myQA PROactive CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information on myQA PROactive 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 intended use of myQA PROactive is to support a risk management team in the prospective risk management (based on TG100) of a clinical workflow, to identify risk and introduce corrective measures when necessary.
- The software can be deployed as a single workstation installation or as an intranet server application.

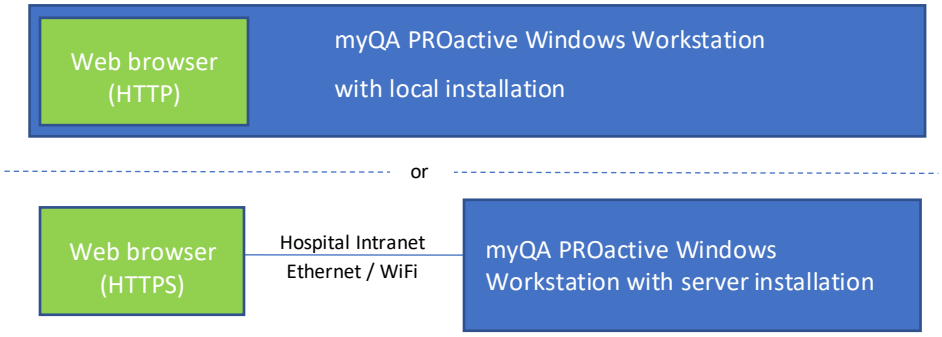
Are there any operating systems or application software supplied?

- The myQA PROactive Software package runs on Hardware provided by the operator
- The operating system must be provided by the operator IT
- The must be accessed with a web browser. The following browsers have been tested:
  - Google Chrome, Microsoft Edge, Firefox
  - Please keep your browsers up to date!

What kind of data is stored and handled?

- The server stores the following data:
  - Software error logs
  - Created risk analysis
  - User data (names, emails, phone numbers if provided)
  - Optionally the application saves incident data for risk analysis validation
- Ports for HTTP and HTTPS access (as configured; 80/443 recommended)

How does the system architecture look like?



Interfaces

- Excel import/export
  - For initial risk analysis data import and append
  - For incidents for risk analysis validation
- PROactive file import/export (.proactive)
  - The application has the capability to export individual Risk Analysis as proprietary XML files
- Proactive form template import/export (.proactive-form-template)
  - The application has the capability to import/export form templates for the purpose of incident analysis

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

- Our source code is continuously scanned for vulnerabilities. We are employing software to regularly assess and improve the code quality during development.
- Data files can only be accessed by staff with administrative privileges on the server.
- Communication between workstation and server uses mandatory TLS.
- Logging (of software error conditions and failed login attempts).
- Updates to the myQA PROactive Software package are signed and protected with a hash value (SHA-256). This hash value can be used to verify the authenticity of the update file received.
- Our source code is continuously scanned for vulnerabilities using SonarQubePrerogatives of different user roles:
  - Administrator: full control on users and groups
  - Leader: full control on risk analysis data
  - Member: limited write rights on risk analysis data
  - Guest: read-only access to risk analysis data
  - Safety officer: the only role which allows to user to see and manage incident data

What if the server is unavailable or data is corrupted?

Non-availability of the application does not have a direct effect on patient safety, nor does it cause a security risk.

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. An adequate password policy is implemented.
- Administrative privileges
  - Only qualified personal should manage the system on which the application is deployed
- Software updates
  - Updates provided by IBA should be deployed to provide highest level of security
- Server operation
  - When running as a server TLS (Transport Layer Security) is mandatory and therefore a valid certificate must be provided by the customer
- Local data backups
  - It is recommended to back up the data files regularly and prior to updates (see manual)
- While no CyberSecurity issues are known at the time of release of myQA PROactive 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 PROactive 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.