myQA Accept with Blue Phantom-2 / CCU CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information on the Blue Phantom-2 / CCU and myQA Accept software for IT personnel.
This information will help ensure the secure and safe use of the system in clinical practice.

What is the system used for?

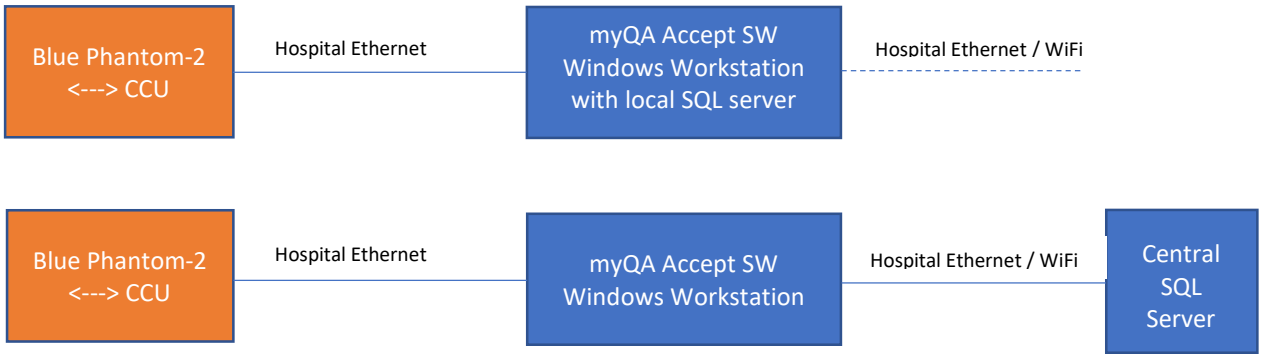
For cancer treatment, Linear accelerators apply ionizing radiation to a patient, by delivering a Dose with different energies, patterns and from different angles.

- The purpose of the system is to measure, verify and analyze radiation dose distributions.
- The Blue Phantom-2 is placed under the linear accelerator, and certain predefined dose distributions are applied. The device records the dose distribution characteristics by scanning through the radiation field in three dimensions with an appropriate detector. The result is compared to the reference data stored in the myQA Accept software. If there are significant deviations, it can be assumed, that the radiation cannot be delivered to a patient as intended. The Linear accelerator will be checked for errors.

What if the measurement device fails or measured data is corrupted?

In this case, the comparison of recorded characteristics vs reference data will fail, the patient will not be treated, and the medical physicists will start a root cause investigation.

What does the system architecture look like?



Are there any operating systems or application software supplied?

The Blue Phantom-2 / CCU is used with the myQA Accept Software package which is delivered together with the system.

- The myQA Accept Software package runs on Hardware / OS provided by the hospital IT.
- The CCU firmware contains an operating system based on NXP MQX version 2.5. For updates (including any security patches), only firmware files supplied by IBA Dosimetry must be used.

What kind of data is stored and handled?

- The myQA Accept Software does not use or store patient related data, nor any personally identifiable data related to patients or users.
- The CCU stores the following data:
  - Linearization values of sensors.
  - Network settings.
- The myQA Accept Workstation stores the following data:
  - TPS transfer files generated from the measurements.
  - Data on radiation device & measurement device.
  - Software error logs.
- The local or central SQL Server stores the following data:
  - Measurements acquired with the Blue Phantom-2 / CCU electrometer.
- The following data are transmitted between workstation and CCU:
  - Commands to move the Blue Phantom-2 to specific positions or to setup the CCU electrometer.
  - Measurements acquired with the Blue Phantom-2 / CCU electrometer.
- The following data are transmitted between workstation and SQL data base:
  - Measurements acquired with the Blue Phantom-2 / CCU electrometer.

- Ports:
  - The myQA Accept Software communicates via the clinical network with the CCU and, where applicable, the database on the central SQL server.
    - For the database, the default port is 1433. It can be changed during installation of the database.
    - The port for the CCU can be configured using the XXSetup Tool (delivered together with the myQA Accept Software).
- Encryption
  - No encryption is applied to the data and logfiles.

Interfaces

- If this option is purchased, the myQA Accept Software is able to create transfer files for the transfer of measurements to a treatment planning system. In some cases the transfer is handled directly from the corresponding software module (using a binary format), in other cases ASCII files are created which are to be transferred manually by the user. The clinic is supposed to take appropriate technical and organizational measures to protect those files when in storage, and their transfer to the TPS (normally done via the clinical network).

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

- Access to SQL server requires authentication (SQL server user defined during installation).
- Communication between workstation and CCU uses TCP/IP as transport protocol.
- Logging (of software error conditions and relevant modification of data).
- The correct format of any data is verified upon opening the data from myQA Accept.
- A MDS-2 form containing further details is published for the myQA Accept Software package, and is available from our customer support team.
- Updates to the myQA Accept Software package are 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 SonarQube.
- The myQA Accept Software does not use the Java log4j library and is therefore not affected by the Log4Shell software vulnerability (CVE-2021-44228, published Dec. 10th, 2021).

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 are used.
  - Internet access is appropriately protected.
  - Server and Client machines are regularly patched from Windows updates.
  - One separate Windows account is created per each natural person, and Windows session timeout is configured according to local policy.
  - Strict hospital-typical access control to the medical devices and network access points is established (physically and electronically).
  - A backup of the SQL database (or the file system, if this option is chosen) is performed frequently.
  - If the application / database is hosted on a third party (Cloud-based) server: ensure the Cloud solution vendor/provider follows the security standards and requirements.
  - Prescribed maintenance is done as required, including installation of security patches and upgrades to the latest version of the software.
    When a particular release reaches the end of support, IBA Dosimetry may no longer be able to reasonably provide security patches or software updates for this release. If the software remains in use following the end of support, the cybersecurity risks can be expected to increase over time.
- Device specific:
  - None.

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

- IBA Dosimetry is available for you 24/7. We welcome any notification about a cybersecurity event or a suspected vulnerability.
- 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.