RN-30: p.d 5.4 Security Overview

Purpose

The purpose of this document is to describe the .decimal p.d software and discuss the security features implemented in p.d to protect patient information. This document should provide answers to many of the commonly asked questions regarding the safety and security of the application.

Software Overview

p.d is a locally installed software application for which the primary purpose is to enable users of various radiation treatment planning systems (TPS) to design, calculate, measure, and order patient-specific radiotherapy devices that are custom manufactured by .decimal. These devices are typically either apertures/blocks or intensity modulators / range compensators. The general software workflow is to import patient information from the TPS via DICOM, then design and/or review the required patient devices (blocks and modulators) with p.d, and finally to order the devices. Additional functions are also available to check order status, digitize scanned electron aperture images, and export data back to the TPS via DICOM, which may also be frequently used by some facilities. Figure 1 describes the communications between the p.d software, .decimal servers, and TPS computers.

Fix Me!

General Security Information

As seen in Figure 1, p.d receives all information from within the local institution via DICOM file transfer. This DICOM information does include PHI and PII and p.d stores a copy of much of this information on the local computer in the protected App Data folder of the active Windows computer user. The application uses a simple database that contains no PHI or PII to reference the record files stored for each patient. These record files are stored in a proprietary format and are encrypted at rest using an AES 128-bit cipher whose key is only accessible from within the p.d software. This encryption should be considered as a secondary safety measure only and its main purpose is to prevent alteration of the data files outside of the p.d software. As such, .decimal recommends that all workstations using p.d utilize full hard drive encryption to meet general security best practices (e.g. BitLocker). Also, it should be noted that all patient critical treatment information is either already in the TPS or must be sent back to the TPS from p.d, therefore data stored by p.d should not be considered part of the authoritative patient treatment record. As such, the need to backup or otherwise include redundant copies of the p.d database is simply

not necessary.

Like all TPS software, p.d does display PHI and PII on the screen during use, so standard precautions should be taken to ensure the local PC locks when idle and is otherwise protected from unintended access. Each p.d installation maintains a log of all login, import, export, and order events that can be reviewed if misuse is suspected. Users of the p.d software are general radiation therapy professionals, including dosimetrists, therapists, and medical physicists.

Since the primary purpose of using the p.d software is to order devices for patients, there is a necessity to transmit device manufacturing parameters and information to .decimal servers. In order to protect patient privacy, our proprietary order file format contains only the minimal data necessary to manufacture the requested device (a full description of the file format can be found at the end of this document). These files do not include PHI or PII or any sensitive customer billing/payment information, although customers can optionally include their internal Medical Record Numbers in the files to ensure invoices received from .decimal can be linked to the appropriate patient. The following are some additional features of note regarding the p.d software:

- The software is installed on a per user basis on Windows based PCs
- Authentication with .decimal servers is required to access the software and all user data is saved in their local Windows directory, preventing access from other accounts
- Communication between p.d and .decimal servers uses a TLS connection
- Each device file created by p.d is transferred to .decimal servers using a secure HTTPS connection
- Before the file for each device is created, the patient name is anonymized such that only the initials are readable

We value the privacy of our customers and the integrity of all our customer data and we employ significant efforts to use IT security best practices regarding the installation, configuration, and management of our servers and other IT infrastructure (see Appendix below for further details). Despite these measures, it is important to recognize that our primary means of protecting our customers' sensitive data is to simply ensure that it never leaves their facility. The data received by .decimal from our customers is therefore intentionally limited, making many of the common questions regarding our policies and security measures with your data not critical to the protection of your patient or facility data (as we simply do not send your sensitive data to our servers). As such, users should not add PHI/PII data in any free-form text fields when ordering devices.

Internet Communications

p.d communicates to .decimal servers via the internet using the HTTPS protocol.

- Using HTTPS, p.d communicates with two different servers. p.d utilizes port 443 (HTTPS) to communicate with .decimal Direct (https://direct.dotdecimal.com or 64.128.252.104) while connected to the internet. Note that these are secure connections using TLS protocols.
- Users are authenticated and p.d is downloaded using the decimal Launcher. As such, the decimal Launcher Network Requirements must also be considered, implemented, and tested to ensure end users are able to login, download, and run p.d.

These ports must be open to passive communication with external addresses from the machine that is

running p.d. Note that all communication is initiated from p.d (i.e., there should be no need to forward incoming ports to the p.d workstation). However, you must ensure that the aforementioned addresses be allowed to communicate with the p.d workstation in order for the software to function properly. The communication with .decimal Direct is used for authenticating the user, ordering devices, checking the status of orders, and synchronizing machine setup information.

This protocol is also used to transfer data files that p.d creates for each device when placing an order. All data is transferred to the .decimal Direct servers using HTTPS.

Data included in device files

Data	Description
TPS Info	The name and version of the TPS where the files originated and the version of p.d
Patient Info	The anonymized patient name containing the patient initials and optionally the medical record (MR) number
Beam Number	Beam number associated with the device
Beam Description	The beam description associated with this device
Machine ID	The name of the LINAC used to create this device
Comp ID	The engraving string to be placed on the device
Comp Date	The date and time the file was created
Site ID	The .decimal assigned site ID number
Contact	The current user's contact information (name, email, and phone number)
Shipping Address	The shipping information entered or auto-populated in the order wizard
Billing Address	The billing information entered or auto-populated in the order wizard with the P.O. number
Required Delivery	The user selected required delivery
Comp Material	The material of the device
Comp Mount	The mounting position of the device
Device Dimensions	The estimated dimensions of the device
Source Comp	Source-to-compensator tray distance or source-to-aperture distance (depending on the device).
Surface or Polyline	Series of (X,Y,Z or X,Y) values in cm that represent the surface map or contour that describes the device. The format of each line is a series of two or three numbers separated by spaces.