myQA® Daily
CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information on the myQA® Daily and software to IT personnel. This information will help ensure the secure and safe use of the system in clinical practice.

What is the system used for?

The myQA® Daily by IBA Dosimetry is a specialized designed for the efficient and accurate quality assurance (QA) of linear accelerators (Linacs) used in radiation therapy.

- myQA® Daily device is the solution for the high-quality morning Linac QA.
- The 125 ionization chambers offered by the myQA® Daily provide the largest amount of measured beam data of any available daily QA device for a more accurate beam quality verification.
- The web browser based myQA® Daily application allows flexible test execution from any network PC or tablet and easy access to test results.
- Its primary functions and objectives include:
    - Ensuring Accuracy and Safety
    - Daily Quality Checks
    - Efficiency in QA Processes
    - Comprehensive Data Collection
    - Flexible and Accessible Use

What if the device fails or data is corrupted?

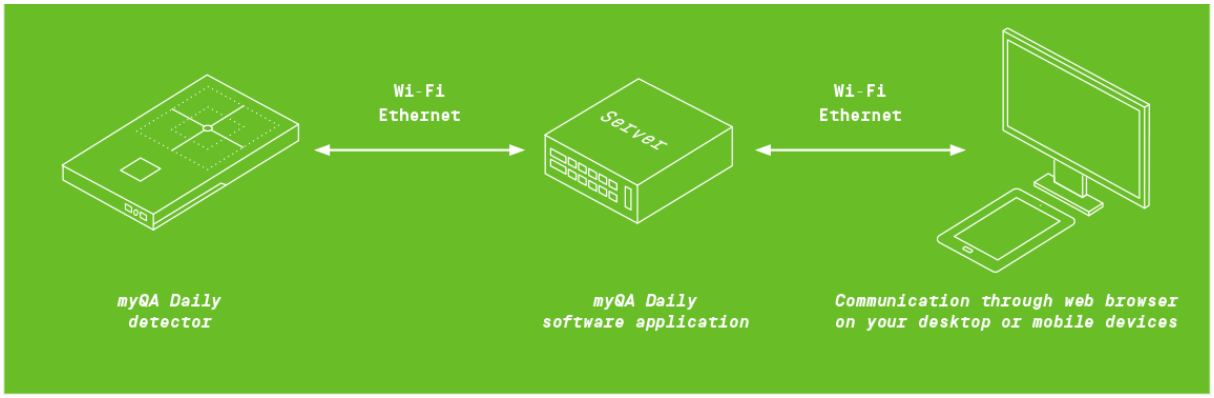
The location of use of the myQA® Daily device is within the premises of a radiotherapy department, near a radiation treatment machine, but not in a publicly accessible space. It is assumed that a high level of physical access control to this area is implemented by the healthcare provider. In addition, the myQA® Daily implements user authentication; any user who has been registered with the system and has (physical or remote) access to the instrument is free to use it after authentication via password. System-wide changes are subject to permission control (authorization) through an admin password.

myQA® Daily
CyberSecurity Leaflet

The myQA® Daily is controlled locally or over the IT network via its corresponding software (web browser), or via software which can directly access API functionality.

Non-availability of data (or of the whole instrument) does not have a direct effect on patient safety, nor does it cause a security risk. However, patient treatment may be delayed in some situations. It is recommended to the healthcare provider to include non-availability of the device in their risk management for the patient treatment process, e.g., by planning for a backup device or taking other precautions.

How does the system architecture look like?



- The myQA® Daily detector is connected via local network (Ethernet or Wi-Fi) to the myQA® Daily software application server.
- The myQA® Daily software application server is connected via local network (Ethernet or Wi-Fi) to the application frontend, which is hosted in a web browser of a desktop or mobile device.
- The myQA® Daily software application server accesses the database (SQLite) via file access.
- HTTPs must be enabled for secure communication over the local network (Ethernet or Wi-Fi).

Are there any operating systems or application software supplied?

- The myQA® Daily consists of a software component (webserver and client) and a hardware component (measurement device). myQA® Daily software/database: Installed centrally on a server or on a PC, web browser application via network workstation, or tablet PC. The web application runs on Hardware / OS provided by the hospital IT.
- The software component and related data are hosted on customers hardware / OS. The customer is responsible for all security / safety relevant topics on hardware, infrastructure and / or operating system level. It is installed on a customer server from where each single user has access from various PCs or tablets.
- The software can be updated via respective digitally signed installers. Only installers supplied by IBA Dosimetry must be used.
- The myQA® Daily hardware component can be controlled remotely via a web browser (of the host or a remote workstation) if it is connected to a network. Accessing the device from a web browser other than specified may introduce risks related to the product safety, usability, or cybersecurity. The following browsers have been tested:
    - Chrome v112 or later for Windows

- Firefox v112 or later
- Mobile Safari v16 or later
- Android Browser: Chrome Mobile v119 or later
- Microsoft Edge v113 or later

What kind of data is stored and handled?

- The measurements taken with the myQA® Daily are related to a treatment machine rather than to an individual patient. The myQA® Daily does not handle or store any personal health information (PHI) or other kind of personally identifiable information (PII) except username and display name. Username and display name are stored and may be exported e.g., as part of PDF reports.
- The admin role and password are not directly attributable to a specific person since several users can assume this role. There is no other confidential data handled or stored on the instrument.
- myQA® Daily ensures by using authentication via login that only authorized users have access to the system. If user has no login, it is not possible to use the software.
- The myQA® Daily application stores the following data:
  - User account information (username and password) in the SQL database.
  - Device information on the device itself and in the application to manage and interoperate with devices.
  - Configuration data, such as the connection configuration.
  - Measurement history required for the QA workflow and analysis in the SQL database.
  - Log files, such as diagnostic logging on the workstation and audit trail logging in the SQL database.
- The myQA® Daily allows the export of measurements via the application UI or API.
- The following ports are used for handling communication:
  - 1338 (TCP) for communication over WebSocket.
  - 1348 (TCP) for communication over GRPC.
  - 5355 (TCP) for LLMNR.
  - 5353 (UDP) to support the search for online devices.
- The following ports are used in addition when the config interface is activated:
  - 80 (TCP) for http access.
  - 443 (TCP) for https access.
  - 19531 (TCP) for systemd-journal-gatewayd logfile access.

TLS Certificate

- The myQA® Daily provides out of the box functionality to either use HTTP (default) or HTTPS. The myQA® Daily software uses port 58321 as default for communication. HTTPS can be explicitly enabled via the system's configuration file and its use is advised. Please note, neither option provides the full level of cybersecurity nor may thus pose a security risk.

- It is recommended that, if possible, a properly signed TLS certificate is used. Both TLS v1.2 and v1.3 use SHA-256 in its pseudorandom function (PRF) and for the finished message hash and thus provide better security over older versions. Both versions are supported and can be used via the system's configuration file.
- The use of certificates is supported either by using certificate files or a certificate storage. The certificate source can be set via the system's configuration file. Please note that the use of a self-signed certificate may pose a security risk.
- Advised adjustments as outlined above can be made by changing the system's configuration file located at **%ProgramData%\IBA Dosimetry\myQA Daily\appsettings.json**. The following screenshot shows the content of the configuration file.

```
{
  "HttpServer": {
    "Endpoints": {
      "Http": {
        "Host": "localhost",
        "Port": 58321,
        "Scheme": "http"
      }
      //"Https": {
      //  "Host": "localhost",
      //  "Port": 44340,
      //  "Scheme": "https",
      //  "CertificateFilePath": "localhost.pfx",
      //  "CertificatePassword": "YourSecurePassword"
      //}
    }
  }
}
```

  - To enable HTTPS for communication, uncomment the section "Https" by removing the "//" for each line.
  - To use a certificate update "CertificateFilePath" to point to the certificate file and provide the respective certificate password via "CertificatePassword".

Which measures are implemented by IBA Dosimetry to support safe and secure operation?

- All login data are encrypted.
- Use of TCP/IP as transport protocol.
- Communication between workstation and myQA® Daily uses our proprietary Hermes protocol and is secured with TLS.
- Event logging (audit log) for measurement and user related operations (Read, Write, Update, Delete).
- The installers have a digital signature.
- An MDS-2 form is published for the myQA® Daily application and is available from our customer support team.
- The source code is continuously scanned for vulnerabilities. We are employing software to regularly assess and improve the code quality during development.

- The admin can further improve the security and ensure the identity of the myQA® device on the IT network by uploading a valid TLS certificate from a trusted provider; thus, securing the communication and data transfer between the device and the PC or tablet.
- Access to the system is protected by a strong password, which is stored as a salted hash. The myQA® Daily requires the users to change their passwords every 30 days by default. The recurrence period can be adjusted via the Settings page of the application by users with the admin role as shown in the screenshot below.
- Auto-Logoff for sessions after a configurable time of inactivity. The logout time can be adjusted via the Settings page of the application by users with the admin role as shown in the screenshot below.

Which CyberSecurity measures are expected to be implemented by the operator (health care provider)?

- General requirements expected:
  - State of the art virus scanners and firewalls for the tablet and PC are used.
  - Prescribed maintenance is done as required, including installation of security patches.
  - Windows session timeout for web application session is configured according to local policy.
  - Access control to the medical devices and network access points is established (physically and electronically). Internet access is appropriately protected. Adequate password policy is implemented.
  - It is recommended to use WPA2 encryption or later if Wi-Fi is used.
- The myQA® Daily does not require an internet connection to function, it can be connected via the local network (wired or wireless), and therefore will be part of an environment that is exposed to cybersecurity threats. This presents a possible security risk. To minimize the chance of an attack IBA recommends the following:
  - Immediately define the admin password.
  - Restrict access by only allowing authorized users to access your network.
  - Use file sharing with caution and avoid sharing over public networks.
  - Ensure your access point software is patched and up to date.
  - Software updates provided by IBA should be deployed to provide highest level of security.
  - It is recommended to back up regularly and prior to updates (see instructions for use).
- The use of the myQA® Daily (especially via remote control) on an IT network could result in previously unidentified risks to patients, users, and third parties. It is therefore recommended to the customer's risk management team, to identify, analyze, evaluate, and control such risks, especially in case of changes to the IT network.
  - Changes in the IT network configuration.
  - Addition of items such as hardware and / or software platforms or software applications to the IT network.
  - Removal of items from the IT network.
  - Upgrades of hardware and / or software platforms or software applications on the IT network.
- While no cybersecurity issues are known at the time of release of the myQA® Daily we cannot completely rule out that in the future previously unidentified vulnerabilities or security issues might arise. It is

therefore recommended that the customer's risk management team performs a risk assessment related to the use of the myQA® Daily in the IT network.

We care: what happens in the case of a CyberSecurity incident?

- IBA Dosimetry is available for you 24/7. We welcome any notification about any cybersecurity event or suspected vulnerability involving IBA hard- or software products.
- Please feel free to call our customer support team or file a request in our helpcenter (see contact information and link below).
- We will handle such reports with high priority, and you will be continuously informed about the progress. If necessary, we will publish a security patch.

Please contact the: IBA Dosimetry Help Center (helpcenter.iba-dosimetry.com) with any further questions

USA, Canada, and Latin America	Europe, Middle East, Africa	Asia Pacif
Phone: +1 786 288 0369	Phone: +49 9128 607 38	Phone: +65 3129 2472
service-usa@iba-group.com	service-emea@iba-group.com	service-apac@iba-group.com