Quibim

24.V1.SS.EN

Security and Privacy Statement

Table of Contents

1.0 Introduction

Quibim places utmost importance on the security and privacy of Customer and Patient data, ensuring that it is always available to only those with an authorized need and protected from unauthorized modification.

Quibim employs industry-standard security measures to safeguard data in its care from both online and physical threats. Data held on our QP-Care® platform hosted on Microsoft Azure, is protected by multi factor authentication and data encryption, which safeguard both data in transit and data at rest, ensuring that data is only accessible by authorised users. Quibim pseudonymizes all data to be processed by its services and does not retain any personal data from user accounts, minimizing the risk of exposure to potential threats.
The QP-Care® platform adheres to the most stringent international security and privacy standards, and regulations, such as ISO 27001, GDPR and HIPAA.

Quibim's commitment to security and privacy is underlined by both its Quality Management System, certified to ISO 13485, and its Information Security Management System, certified against ISO 27001. This security and privacy statement will be regularly reviewed and updated to reflect changes in the organization's security posture and to ensure continued compliance with relevant regulations and standards.

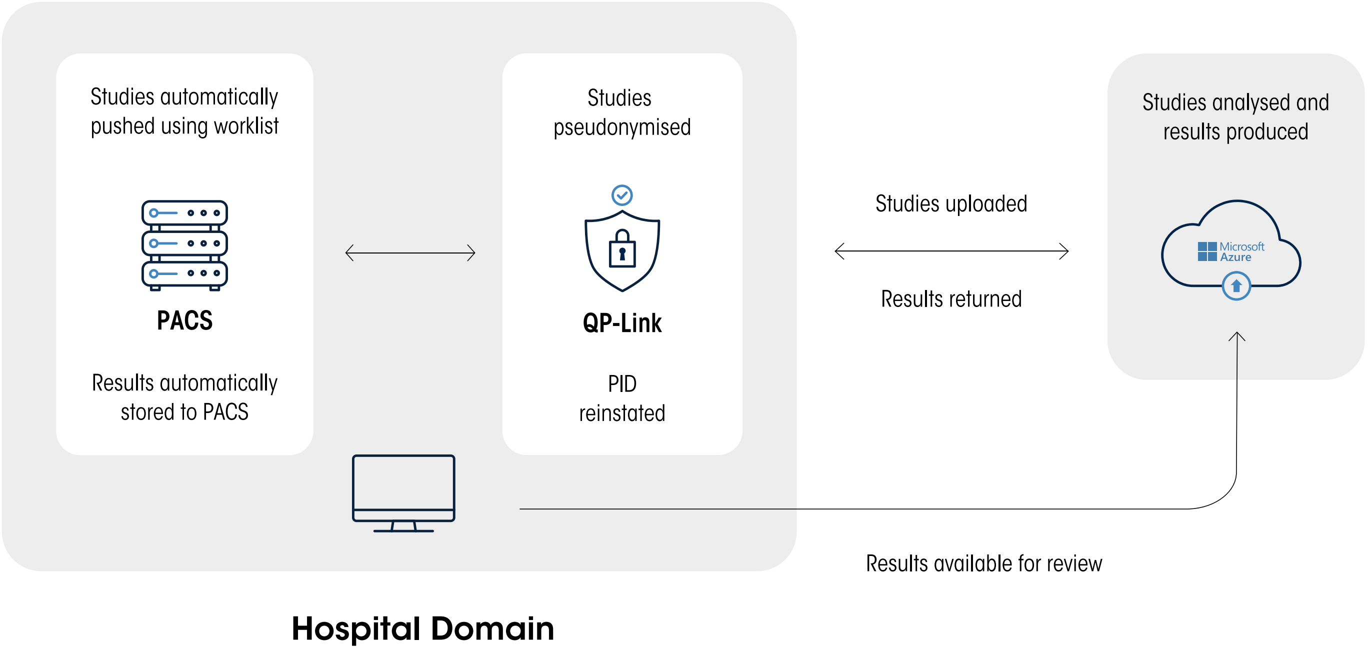
2.0 Quibim certifications

Quibim's quality management system is certified by following ISO 13485 and EN ISO 13485. This system allows Quibim to coordinate and direct activities to meet regulatory and Customer requirements and continuously improve effectiveness and efficiency. Quibim has implemented processes, procedures and privacy policies to comply with all applicable privacy regulations. Microsoft Azure is compliant with several healthcare specific regulations, such as GDPR, HIPAA and HITECH, and has received several industry certifications, such as ISO 27001 and SOC 1& 2.
Quibim has also implemented and maintains an Information Security Management System, which has been certified against ISO 27001. Quibim has internal information security policies that are updated regularly to address new threats and trends.

Quibim performs all the recurrent security duties identified by the certification body, including collaboration with companies specializing in cybersecurity to carry out regular penetration tests following the internationally recognized OSSTMM security audit methodology (Open Source Security Testing Methodology Manual, maintained by the Institute for Security and Open Methodologies, ISECOM; http://www.isecom.org/research/) and the web audit methodology dictated by OWASP (Open Worldwide Application Security Project, https://owasp.org/www-project-top-ten/).

The details of the most recent penetration test are available to Customers and prospective Customers on request, with any confidential information first removed or redacted.

3.0 Processing architecture


Studies automatically pushed using worklist
PACS
Results automatically stored to PACS
Studies pseudonymised
QP-Link
PID reinstated
Studies uploaded
Results returned
Studies analysed and results produced
Microsoft Azure
Results available for review
Hospital Domain

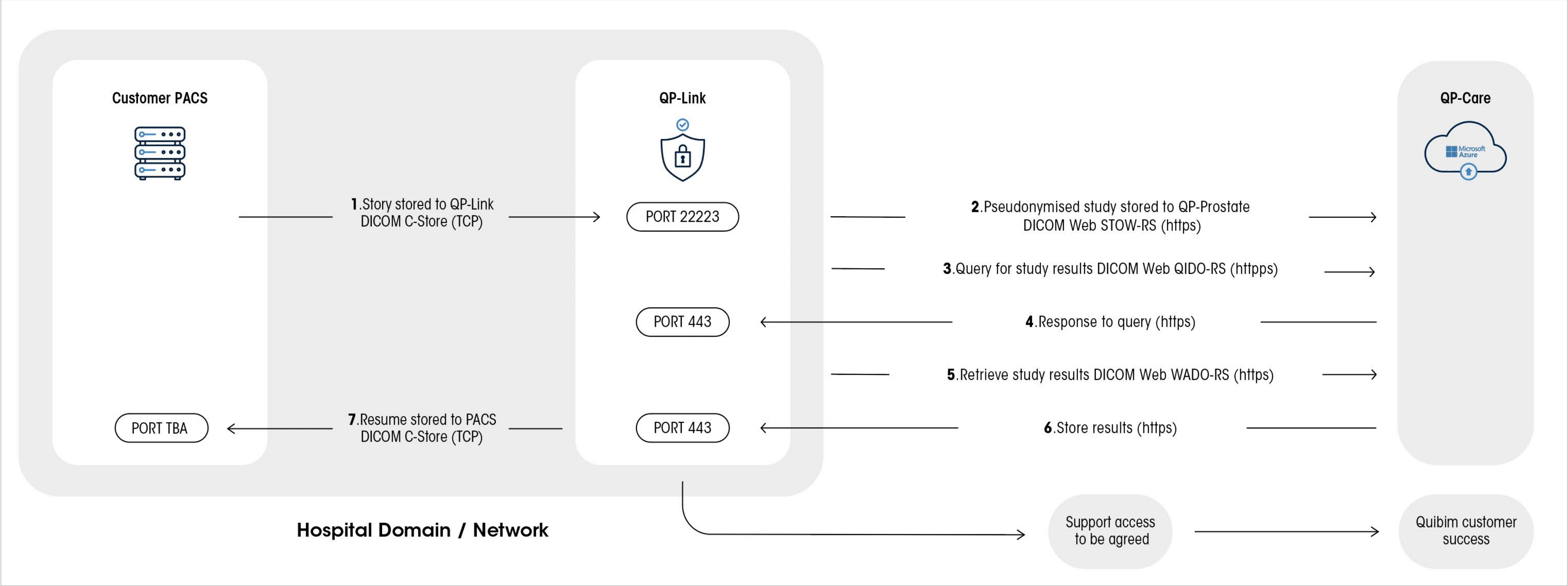
Quibim's Care family of products share a common architecture, simplifying implementation, use and support. To facilitate secure access to the Cloud, Quibim implements QP-Link® on a small footprint server provided by the Customer. QP-Link® receives studies automatically pushed from the PACS or modalities, deidentifies the data and sends the studies to QP-Care® for processing. On completion of processing, QP-Link® retrieves the results from QP-Care®, reinstates the Patient identity and stores the new series to the PACS. Several of Quibim's Care products are provided with a viewer to facilitate manual trials and review of results before download. The viewer is accessed via QP-Care®.

4.0 QP-Link®

QP-Link®, sited in the Hospital domain, provides the integration between the Customer PACS and QP-Care® in the Microsoft Azure cloud. It is responsible for pseudonymizing data before sending it securely to QP-Care® and retrieving the results it reidentifies before storing it in the PACS.

4.1 Operation

When QP-Link® receives a study from the PACS or a modality, by default, it uses a locally held encryption key, unique to each Customer, to pseudonymize the Patient ID and name, change the date of birth to the 1st of January of the birth year and clears DICOM tags (fields) which are not required for processing. The pseudonymization can be turned off at Customer's request. QP-Link® then uploads the study for processing using DICOM Web tools over an HTTPS connection (using TLS 1.2). The images are processed to generate results that QP-Link® automatically pulls to the local QP-Link® server. QP-Link® then reinstates the Patient Id and name by using the encryption key to decrypt the returned data, and the results are stored as part of the original study in the PACS.



Customer PACS
QP-Link
QP-Care
1.Story stored to QP-Link DICOM C-Store (TCP)
PORT 22223
2.Pseudonymised study stored to QP-Prostate DICOM Web STOW-RS (https)
3.Query for study results DICOM Web QIDO-RS (httpps)
PORT 443
4.Response to query (https)
5.Retrieve study results DICOM Web WADO-RS (https)
PORT TBA
7.Resume stored to PACS DICOM C-Store (TCP)
PORT 443
6.Store results (https)
Support access to be agreed
Quibim customer success
Hospital Domain / Network

Step-by-step flow

1. General routing worklist on PACS uses DICOM C-Store to send appropriate studies to local QP-Link®.
2. When required, QP-Link® pseudonymizes identifiable Patient data in the DICOM tags using an encryption key unique to the Customer, which is only stored on-site.
3. QP-Link® uses STOW-RS (https DICOM Web store operation) to send and store the pseudonymized studies to QP-Care® in the Azure cloud.
4. The pseudonymized studies are analyzed, and results are produced.
5. QP-Link® regularly checks if the analyses are finished.
6. When the results are available, QP-Link® uses WADO-RS (https DICOM Web retrieve operation) to retrieve the results from QP-Care®.
7. QP-Link® will reinstate personal information using the encryption key held locally.
8. QP-Link® uses DICOM C-Store to store the results in the local PACS.

4.2 Confidentiality

Confidentiality of data (access restricted to only those with an authorised need) is protected in many ways (ensuring resilience of processing systems and services):

1. No person-identifiable data is held on the QP-Link server. All person-identifiable data is either removed or pseudonymized within QP-Link®.
2. The key used for pseudonymization unique to each Customer is only held on the QP-Link® server in the Hospital domain. Any backups of this file are to be kept in the Hospital domain
3. The QP-Link® logs are currently recycled daily but never deleted. They do not contain any person-identifiable data.
4. Non authorized users are unable to access QP-Link®:
   A. QP-Link® does not support User access (there is no direct user interaction).
   B. Access to the QP-Link® server is managed by local Hospital staff, and limited access should be provided. It is recommended that the only accounts available should be:

      I. Administrator account(s) for local IT staff.
      II. Administrator accounts for Quibim remote access (for installation, support, and maintenance), which will be over VPN. This account may be disabled when not required.
      III. A service account for running QP-Link®.

5. Data in transit to and from QP-Care® in the cloud is encrypted using TLS and, therefore, is protected from interception (if intercepted, it does not provide meaningful data).

4.3 Integrity

Data integrity ensures data's accuracy, completeness, and reliability. (ensuring resilience of processing systems and services):

1. Access to QP-Link® is restricted:
    A. QP-Link® does not support User access
    B. Access to the QP-Link® server is managed by local Hospital staff, and limited access should be provided (see Confidentiality above).
2. Data in transit to and from QP-Care® in the cloud is transmitted using proven DICOM Web tools, and Quibim has further tested the mechanism as part of the development process.
3. Changes to QP-Link® are minimal and are subject to internal processes, that ensure an individualized control of every change from design through development and testing, to minimize the risk of any negative impact of a change.

4.4 Availability

Availability of data and the service is protected in a many ways (ensuring resilience of processing systems and services):

1. The QP-Link® server is dedicated to the running of QP-Link® only; there are no competing or potentially clashing applications.
2. The server can be provided as a Virtual Machine, and the Virtual technology can be used to provide resilience (including a backup of the encryption key).
3. The only data on the server are:
    A. Operational logs are used for investigating any issues. Loss of these does not threaten ongoing operation (and there is no person-identifiable data held).
    B. The Customer unique encryption key is used for pseudonymizing Patient data. It is recommended a backup be taken of this file to a secure local location.
4. The link between the PACS and QP-Link® is across a local network which typically offers a very high level of availability.
5. The availability and reliability of the link between QP-Link® and the Cloud will depend on the external internet circuits and connections provided by the Hospital. Still, these typically offers a good level of availability.
6. Changes to QP-Link® are minimal and are subject to internal processes, from design through development and testing, to minimize the risk of any negative impact of a change.
7. The Customer will provide the QP-Link® server and reside on their domain, as a result of which patching for the hardware and operating system needs to be built into the local schedule and coordinated with Quibim.

4.5 Auditability

Though no formal auditing requirement is under current regulations, operational logs are still maintained in QP-Link®.

5.0 QP-Care® platform

QP-Care® resides in the Microsoft Azure cloud and is responsible for the following:

1. Initiating the processing of studies sent to the cloud
2. Providing authorized user access to:
    A. Upload studies for processing and download results, if required (for a manual trial).
    B. Access a list of studies and, when needed, the viewer to review results and structured report
    C. Download and configure QP-Link® (administration users only).
3. Providing results to QP-Link® when available and when requested.

Each Customer is provided with a separate QP-Care® instance, and all tools are accessed using a browser based on a Chrome engine.

For each territory's customers, a dedicated server is set up in their region. Specifically for those in Europe, the primary Azure region is North Europe, followed by West Europe.

5.1 Confidentiality

No person-identifiable data is held in QP-Care®. The system doesn't generate or store cookies. Microsoft generates some technical cookies with the MSAL (Microsoft Authentication Library) that are deleted when the session or the browser is closed.

5.1.1 Identity and access management

Quibim uses multi-factor authentication and role-based access controls through Microsoft Azure to ensure that only authorized personnel can access medical devices and pseudonymized Patient data. Multi-factor authentication is a procedure in which users are asked during login for an additional form of identification, such as a code on their mobile phone. Azure implements role-based access control (RBAC) to control access to resources and data. RBAC allows administrators at Quibim to assign specific roles to users, specifically user/reader or administrator, based on their level of access needs. Administrator users can download, install and configure QP-Link®, assuming sufficient permissions on the local (QP-Link®) server, and view Studies. User/reader users are only able to view studies.

User access to QP-Care® (and the viewer) is restricted to clinical staff identified by the Customer and a restricted number of Quibim staff.

5.1.2 Data at rest and in transit

Once uploaded to the Microsoft Azure cloud, data at rest is stored in Customer dedicated partitions, fully encrypted (using AES256, i.e., 256-bit Advanced Encryption Standard), and accessible only by authenticated, authorized client systems and Users.

Quibim shall only retain copies of Customer data if authorized under a legal agreement and in full compliance with applicable data protection legislation and other regulations.

Secure virtual networks protect data in transit within the cloud to prevent unauthorized access and restrict network traffic to approved sources.

The QP-Care® platform uses Azure Web Application Firewall (WAF) that provides inspection of HTTP requests and prevents malicious attacks at the web layer, such as SQL Injection or Cross-Site Scripting.

5.2 Integrity

The integrity of data held in QP-Care® relies on the same protection mechanisms provided for Confidentiality and the use of internal processes, from design through development and testing, which validate that processing produces the desired and expected results. Authorized Users who are to access QP-Care® are provided training in the tool as part of the onboarding process, along with an Instructions for Use document.

5.3 Availability

Azure provides a Service Level Agreement (SLA) of 99.9% uptime for services, though actual uptime may vary depending on factors such as maintenance and update slots.

High availability is provided through Availability Zones within region and region pairs. An Availability Zone consists of three separate datacentres in a Region, such that if one Zone fails, the other Zones continue processing. Using Zone redundant services, QP-Care® automatically replicates across Zones so that the new Zone processes the workload.

QP-Care® also uses Region Pairs. For those in Europe, the primary Azure region is North Europe, followed by West Europe. In the event of one Region failing, processing continues in the other. A dedicated server is set up in each of the other territories.

To support the failover scenarios noted above, data is automatically replicated. With Geo-zone-redundant storage, data is synchronously replicated across three Zones in the primary region and then asynchronously to a single physical location in the secondary area, where it is again replicated a further two times such that there are another three copies. Microsoft Azure services include continuous uptime monitoring, with immediate escalation upon any service interruption. Quibim also makes use of Azure Backups; the scheduling and retention period of the backups is as follows:

Frequency Unit	Every	Retention Time	Snapshot Time
Hourly Snapshot	N/A	N/A	N/A
Daily Snapshot	1	30	days
Weekly Snapshot	Saturday	4	weeks
Monthly Snapshot	Last day of month	12	months
Yearly Snapshot	Last day of year	1	year

Backups are tested annually to ensure they can be relied upon in an emergency.

All clinical data used in the project is transient, with the PACS remaining the host of the clinical records.

The Microsoft Azure Cloud system is patched in accordance with Microsoft recommendations and is performed one Zone at a time and one Region at a time.

Changes to QP-Care® are limited and are subject to strict internal processes, from design through development and testing, to minimize the risk of any negative impact of a change. Such changes will be preceded by communication, identifying when the update is to take place, to all affected Customers.

5.4 Auditability

QP-Care® maintains an audit log of events within the QP-Care® environment. The audit log is currently kept indefinitely due to the potential need to support Customers in future investigations.

Should a Customer need details from the audit log, an authorized representative may contact Quibim Customer Success specifying the details required and the period.

6.0 Quibim Team

6.1 Security

Quibim takes steps to mitigate the risk of employing anyone who is unwilling or unable to accept the need to maintain good security practices and then ensures staff is provided with appropriate quality management and information security training and awareness. At Quibim, all the team follows the ISMS and is trained on it on regular basis.

All candidates provide their background history by sending the CV and cover letter and People & Culture department checks it prior to joining the company and during several interviews.

Successful applicants join the company and are subject to a probationary period. As part of their onboarding, staff are provided with appropriate training and the ability to become familiar with all Company policies and procedures, focusing on the information security and quality management system. This training is performed annually and constantly monitored by the team.

In addition to formal training programs, Quibim provides ongoing awareness campaigns to reinforce cybersecurity best practices and promote a security culture.

Alongside information security training, Quibim's employees are regularly trained in data protection principles and are bound by confidentiality obligations.

6.2 Access to Information and systems

Access to information and systems is provided only on a need-to-know basis and under the least privilege principle, dependent upon the job role. At Quibim, we follow the 'Need to Know' and 'Need to have' principles with regards to the information access.

Quibim

This document is confidential and contains proprietary information of Quibim, S.L. All rights reserved. No part of this document shall be reproduced or transmitted in any form or by any means without prior authorisation. The information herein is subject to change with or without notice. Quibim, S.L. disclaims any liability from the use of the information herein.

New York I USA
230 Park Avenue,
Spaces, office 423
10169, New York
T: +1 (858) 449-1871

Cambridge I UK
184 Cambridge Science Park,
Milton Road, Milton
CB4 0GA, Cambridge
T: +44 (0)7779 797644

Madrid I Spain
Calle de Alfonso XII 62,
3rd floor, office 3055
28014, Madrid
T: +34 961 243 225

Barcelona I Spain
Via Augusta, 123
7th floor, oficina 708
08006, Barcelona
T: +34 961 243 225

Valencia I Spain (HQ)
Avenida Aragón 30
13th floor, office I – J
46021, Valencia
T: +34 961 243 225