical implementation, organizational structure, and many other business operations to ensure the highest level of security and safety at all times. The client's data is protected at all times - whether it is traveling over the internet or stored in the platform.

Platform & infrastructure security

QMENTA's platform is hosted on a cloud provider infrastructure that provides built-in compliance and security with top industry certifications. The platform runs in the segregated network so that the data access is separated from other networks in the infrastructure and monitored by an active firewall to prevent cyberattacks.

When a user opens the platform, all data is transferred in an encrypted format via the HTTPS protocol. Only authenticated users are allowed to browse and upload data on the platform. After a successful login, the user automatically receives an access token, which is checked upon each subsequent request. Each token is valid only within the expiration period. The web server is protected from malicious attempts by multiple firewalls.

The server also provides the business logic as a service, and the user interface utilizes this service. When an analysis is launched, a dynamic worker instance is initiated to run the analysis. The platform integrates multiple cloud providers to optimize the performance as needed. The images are stored in an encrypted storage bucket. Each server executing the analysis has a dedicated user to call the centralized API of the platform. The API checks any request regarding its permissions, i.e., the context of operations allowed to the user.



Data Security

Access Control

Access control is flexible and secure. Patient data is organized in a 'Project' and the access permissions are granted by the Project owner (administrator). The Project owner can assign collaborator access - who can modify the subjects' data -, or guest access - who are only allowed to view the information - to users. The platform offers other custom roles according to the client's needs and requirements.

QMENTA takes care of internal procedures for data handling. The access to the patient's data is limited to QMENTA administrators, for support service only, and they follow appropriate data access protocols.

The access to the platform is possible only for authorized users through a unique username, and password (must be changed every 90 days), a two-factor authentication may be enforced depending on the project requirements. Every user must use their own username and password. QMENTA administrators monitor usage, and block or deactivate invalid user accounts. Furthermore, QMENTA retains audit logs to track all activity on the platform as required by HIPAA.

Data Location

QMENTA's aim is to facilitate and guarantee a study's confidentiality and integrity of all the data. When creating a new study, you can choose a data center where all imaging data will be stored, from a list of countries in Europe, North or South America, or Asia Pacific. For example a site in Germany can select to keep all data in Germany.

The selection of data location is important to comply with the EU-US Privacy Shield. The Shield highly regulates the transfer of personal data from EU to US and recommends limiting the transatlantic data transfer only for necessary situations.

QMENTA's platform helps you comply with these privacy regulations. If you run your R&D activities in the EU, for example, you can choose to store your data in an EU region to avoid transatlantic data transfer. You can also choose the location for the data of all other users or uploaders involved in the study. So you may have a site in Australia that will be taking part in the project, but their data will stay in Australia.

Encryption

Communication between client's web browser and the cloud infrastructure is through an encrypted and authenticated channel, with a strong protocol (TLS 1.2), a strong key exchange (ECDHE_RSA), and a strong cipher (AES_256_GCM).

Protected health information (PHI) and data anonymization

QMENTA's cloud platform provides built-in and automated anonymization of all uploaded imaging data, removing PHI from uploaded DICOM image files regarding the requirements to protect patient identity.

QMENTA also offers a tool to automatically remove facial features from 3D anatomical images, should it be desired by the user. For the user's convenience, it is also possible to upload data to the platform directly through our web-app. This is intended for experts who wish to upload data quickly without any installation and with minimal effort. In this case, the data is sent through an encrypted channel and de-identified immediately upon receival in the platform.

QMENTA provides PACS connection capability that facilitates the data transfer between the platform and the PACS system within the user's local network. The application, QMENTA PACS Nexus, runs on a local workstation inside the hospital network and automates the task of exporting images to the platform and retrieving the analysis results. Images are de-identified before the data leaves the client site and the images are sent via secure HTTPS protocol.

Security controls

A rigorous security framework is ensured with the implementation of administrative, physical, technical, organizational, documentational, retentional, and other measures of security control. QMENTA platform is compliant with strict industry standards such as HIPAA, GDPR, FDA Part 11 & 820, ISO 27001

Requirement	Compliance on QMENTA's platform
Administrative Safeguards	The platform covers all required procedures, including risk assessment and workforce security. A contingency plan is built together with our cloud partners.
Physical Safeguards	Data center security is handled by our cloud partners. QMENTA has implemented workstation securities.
Technical Safeguards	QMENTA platform offers access controls, audit trails, and user authentication. Additionally, QMENTA provides a functionality to strip out Protected Health Information (PHI) from the datasets before transferring them onto the platform.
Organizational Requirements	A Business Associate Agreement (BAA) is signed between QMENTA and its clients & its cloud providers.
Documentation Requirements	QMENTA team has built required procedures and documents them in a repository.

GDPR on Healthcare Data

Under the new GDPR (General Data Protection Regulation), which went into force throughout the EU on the 25th of May 2018, these rules have strengthened the protection of individuals' personal data and threaten significant fines and penalties for anyone that is non-compliant. In clinical research or clinical trials, health data collected is subject to tighter Regulations for processing compared to other types of personal data.

Responsibilities of Principal Investigators

Hospitals, research centers, pharmaceutical companies or CRO's must be responsible for collecting and processing personal data as a Data Controller under the GDPR in clinical research or trials. Penalties under the GDPR are extremely large; potential fines of up to €20 million or 4 percent annual global turnover, whichever is higher.

Even when a clinical trial is conducted outside of the EU, there are still possible issues regarding GDPR compliance. First, GDPR is applicable if EU citizens participated in the trial regardless of the geographical locations. Second, according to EU Regulations 536/2014, clinical trials outside of the EU have to follow the regulations when the trials are submitted for marketing authorization in the EU.

Key points

Data protection impact assessment

The GDPR requires Principal Investigators to conduct an assessment; a description of data processing operations and its purposes, the necessity of the processing, and risks to the rights of clinical trial participants. It is likely that the Principal Investigator needs to appoint a Data Protection Officer.

Participant consent

Consent must be specific to each data-processing procedure. Such consent must be explicit and unambiguous. The obtained data cannot be used for any purpose except those the patient clearly indicated their consent. As the use of "big data" has been increasingly important in clinical research and trials, the terms and conditions must be reviewed and updated.

Data transfer outside of the EU

GDPR requires that EU citizens' personal data should be protected in a manner that is consistent with GDPR when it is transferred outside of the EU. Also, consent should specify that data is being sent outside the EU.

This can be an issue as multi-site neuroimaging studies are becoming more prevalent. Principal Investigators should demonstrate their compliance and are accountable for necessary documentation.

Subject right

Under GDPR, a trial participant can request to remove all of their data without undue delay and to receive their data to transmit it to another Data Controller. Principal Investigators must be ready to delete data or export it in a commonly used and machine-readable format, whether stored in their on-premise environment or in any other third-party.

Pseudonymisation/ Anonymization

Pseudonymized data can be attributed to a trial participant by the use of other information such as mapping of ID numbers and should be treated as sensitive data. On the other hand, anonymized data doesn't contain any links between de-identified data and original data. Under GDPR, anonymized data is not considered to be personal health data.

QMENTA's approach

QMENTA is in compliance with GDPR and has implemented the necessary controls. For example, QMENTA's cloud platform provides built-in and automated anonymization of all uploaded data, removing PHI from DICOM image files as mentioned above, as well as the above-mentioned de-facing feature for head images. In this way, medical images in the platform are not considered to be personal health information (PHI) under GDPR.

It is easy to control where the data will stay geographically by using the QMENTA platform because it allows users to select the location of data storage as described above in section "Data Security". Local investigators manage their own data in multi-site studies without worrying about the difference in regulations between countries.

QMENTA has implemented the procedures to deal with the request of trial participants that would like to delete or remove their data. Data can be exported in a commonly used format to comply with the requirements of GDPR.

Quality Management System at QMENTA

QMENTA's Quality Management System (QMS) is a company-wide initiative to enhance product quality and improve patient safety. It defines the PDCA (Plan - Do - Check - Action) cycle to optimize product development procedures and analyze opportunities for improvement. Its risk-based approach helps the organization to determine any risk factors that could potentially harm patients and apply risk mitigation measures.

QMENTA holds the, ISO 13485:2016 certification for our quality management system from LL-C - an accredited certification body. ISO 13485:2016 is the most widely known and internationally accepted quality standard, specific to the medical device industry. We use all the necessary procedures and have repeatedly and successfully demonstrated our ability to consistently provide products that meet both our customers' needs, as well as the applicable statutory and regulatory requirements.

This certification paved the way for the use of our products in the strictly regulated clinical care market. In fact, ISO 13485 is considered as a prerequisite of the CE marking certification process in the European Economic Area.

Together with the ISO 13485:2016 certification, QMENTA has implemented processes to comply with FDA's CFR 21 Part 11 (Regulations on electronic records and electronic signature) and CFR 21 Part 820 (Quality system regulation) that are considered as a prerequisite of the 510(k) pre-market submission made to FDA (Food and Drug Administration), Annex 11 (Medicinal products for human and veterinary use - Computerised systems), and IEC 62304 (Software life cycle for medical device software).

QMENTA's Quality policy

At QMENTA we commit to excellence in all aspects of our work, and through the implementation and strict adherence of our quality management system we apply the current legislation in all our activities. This allows us to maintain the highest standards to our products and services, as well as ensuring compliance with all applicable standards for our activities and systems.

At QMENTA we ensure the involvement of management, to be sure that all aspects and areas of our company conform to both our own internal standards as well as the international quality standards.

In commitment to our quality policy, we will promote its understanding and dissemination within the organization through internal channels for training and communication.

Implementation of quality management procedures

Strategic processes

QMENTA collects all customers requirements and relevant regulations to determine and document the project objectives, scope, constraints, milestones, resources, success measurements, etc. Hazards and risks are identified and mitigated to assure patient safety at all times. All product design documents are filed into a design-history file throughout the product life cycle, allowing for traceability starting from user requirements, to functional requirements, software tests, and ultimately the final product.

Product development

Development of QMENTA software products are conducted in accordance with the Agile life cycle model, adapted to the lifecycle requirements of IEC 62304 regulation. It has been shown that the Agile methodology, which takes an evolutionary/ incremental development and a continuous testing approach, enables companies to produce software of higher quality and lower risk when compared to the Waterfall development approaches, which are less iterative and flexible.

Design reviews are conducted to evaluate specifications, user interfaces, or architecture to see if the product will respond to the business requirements, and to see if the system is optimized properly. Moreover, we document all user requirements and functional requirements, then proceed to conduct a risk assessment for each functional requirement.

The requirements for each release are established and described in a release-specific requirements plan. We define Epics as large bodies of work that can be broken down into a number of smaller tasks. Through tracking Epics and smaller tasks, we keep a good balance between structure, flexibility, and effectiveness. We also conduct a code review for each task.

Release

Software validation and verification procedures are conducted to make sure that the requirements can be traced to the implementation, and to also check if the requirements are realized in the final product. Change control procedures ensure that the software changes are carried out in the proper way. We release a new software version of the product only after all change requests are approved, and necessary testing has been performed and was successful.

Post-commercialization

All customer feedback via email, phone calls, or any other channel is collected in one of QMENTA's main internal systems, and tracked to make sure it is addressed. For complaints or defects, we always evaluate the root cause and look for any potential problems it could cause to evaluate a fix. In addition to this, we have defined the necessary procedures to report to the authorities when necessary for extreme events.

Corrective action or preventive action (CAPA) are created for any potential medium to major issues related to product quality. Overall performance of the quality management system is reviewed quarterly in management review meetings to discuss possibilities for improvement.

Administrative process

Critical procedures are documented and implemented to support the running of the quality management system. For example, QMENTA regularly assesses critical suppliers and requires the same level of quality management procedures from them, when applicable. Finally, information security and data integrity are managed at all times following the QMS requirements.

FDA

510 (k)

FDA clearance

In 2021 the QMENTA platform was cleared by FDA as a 510(k) Class II Medical Device (K202718) for use in the clinical setting under the label QMENTA Care Platform Family.

Through the 510(k) premarket approval process, the FDA determined that the QMENTA Platform is as safe and effective, that is, substantially equivalent, to a legally marketed device.

Through this process, the FDA evaluated that the full QMENTA Platform development lifecycle, from design to validation and verification, follows the design control procedure of the Quality Management System. Furthermore, the FDA pays special attention to cybersecurity vulnerabilities in medical devices, and has determined that the cybersecurity control requirements are met by our solution.

Case Study

Multi-center study with UCSF

This is a large, multi-site study on patients with Multiple Sclerosis (MS). A large amount of Imaging data will need to be uploaded over an extended period of time (5 years). At the end of the "MultipleMS" project, it is estimated for the project to contain a total of 3000-4000 MRI datasets, uploaded from 16 sites around the world, including sites in the USA and Germany. The partners of the consortium include major research organizations such as UCSF (USA), TUM School of Medicine (Germany), Karolinska Institute (Sweden), KU Leuven (Belgium), University of Cambridge (UK). Up to date, 10 imaging sites have already uploaded and collaborated on approximately 1000 MRI datasets through QMENTA platform.

Because the sites providing the data are located in various countries, we have to adhere to the laws and restrictions of the countries involved. To avoid issues, we always apply rules that are at least as strict as the most strict laws involved.

The QMENTA platform helps users from different sites collaborate on the project and share results via the platform. The project owner can add users, and can set the permissions per user and per site. The fine-grained permission setting allows them to define who can upload data, edit information, browse analysis results and so on.

Each site can select the location to store imaging data. For example, a German site keeps imaging data in a data center located in Germany, ensuring compliance with local jurisdiction for data storage and processing. Data transfer agreements are signed between different sites.

Our approach to this project is described in more detail in our MultipleMS whitepaper.

Precise4Q

PRECISE4Q will create multidimensional data-driven predictive simulation computer models enabling – for the first time – personalized stroke treatment, addressing patient's needs in four stages: prevention, acute treatment, rehabilitation, and reintegration. The consortium consists of 11 partners from 8 countries, including Charité (Germany) and Institute Guttmann (Spain).

PRECISE4Q will develop clinical decision support systems (CDSSs) for stroke, based on validated predictive models. They will be available "standalone" as well as part of a comprehensive Digital Stroke Patient Platform. Also, the models and data ecosystem of the Digital Stroke Patient Platform will be utilized as a European Modelling Platform for Open Stroke Research (EUROPE-STROKE). This service will enable the collection and integration of large scale data support for both hospitals and the research community to advance precision medicine in stroke. Up to date, already 8 sites have been connected through QMENTA platform and more than 80000 data points have been shared in the platform.

QMENTA hosts and provides the data used in the study across the different partners. The platform supports secure access to the heterogeneous data sources and their mapping to the Precise4Q data model, and integrates the different software modules provided by each project partner.

Data Protection in Germany

Regulation overview

Data protection in Germany is governed by the EU General Data Protection Regulation (GDPR) entering into force on 25 May 2018, as standardized European law. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of the GDPR's requirements. The Federal Data Protection Act (BDSG) has come into force in Germany.

The German legislator and authorities have developed specific regulations on IT security requirements. Under the Telemedia Act (TMG), each telemedia provider (for example, each provider of a website, a web-application and smartphone app) must ensure through appropriate, economically proportional arrangements that unauthorized access is not possible.

The Data Protection Authority (DPA) has issued a guidance paper for using cloud computing services. According to this guidance paper, data controllers must implement sufficient control measures for the cloud provider, use data encryption where necessary, and safeguard that all requirements for cross-border transfers are met, if applicable.

QMENTA´s approach

QMENTA implemented appropriate technical and organizational measures to protect Personally Identifiable Information (PII) against loss or any form of unlawful processing (including theft, unlawful copying or recording). These measures guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, based on the evaluation of the risks associated with the processing and nature of the data to be protected. Following the GDPR's practices, our security measures include the pseudonymisation and encryption of personal data.

Internal application database handles authentication settings. Access to the platform is permitted only for authorized users. All users are identified by a unique ID and password that requires at least 8 characters with complexity (containing symbol, number and capital letter). Also, our administrators monitor the usage to deactivate invalid user accounts in case of improper use.

QMENTA makes cross-border transfer minimal by allowing users to select the image data location. Transfers outside the European Economic Area (EEA) are only allowed to countries or territories that are considered by the European Commission to provide an adequate level of data protection.

QMENTA evaluates the technical and organizational security control measures to select a cloud service provider and requires a data processor agreement upon contract with cloud service providers. We partner with prominent providers such as Google (Google Cloud Platform), Amazon (Amazon Web Services), or Microsoft (Azure). The providers guarantees adequate technical and organizational information security in compliant with certifications of industry standards such as ISO 27001.

The data can be kept within the U.S.A., The EU, Germany, Australia, and Asia by just selecting the location from a drop-down menu when setting up the project, and also can select where the data of each user will reside when adding them to the project.

QMENTA®

IMAGING TO INSIGHT

LEARN MORE

US Headquarters

75 State Street, Suite 100
Boston, MA 02109
+1 339 368 8040

EU Offices

C/ Roger de Llúria 46, Pral. 1ª
08009 Barcelona, Spain
+34 933 282 007

qmenta_inc

@QMENTA_Inc

www.qmenta.com