Laurel Bridge Beacon
Privacy and Security Statement

Laurel Bridge Software, Inc.
302-453-0222
www.laurelbridge.com

Document Version: 1.4.3
Document Number: LBDC-000133-010403
Last Saved: 11/30/2022 9:34:00 AM

Table of Contents

1 Beacon Privacy and Security Statement

Because the Laurel Bridge Beacon application is installed on hardware that is provided, configured, and controlled by the Beacon customer, Laurel Bridge Software (LBS) cannot make assertions about the privacy and security of a particular Beacon installation. It is up to the customer to ensure that the host Windows system onto which Beacon is installed has been adequately secured and locked down. However, LBS does provide technology, tools, and guidance to assist customers in locking down their Beacon installations. In the context of this document, the term "Beacon customer" refers to the administrators for the host hardware system and for the Beacon application.

Section 1.3 - GDPR Notes found below contains comments regarding the European Union's (EU's) GDPR - General Data Protection Regulation.

An overview of the Beacon application privacy and security features is given in the sections below, roughly following the format given in the HIMSS/NEMA Standard HN 1-2013, "Manufacturer Disclosure Statement for Medical Device Security", or MDS2 for short. For more details about this form or to download it, see `http://www.himss.org/resourcelibrary/MDS2` (NEMA Document ID: 100382).

The headers in the following sections map directly to the headers in the MDS2 document. The Beacon MDS2 document for a particular release is available upon request from LBS.

1.1 Management of Private Data

The Laurel Bridge Beacon application acts as a QC station for DICOM studies, which may contain protected health information (PHI). Beacon can receive studies from one or more sources, allow authorized users to edit and sign the contents of these studies, and then send these edited/signed studies to a single destination. Consequently, Beacon can ingest, store, display, and transmit PHI. However, since the PHI only resides in Beacon temporarily, Beacon is not considered a primary repository of electronic health record (EHR) or electronic medical record (EMR) data, and thus is not maintaining part of the designated record set (as defined by HIPAA). Also, the Beacon application and the data it stores and manages is entirely resident within the customer premises (i.e., no part of the application or its data is cloud-hosted or hosted by LBS).

1.1.1 Types of PHI Maintained

Because Beacon handles DICOM messages, it potentially transports and caches the following types of PHI:

- Patient demographic information
- Patient medical record information
- Patient diagnostic and therapeutic information (including diagnostic images)

1.1.2 Persistence of Private Data

Beacon maintains PHI both temporarily in memory (while running) and on disk (persistent storage). PHI may be found in data transmitted or cached by the application, and in log files generated during use of the application. Data can be imported from other medical systems via

network-mounted hot folders or removable media, but these features must be explicitly configured by the Beacon customer, and their use remains under the full control of the customer. Available security features to protect PHI when at rest are described below and, in more detail, in the Beacon User Manual.

Note: Due to the sensitive nature of the PHI that Beacon handles, the only non-destructive and completely safe way to decommission a (non-virtual) computer system on which a production Beacon application has been running is to wipe the hard drive clean using a suitable hard drive wiping application. For self-encrypting drives, changing or overwriting the encryption key(s) may be sufficient.

1.1.3 Transmission of Private Data

PHI can be transmitted or received over the network via DICOM messages. The ability to configure and control the behavior of this functionality is under the full control of the Beacon customer, and the use of these features remains under the full control of the customer. Available security features to protect PHI when in transit are described below and, in more detail, in the Beacon User Manual.

1.1.4 Payment Card Industry (PCI) Data Security Standard

Because Beacon does not process any patient billing transactions, it is not subject to the requirements of the Payment Card Industry (PCI) Data Security Standard.

1.2 Security Capabilities

The Laurel Bridge Beacon application is comprised of two parts:

1. **Beacon Service**, which runs as a Windows Service
2. **Beacon Web**, a web application which is used to configure the Beacon Service, edit and sign studies, and monitor the system

The following sections briefly describe available security features of the Beacon application. For more details, see the Beacon User Manual.

1.2.1 Automatic Logoff

The Beacon Web application can be configured to automatically log off Beacon users in a configurable number of minutes. The default timeout is 10 minutes, and the timeout can be configured to any value from 1 minute to 65536 minutes. Note that enabling the web auto-refresh functionality on the status screen disables the web user auto-logoff.

1.2.2 Audit Controls

Beacon can be configured to send DICOM PS3.15 Appendix A.5 ("Audit Trail Message Format Profile") audit messages to a syslog server (such as **syslog-ng** or **nsyslog)**. Messages can be sent via the TLS (recommended), UDP, or TCP protocols, and all messages include the user ID of the user performing the action as well as a date/time stamp.

The following types of audit trail messages can be enabled/disabled independently:

- **Application Start/Stop** – Logs when an application is started/stopped.
- **Software Configuration** – Logs when changes are made to the software configuration.
- **DICOM Instance Network Transfer** – Logs when DICOM instances are transmitted via the network.
- **DICOM Instance Import** – Logs when DICOM instances are imported.
- **User/Security Alerts** – Logs when web user or security alerts occur.
  These include events such as web user logon/logoff, web user addition/removal, web user password/role changes, and any modifications of DICOM data.

The following DICOM PS3.15 Appendix A.5 audit trail message types are supported by Beacon:

- **Application Activity**
  - Application Start
  - Application Stop
- **Begin Transferring DICOM Instances**
- **Data Import** (optional configuration)
- **DICOM Instances Accessed**
- **DICOM Instances Transferred**
- **Security Alert**
  - Security Configuration
  - Software Configuration
  - Use of Restricted Function
  - User Security Attributes Changed

- **User Authentication**
  - Login
  - Logout

1.2.3 User Authorization

The Beacon Web users can either be locally administered (by the Beacon Web application), or they can be administered using LDAP / Active Directory. This is done by the Beacon customer configuring one or more Active Directory groups for each of following built-in web user roles:

- Admin user
- Regular user
- View-only user

1.2.4 Security Configuration

The Beacon customer has full control over and responsibility for the security of Beacon, both through the ability to lock down the Windows system on which Beacon is installed, as well as through the ability to configure the security features built into the Beacon application. Extensive information about how to do this is found in the Beacon User Manual.

1.2.5 Security Updates

The Beacon customer has full control over the installation of Windows security updates, as well as over the installation of any Beacon application updates.

1.2.6 De-Identification of PHI

Beacon does not support the de-identification of PHI.

1.2.7 Backup and Restore

The Beacon customer has full responsibility to both install and maintain the SQL Server database which provides the backing store for the Beacon jobs. As such, the customer is also responsible for providing backup and restore capabilities for the SQL Server database. Microsoft provides an extensive set of SQL Server backup, restore, and replication technologies.

1.2.8 Emergency Access

Since the Beacon customer has full control over the installation and configuration of both the host system and the Beacon application itself, it is up to the customer to provide a means of emergency access (“break-glass” feature) by maintaining alternate access to administrative credentials for the systems involved.

1.2.9 Data Integrity and Authenticity

Since one of the primary functions of Beacon is to modify DICOM data, it is simply not practical to implement a mechanism whereby alteration of data can be detected. Instead, the following techniques can be used to control and track data modifications:

- Use Audit Trail logging to record any access to or modification of data.
- Use Windows Authentication to ensure that unauthorized Windows users cannot access the host Windows system on which Beacon is installed.
- Use Beacon Web authentication (either locally administered or using Windows Authentication) to ensure that unauthorized web users cannot access the Beacon data remotely.
- Use TLS encryption on the network connections used by the system to ensure privacy, node authentication, and protection against man-in-the-middle (MITM) attacks.

Beacon does not currently use explicit error detection on data at rest, but rather depends on the built-in ECC error detection and correction technology provided by modern hard drives (as supported by Windows). If data redundancy is desired, LBS recommends the use of RAID data storage technology for both the SQL Server database repository and for the DICOM image cache.

1.2.10 Malware Protection

Since the Beacon customer has full control over the installation and configuration of both the host Windows system and the Beacon application itself, it is up to the customer to install and maintain malware protection technology. Beacon itself should be unaffected by the use of such technology (beyond the obvious potential impact to system performance that can occur when using anti-virus software). For performance reasons, it is generally recommended that antivirus checking be turned off for the DICOM data directories and SQL data directories used by Beacon.

1.2.11 Node Authentication

Node authentication (the ability to confirm the identity of both the sender and receiver of DICOM data) can be implemented using TLS protocols on all network connections. Beacon supports TLS versions 1.0, 1.1, and 1.2 as both client and server. TLS must be enabled separately on DICOM inputs and outputs, as well as on the Beacon Web interface. More details about how to do this and further security details can be found elsewhere in the Beacon User Manual.

1.2.12 Person Authentication

As mentioned earlier, user authentication for the host Windows system can be controlled locally, using a domain with single sign-on technology such as LDAP / Active Directory. User authentication for web interface users can also be controlled either locally or using LDAP/AD.

1.2.12.1 Local Web User Administration

If you elect to administer web users locally, then there are no limits placed on the number of user accounts that can be created. Customers can and should immediately change default passwords during the installation process (there are only two default accounts, “Administrator” and a view-only user “Beacon”). Passwords must be a minimum of 8 characters long and must contain both uppercase and lowercase letters. Optionally, a high-security password mode can be enabled, which requires that passwords be a minimum of 12 characters long and must contain numeric digits, in addition to uppercase and lowercase letters. Shared user IDs can be used, but the default behavior is to only allow a user to log on from a single computer at a time. Local users’ passwords cannot currently be configured to expire.

1.2.12.2 Single Sign-On (LDAP/AD) Web User Administration

When web users are administered via a single sign-on technology such as LDAP/AD (recommended), the rules regarding users and passwords are up to the single sign-on technology. Active Directory allows for the configuration of password complexity and expiration rules, account locking, centralized account administration, etc.

1.2.13 Physical Locks

Since the Beacon customer owns and has full control over the host Windows system on which Beacon is installed, it is up to the customer to maintain the physical security of the host system.

1.2.14 Device Life Cycle Roadmap

The Beacon application currently supports the following Windows operating systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows 10

LBS intends to support each of these operating systems up until their respective end-of-extended-support dates.

In addition, the Beacon application has the following software dependencies:

- SQL Server (2012 x64, 2014 x64, or 2016 x64)
- SQL Server Management Studio
- .NET Core 3.1 (or later)

See also the Beacon User Manual section regarding prerequisites.

1.2.15 System and Application Hardening

Since the Beacon customer provides, configures, owns, and has full control over the host system on which Beacon is installed, it is up to the customer to perform system hardening, as well as to configure the Beacon application for the desired level of application hardening. More details about hardening of the host Windows system and the Beacon application can be found in the Beacon User Manual.

Some specific application hardening techniques that are supported by and/or implemented in Beacon include:

- Use of Authenticode digital signatures (currently SHA256) for all LBS executables and DLLs
- Support for TLS encryption for data in transit
- Provision of instructions for how to lock down the TLS protocols and ciphers, which affects both the Beacon Web interface, as well as any DICOM connections which are configured to use TLS encryption (see the Beacon User Manual for more details)
- Support for single sign on (Windows Authentication / Active Directory)

The implementation of the following lockdown techniques on the host Windows system is the responsibility of the Beacon customer:

- Disabling of unnecessary Windows accounts
- Disabling of unnecessary open network ports (e.g., telnet, ftp, etc.)
- Removal of any unnecessary off-the-shelf applications
- Enabling of Windows password-protected, inactivity-activated screen lockout
- Disabling of the ability to boot from removable media (if physical access to the host Windows system cannot be controlled)
- Enabling of BitLocker or other at-rest, full-disk encryption technologies (if desired)
- Enabling of SQL Server encryption (especially if the database resides on a different, unencrypted system)

1.2.16 Security Guidance

The security-related features of the Beacon application are described in detail in the Beacon User Manual.

1.2.17 Data Storage Confidentiality

Beacon does not encrypt data while at rest on the hard drive(s). PHI is stored both in the SQL Server database, as well as in the cached data files. If at-rest encryption of PHI is deemed necessary (e.g., if physical access to the host Windows system cannot be controlled), we recommend the use of a full disk encryption technology such as BitLocker or the use of self-encrypting drives. SQL Server at-rest encryption technologies such as Transparent Data Encryption (TDE) may also be necessary if the SQL Server database is resident on a different (unencrypted) system. Beacon does support encrypted SQL Server connections, and their use is highly recommended in the case of SQL Server instances accessed over a network.

1.2.18 Data Transmission Confidentiality

Beacon can be configured to encrypt data in transit (using TLS), which will protect the data against interception by unauthorized parties. And as mentioned above, Beacon supports encrypted SQL Server connections, and LBS highly recommends using them in the case of SQL Server instances accessed over a network.

1.2.19 Data Transmission Integrity

TLS encryption also protects the data against any attempt to modify the data during transmission (i.e., Man In The Middle (MITM) attacks). Beacon will only transmit data to destinations that have been explicitly configured within the application by the customer.

1.2.20 Other Security Considerations

Beacon can be serviced remotely by LBS only with the express permission of the Beacon customer, as access to the host system onto which Beacon is installed is completely controlled by the customer. Beacon does not contain any service backdoors, nor does it contain any secret service accounts. All LBS access to an installed Beacon application must be explicitly enabled/allowed by the customer using standard Windows secure remote access technologies.

The following port numbers are the defaults used by the Beacon application. Note that these can all be changed by the Beacon customer, if so desired.

- DICOM input port = **11112** (**2762** if using TLS)
- HTTP port = **10600** (**10601** if using HTTPS)

1.3 GDPR Notes

The European Union's (EU) General Data Protection Regulation (GDPR) is a refresh of Europe's data-protection laws that harmonizes statutes across the 28 EU member states; it became effective May 25, 2018. GDPR is a law that applies to any organization doing business in the EU or with EU-based clients. It is up to the Laurel Bridge application customer to ensure that they manage the Beacon application and the medical imaging data processed by it in a way that is conformant to their GDPR policies and practices.

The content in this document describes the relevant security and privacy information associated with this application. Relative to the GDPR some key points to remember are:

- The Laurel Bridge application is installed on virtual or physical systems that are provided, configured, and controlled by the customer, therefore Laurel Bridge Software (LBS) cannot make assertions about the privacy and security of a particular installation.
- It is up to the customer to ensure that the customer's host systems on which the application components are installed have been adequately secured.
- By virtue of using this application, Laurel Bridge Software receives no private data from the customer or the customer's clients; data remains with and under the control of the customer.
- The application does not maintain a designated record set and is not a primary repository of electronic health record (EHR) or electronic medical record (EMR) data. Data processed and tracked by the application is transient and purged after a user-configurable period of time.
- Section 1.1 in this document, Management of Private Data, describes private data that may be processed by the application and which may be relevant to the customer's GDPR compliance activities.
- Log files may possibly contain private data associated with the medical imaging data being processed. Such files should be handled in a way that is compliant with the customer's data retention and privacy policies.

