Radlink
PRECISION DIGITAL IMAGING

Information Technology & Information Security FAQ

System Overview

What operating system does the solution require?
The Radlink GPS uses Windows 10 OS (64 bit) Enterprise. The Radlink GPS Tablet uses Windows 10 OS (64 bit) Professional.

What hardware and software is required for the system?
The necessary hardware and software is provided by Radlink as part of the system.

What users are expected to be using the solution?
Surgeons, x-ray techs, implant reps.

Is the system client-server or hosted/ASP?
The Radlink GPS is a standalone system.

Does the system include a mobile app?
No.

Will there be a test system built and maintained throughout the use of the product?
No.

Can the application run on a virtual machine?
No.

Does the client require client-side middleware?
No.

Are all device components maintaining private data (other than removable media) physically secure?
Yes.

Is a list of third party applications provided by the manufacturer available?
Yes.

Are all shared resources which are not required for the intended use of the device disabled?
Yes.

Are all communication ports which are not required for the intended use of the device closed/disabled?
Yes.

Are security-related features documented for the device user?
Yes.

Does the system have the capability to impose access control on the basis of functions such as Create, Read, Update, and Delete?
No.

What is the size of the image files?
C-Arm images are 1-2 Mb and X-ray images are 8 Mb.

System Access

Does the system use role-based access?
Yes, standard windows user authentication is used.

Can the customer organization assign, modify, and terminate user access?
Yes, this is done by editing or removing the Windows user account through the administrative account given to the IT department.

Are the number of Administrator, Root, or SA privilege accounts limited?
Yes.

Is a back door built into the system?
No.

Does the system provide the capability to generate an administrator-configurable warning banner?
Yes.

Can the system be set to automatically save and log-off users after a period of inactivity?
Yes, the system can be set to lock the screen after 3 hours of inactivity and log off after 5 hours.

Who sets the auto log-off timeframe?
Only the administrator can set the timeframe.

Does the system block user access after a pre-determined number of unsuccessful password attempts?
Yes, this is set to a default of 50 attempts, which can be changed.

What are the default settings for passwords in the system?
Default passwords are assigned and can be changed upon arrival.

Does the system require the use of well-known privileged accounts?
No.

Are dev, test, and other special user accounts removed before the application goes into production?
Yes.

Remote Access

What type of technology is used for remote access and support?
Logmein over https if allowed.

Can a remote party recipient adequately protect data after receipt?
Yes, Radlink maintains and supports proper HIPPA and PHI procedures.

Can the system restrict remote access to/from specified devices or users or network locations?
Yes. IP address filtering can be set up to allow only certain devices to remote access the system.

Can the system be configured to require the local user to accept or initiate remote access?
Yes.

Does the system track remote support activities to the individual user level?
No.

Authorization and Authentication

What type of authentication is used?
The system allows unique user IDs to be created for each user and a password for each ID.

Does the system work with single sign-on applications?
Yes, if active directory is enabled and configured.

Does the system support integration with Microsoft Active Directory?
Yes, at a user level.

What are the requirements for the password?
This is customizable but the default requirements are:
Passwords must be reset every 90 days and will have the following requirements:

- Not contain the user’s account name or parts of the user’s full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Are any shared user IDs used in the system?
No, the system comes with one user account and additional accounts can be created.

Can the device be configured to authenticate users through an external authentication service?
Yes.

Can users be assigned different privilege levels based on roles?
Yes, the system comes with one administrator account and one general user account.

Can the customer reconfigure product security capabilities?
Yes

Does the system support the use of two-factor authentication?
No.

Are the users forced to change passwords after first log-in?
Yes, for new user accounts that are created, not for default accounts.

Does the system support LDAP authentication?
Yes.

Is the system compatible with VCS high availability software (Symantec)?
N/A

Does the system incorporate an emergency recovery feature?
Yes, contact technical support in case of loss of all passwords.

Does the system provide any means of node authentication that assures both the sender and recipient of data are known to each other and are authorized to receive transferred information?
Yes.

Encryption

Is data at rest encrypted?
Yes, Windows 10 Operating Systems all have full data encryption using BitLocker.

Where is ePHI (electronic protected health information) stored?
ePHI is stored onsite.

Is ePHI stored with encryption?
Yes.

Is data in transit encrypted?
No.

How often are system security patches monitored and updated?
All updates are off but Radlink will notify registered sites of critical security patches.

Is there a firewall and anti-virus protection?
Windows Defender and Windows Firewall are included in the system.

Is there an anti-virus exclusion list?
No.

Is HL7 message encryption supported?
No.

Does the system employ any hardening measures?
No.

Does the system employ any mechanism to ensure the installed program/update is the manufacturer-authorized program or software update?
No.

Audit Controls

Can the system create an audit trail?
Yes, it is configurable via Windows Audit Policy.

Can the customer run the audit trail?
Yes.

What is included in the audit trail?
It can include all activity including login/log off, restarts and hard shut downs and opening of software, along with the user ID and date/time to identify individual events.
Windows audit policy events:

- Account logon events
- Account management
- Directory service access
- Logon events
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

How are the system event logs accessed?
They can be accessed through the Windows Event Viewer interface and are stored in the Windows system drive.

How long are the audit reports maintained?
This is configurable via Windows Event Log properties.

Data Management

How are the data on the system secured?
1. The hard drive is fully encrypted

What database management system is used?
MySQL version 5.7.16.0 is used.

What type/class of server does the database management system run on?
It runs locally on the system.

Can the customer organization install and use the system with existing organization tools, policies and procedures, etc.?
Yes.

What PHI or PII data is generated, processed, stored, or transferred?
Name, Date of birth, medical record number, diagnostic/therapeutic data, and open, unstructured text entered by the user.

What PCI data is processed, stored, or transferred?
N/A

How is private data maintained?
The system can maintain private data, stored persistently on encrypted local media, import/export with other systems, and during power service interruptions.

Does the system provide an integral capability to de-identify private data?
Yes.

How is data backed up?
DICOM images are archived into hospital PACS when the user initiates. Data can also be stored on portable media.

How often are backups tested?
The user initiates and reports any errors.

How long can the data be stored?
Data on the system is kept until the user deletes it.

What portable media types are used by the system?
USB and CD/DVD drives allow importing and copying of x-ray images.

Can the system generate hardcopy reports or images containing private data?
No.

Can the system import private data via scanning?
No.

Does the system ensure the integrity of stored data with implicit or explicit error detection/correction technology?
Yes, the integrity is enforced by the DICOM standard

Is the data retrievable, readable, and able to be integrated into a different system should the vendor go out of business?
Yes.

Does the file system allow the implementation of file-level access controls?
Yes.

Network

What kinds of data connections are required?
Wifi connection or wired Ethernet connection to hospital RIS/PACS is required. Both connection types can be used.

What wireless environment and security are used?
Wifi 802.1x(A/B/G/N/AC) and WPA2- Enterprise.

What web servers does the system support?
None.

Does the web application use HTTPS?
N/A

Is private data transmission restricted to a fixed list of network destinations?
Yes.

Does the system support any mechanism intended to ensure data is not modified during transmission?
Yes, the system uses a fully HIPAA compliant PACS system to ensure data is not modified during transmission.

Maintenance and Support

Who is responsible for ongoing maintenance?
The customer is responsible for preventative maintenance and Radlink is responsible for anything beyond routine maintenance.

What is the policy on Windows OS Updates?
Automatic Windows updates are disabled, and Radlink will be in charge of testing and applying critical security updates.

Does the system require a system administrator to maintain the software and/or hardware?
No, but a local system administrator is encouraged to maintain the user accounts.

How often are updates performed to the application?
Updates are performed at least once every six months and registered sites will be notified by Radlink.

What is the process for deploying emergency patches?
Radlink will notify registered sites of critical patches and security updates after they become publicly available.

What is the warranty for the software, servers, hardware, etc.?
There is a one year warranty after purchase. If out of warranty, time and materials charges apply.

Does the vendor allow updates to the operating system by the customer without voiding the warranty or support agreement?
Yes, it is not recommended but it will not void their warranty.

Will the vendor or a third party with whom they contract have the ability to access the customer organization's PHI?
Yes, if granted access by a facility member. Only the minimum required number of technical support representatives needed to resolve the issue will be authorized to use the account.

Is the support account the same for all implementations of the system, software, etc.?
Yes.

Are all of the security features "on" or is controlled by the customer organization?
They are on and included with the system.

What are the hours for support?
Support is available 6AM – 5PM PST. Voicemail is available after hours.