Contents

[Terminology 2](#_Toc531335253)

[Background 2](#_Toc531335254)

[Environment 2](#_Toc531335255)

[Platforms 2](#_Toc531335256)

[Zone 1 2](#_Toc531335257)

[Description 2](#_Toc531335258)

[Networking 2](#_Toc531335259)

[Security 2](#_Toc531335260)

[Zone 2 2](#_Toc531335261)

[Description 2](#_Toc531335262)

[Networking 2](#_Toc531335263)

[Security 3](#_Toc531335264)

[Zone 3 3](#_Toc531335265)

[Description 3](#_Toc531335266)

[Networking 3](#_Toc531335267)

[Security 3](#_Toc531335268)

[Operation 3](#_Toc531335269)

[User Management 3](#_Toc531335270)

[Connectivity 4](#_Toc531335271)

[Data Management 4](#_Toc531335272)

[Product Integrity 4](#_Toc531335273)

[System Maintenance 5](#_Toc531335274)

# Terminology

ACL – Access control list

DICOM – Digital Imaging and Communications in Medicine

PACS – Picture Archiving and Communication System

RDBMS – Relational Database Management System

SRM – Safety Risk Management

SQL – Structured Query Language

# Background

(XYZ) is the latest release of (123)

# Environment

Figure 1 illustrates the relationship between the (123) software application and other key elements of the (ABC) system. Zones 1, 2, and 3 illustrate relevant interconnectivity interface boundaries which also correspond to typical physical and network boundaries.

Figure 1 - (XYZ) System Block Diagram

## Platforms

The (XYZ) software is capable of running on a (ABC).

## Zone 1

### Description

This zone corresponds to the medical facility’s surgical environment.

### Networking

Device interconnectivity can be with other Medtronic medical devices or with devices supplied by the medical facility. This connectivity typically involves a point-to-point, wired connection. The information passed across these connections is limited to patient imaging data and related patient image, metadata. There are no remote access or control capabilities accessible on this link.

### Security

To gain access to the operating environment typically requires access to restricted areas of the medical facility. Control of these areas is part of the site’s overall security management policies and practices to limit physical access to only authorized personnel.

## Zone 2

### Description

This Zone corresponds to the institution’s private sub-net supporting the medical facility’s surgical area.

### Networking

The primary use of networking into Zone 2 is to obtain patient scan (CT, MRI) data from the medical facility’s PACS using the DICOM standard. This connectivity typically involves a networked, wired connection. The information passed across this connection is limited to supporting the DICOM protocol for obtaining patient imaging data.

With the exception of metadata, this is a unidirectional channel. The Device requests patient image data from the facility’s PACS system but does not transfer any data back to the PACS system.

While access to the Zone 2 network and associated assets is not as strictly controlled as the Zone 1 network, medical facilities typically incorporate various types of secure policies such as

1. Managing user ACL’s to control access to assets connected in Zone 2
2. Establishing and following policies and practices for adding devices to the Zone 2 network
3. Strictly limiting access from other networks such as found in Zone 3.

### Security

The DICOM standard is inherently insecure and highly dependent on site-specific installation and security policies.[[1]](#footnote-1) While the DICOM standard covers mechanisms for Application Entities to authenticate each other, detect tampering with or alteration of exchanged data and protection of the exchanged data, it specifically does not address user identification or user authorization.

Any security features are also dependent on the specific DICOM installation and security policies of the medical facility.

## Zone 3

### Description

This Zone corresponds to any networks, both public and private, that are not part of Zones 1 or 2.

### Networking

Zone 3 is sufficiently isolated and protected from Zone 2. The Device does not interact directly or indirectly with any entity located in Zone 3.

### Security

Because the Device does not communicate with any system located in Zone 3, any Zone 3 security policies and adherence to any Zone 3 security policies does not affect the Device.

# Operation

## User Management

(XYZ) does not support any type of remote operation so a user must physically interact with the Device to use (XYZ). A physical presence requires access into Zone 1 of the medical facility and is limited to authorized personnel only.

The Device contains modem hardware capable of supporting a remote, dial-up session. Invoking this capability requires physical access to the device including manually connecting an analog phone line and launching the modem communication utility.

## Connectivity

Table 1 summarizes the connectivity options for the (XYZ) application. General network connectivity and communication is not supported. Only required network ports are available and those ports are explicitly managed along with the release of (XYZ).

There is no support for generic wireless communications. No wifi capabilities are included on the Device and Bluetooth support is limited to supporting a supplied bluetooth mouse.

The Device relies on the network protection mechanisms (firewalls, intrusion detection) provided by the medical facility for any networking outside Zone 1.

|  |  |
| --- | --- |
| Table 1 - Device Connectivity | |
| Type | Details |
| Other Medical Devices | Connectivity is limited to imaging devices co-located with the Device and possibly the transfer of surgical planning information from an instance of (XYZ) running on a (ABC) to (XYZ) running on a Device. |
| Other Networks | Connectivity is limited to any network required to gain access to the facilities PACS system |
| Internet | The Device does not connect to the internet |
| Portable Media | The Device does not provide a generic mechanism to read from or write to removable media (either CD/DVD or USB). The Device provides built in support to transfer patient data onto the Device and provides support to copy plan and procedure data onto the removable media. |

| Table 2 - Device Networking Ports | |
| --- | --- |
| Ports | Use |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Data Management

Patient and procedure information can be stored on a Device in a proprietary format. (XYZ) does not include any RDBMS or SQL related technologies.

## Product Integrity

Installing (XYZ) involves physical access to the Device along with manually invoking the installation process which in turn copies a set of files onto the Device. There is no provision to remotely install (XYZ).

## System Maintenance

The (XYZ) product is deployed as a combination of both the (XYZ) application software as well as the supporting operating system environment.

Installing any Device software product including (XYZ) requires the use o a proprietary installation mechanism. Once installed, no further updates or changes to (XYZ) are made.

Because the installation of (XYZ) includes a dedicated operating system, there is no mechanism to introduce a security risk to any other Device software. Because no field updates are performed on (XYZ) once it has been deployed, there is no mechanism to introduce a security risk into the (XYZ) application.

Other, supporting software products can be replaced on the Device with newer versions of the same software product. Examples of this class of product include but are not limited to the following: foo, bar, panda.

To assure continued safe and effective device use, the systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up-to-date protection and to address the product life-cycle.

Device instructions for use and product specifications related to recommended anti-virus software and/or firewall use appropriate for the environment of use, even when it is anticipated that users may use their own virus protection software.

1. DICOM Standard Part 15: Security and System Management Profiles; Section 1.1 Security Policies and Mechanisms [↑](#footnote-ref-1)