stryker

LIFENET® System

Security information for the LIFENET System

This information is being provided to help our customers meet the HIPAA Security Standards, and applies to the following components of the LIFENET system: LIFENET Adapter, LIFENET AED Event Viewer, LIFENET Alert, LIFENET Alert with archive, LIFENET Care, LIFENET Care app, LIFENET Care Client, LIFENET Connect, LIFENET Connect gateway, LIFENET Consult, LIFENET device agent, LIFENET Export, LIFENET mobile gateway, LIFENET PC gateway, LIFENET server, and Wi-Fi® Configuration Tool. The LIFEPAK® 15 monitor/defibrillator, LIFEPAK CR2 AED, and LUCAS® chest compression system are stand-alone products that interface to the LIFENET system and are covered under separate HIPAA statements.

Stryker performed a security and HIPAA assessment to review the LIFENET system with respect to the standards and implementation specifications of the Security Rule. The following information describes the security features and potential risks we have identified as a result of our assessment. In addition, it identifies possible administrative, physical and technical safeguards to help you, as a Covered Entity, establish processes and procedures for use of the Stryker products that are reasonable and appropriate for your institution.

Understanding the system capabilities, using its security features and implementing the recommended procedures can assist you in safeguarding electronic patient data as you use the LIFENET system. This information is not intended as an exhaustive list of recommendations. Your organization's particular needs and security requirements may call for additional actions and controls.

System use/technical features

The LIFENET system consists of a set of components designed to receive information transmitted from Stryker and third party monitoring devices in order to provide patient information from devices to remote care team members. The system can alert personnel when data has been received and forward a diagnostic quality 12-lead ECG from a LIFEPAK device which can then be viewed, printed, forwarded to another organization and sent to another user via e-mail attachment. In addition, data, including patient information and 12-lead ECG reports, can also be sent to clinicians through a dedicated smartphone app or the purpose of remote consultations and decision support. Patient data can also be exported from the LIFENET system in various formats so that the data can be incorporated into hospital systems as well as in the Stryker CODE-STAT™ data review product.

The LIFENET system consists of the following components:

- Gateways are software applications that run on a variety of platform types (e.g., modem, vehicle mounted personal computer, tablet PC) and transfer data from LIFEPAK devices to the LIFENET Server.
- The LIFENET Server is a hosted web system comprised of a set of servers and associated software. These servers route received data to target destinations. A web application is provided to configure routing information, manage users, monitor the status of the system, provide asset and device configuration and software management features and access comprehensive reporting tools including audit and job logs.
- LIFENET Care is a browser-based application that provides users with the ability to manage patients with non-emergency and emergency events. Users can receive incoming patient transmissions, images, videos and 12-Lead ECG information as well as request a consult, activate care teams and participate in group messages with selected users.
- LIFENET Care Client is an optional component installed on Windows-based devices to provide additional functionality such as providing notifications to incoming cases when the LIFENET Care application is closed.
- LIFENET Alert is a software application that runs on a windows-based computer, and provides users with the ability to print, view or forward received 12-lead ECG reports and vital sign reports, send an e-mail notification with the 12-lead ECG report attached or send a consult request and receive a consult reply.
- LIFENET Archive is an optional component of LIFENET Alert that allows users to store received 12-lead ECG reports on a local PC and export information to external systems, including CODE-STAT data review software, and Microsoft® Excel.
- LIFENET Adapter is a component installed with third party 12-lead ECG management systems that leverages XML and image file formats, importing them into the LIFENET system for distribution. Files received from the LIFENET Adapter are not altered in any way by the LIFENET system and are distributed in their original format.
- LIFENET Export is a component that allows 12-lead ECG reports to be exported to external systems (e.g., GE MUSE®), as HL7 aECG XML format that can then be imported by an external system.
- LIFENET Connect and LIFENET Connect gateway are components that allow data to move from a LIFEPAK device, DT EXPRESS™ software or CODE-STAT software into other CODE-STAT software installations via the LIFENET system.
- LIFENET AED Event Viewer is an application that allows you to receive streaming data from a LIFENET-connected AED device.
- LIFENET Care app is an application running on Apple iOS platforms, allowing users to receive incoming patient transmissions, images, videos, 12-Lead ECG information, receive care team activations and contains group messaging connecting selected users on both LIFENET Care and the LIFENET Care app.
- LIFENET Consult is an application that runs on the Apple iOS and Android platforms, allowing users to receive a consult request and associated patient and 12-Lead ECG information, and provide a consult response back to the requesting user at LIFENET Alert.
- LIFENET Device Agent is an application that runs on a Windows-based computer and provides the interface between the LIFENET system and LIFEPAK, CodeManagement Module®, and LUCAS 3, v3.1 devices for management of device settings and software.
- Wi-Fi Configuration Tool is an application that runs on a Windows-based computer that configures wireless networks on capable LIFEPAK and LUCAS 3, v3.1 devices.

Patient data

The LIFENET system passes pertinent patient data from Stryker devices and other select third party monitors to the LIFENET Server. A report is rendered at the LIFENET Server and is then distributed to destinations. Destinations may include LIFENET Alert or Care and Care app for printing or viewing, LIFENET Export for exporting to an external system, or CODE-STAT for data review via LIFENET Connect. Report data that is passed to LIFENET Alert is stored on the LIFENET Server for a period of time configured within the account (up to 7 days). During this time, LIFENET Alert users may select to forward the information via the server to another destination defined within the system, e-mail a copy of the report to a user defined within their account, export to a destination defined in an account or send the 12-Lead ECG report to a user to request a remote consult. Protected health information acquired and transmitted by the defibrillator is not stored long-term within the LIFENET system and Stryker does not have access to patient information. LIFENET Archive users can store received reports on their local PC indefinitely.

For LIFENET Adapter users, data will flow into a third party's 12-lead management system from that third party's field devices as per the established process for that equipment. The LIFENET Adapter, installed with the third party's 12-lead management system, will take the original file in an image format and send it to the LIFENET Server for distribution. Data from third party monitoring devices can be printed, viewed or exported (in image format only).

Potential security exposures

Examples of possible risks or disclosure of patient data include:

- Misconfiguration or purposeful damage to the system.
- Improper disclosure by an employer or outsider who acquires or copies electronic patient data.
- Unintentional disclosure of printed patient data when equipment is serviced or put into surplus.
- Unintentional disclosure of printed patient data when equipment is installed in an unsecured area.
- Improper disclosure or loss of printed patient data.
- Transfer of electronic patient data to the incorrect destination.

Product security features

Login controls: The following login controls have been implemented to help ensure that access to the website is limited to authorized personnel only: The LIFENET System website will automatically log users off after 15 minutes of inactivity and Automatic lock-out after 3 failed login attempts. Administrative users have the ability to set password expiration dates and define these expiration intervals. Consult users have an optional password configuration feature that requires a user to enter the password before viewing a consult request. Email attachments containing protected health information are encrypted and password protected.

Authentication: Access to the system is allowed after authentication with a user name and password. There are automated processes in place to authenticate new and existing user accounts. Gateways sending data to the system are authenticated by an identifier and password before data is accepted, and destinations receiving data are authenticated by an identifier and password before data is transferred to them. Consult and LIFENET Care app users are "invited" to be linked to requesting organizations, ensuring that any methods of communication or submission of information can only be sent to users that have been preapproved by the requesting organizations and that consult users can only receive requests from organizations that they have specifically accepted.

Auditing: All system access, configuration changes, transmission history and error conditions are recorded and available for review by the customer and Stryker system administrators. LIFENET Alert destinations can be configured to require users to enter either an account password or their LIFENET system credentials prior to accessing any patient information or modifying configuration options.

Patient identifiable information: All LIFENET system components that present or transfer patient data have a configuration setting that allows patient information to automatically be removed from reports and logs.

Encryption/decryption: All data paths between LIFENET components use TLS encrypted connections.

Email: The LIFENET system can send patient information through email Notifications. While email is not encrypted, we provide security features to help ensure patient privacy. You can password protect the patient information or you can configure the data to strip patient identifying information before sending.

Data integrity: Patient data files originating from LIFEPAK devices have associated CRC's (cyclic redundancy checks) that are checked for accuracy prior to opening the file for rendering, viewing or printing.

Data backup: All LIFENET system configuration data, audit information, and temporary patient files stored on the LIFENET Server are backed up regularly and encrypted. The patient data backups are only kept for 7 days. No patient data is stored long-term within the system.

Data storage: LIFENET Alert with Archive stores patient data on your local computer. If LIFENET Alert is configured to require users to identify themselves before being able to open any records, the same is then required in the Archive tab. LIFENET Care app temporarily stores records on the phone accessible only by our application.

Security features of LIFENET system

HIPAA standard	Security issue and feature	Recommended action
Login controls (implement policies and procedures authorizing access to system configuration).	If users change system routing information, electronic patient data could be routed to the wrong destinations or printer.	To help guard against misconfiguration of the system routing information, define user login levels and provide edit access only to individuals understanding the relationship between devices, gateways, sites, receiving targets and destinations.
Authentication	Unauthorized users could change routing information, resulting in electronic data being routed to the wrong destination or printer.	Use the password expiration feature to require users to change their passwords. Keep user names and passwords secure from unauthorized access. Have unique user IDs and passwords for each user.
Access control	If routing configuration is incorrect, data will not be received at the appropriate destination, and may be routed to an incorrect destination.	System End-to-End Testing — To ensure that patient data is received at the intended destination, perform an end-to-end data transmission test to ensure that data correctly moves from the LIFEPAK device through the Gateway and LIFENET Server to the appropriate destination. Also include checks to ensure that destinations that are forwarded to/from LIFENET Alert, LIFENET Care, Care application or users that are intended to receive e-mail notifications are correctly configured.
	If the computer used for LIFENET Alert, LIFENET Care or Care Client, or the printer configured for use is not adequately protected, unauthorized personnel could gain access to the viewed or printed patient data, and it could be copied, destroyed or sent to an unintended destination or user.	To prevent theft or unauthorized access to patient data, follow your organization's physical security policies and standards. Consider locating the LIFENET Alert, LIFENET Care or Care Client computer and printer so that access is permitted only to authorized personnel.
	If an iOS or Android device is not secured, unauthorized personnel may gain access to patient information via the LIFENET Consult and LIFENET Care applications.	Ensure the iOS or Android device is set to lock after a certain period of inactivity and enable additional passcode requirement at LIFENET Consult start or LIFENET Care application.
System health monitoring	LIFENET Alert, LIFENET Care or Care Client could be inoperable with no direct operator notification. LIFENET Alert, LIFENET Care or Care Client printer could be disabled and inoperable with no direct operator notification.	Review system health status and audit log information periodically to assure that all system components are operational. Define an account contact responsible for subscribing to and acting on system health notifications and audit log review. Implement a process to regularly review the audit log looking for unauthorized attempts to login into LIFENET Server accounts. Review audit log to monitor system routing information changes.
Security awareness training (to protect against malicious software)	Computers on which LIFENET system components are installed may not include anti-virus software or be automatically updated with service patch releases.	Install anti-virus software and any necessary security updates on the platform that LIFENET components are installed on, and define a process to ensure it stays up-to-date.
	Service patch releases or other application changes applied to the PC that LIFENET components resides on could inadvertently affect system operation. Service patch releases or other application changes applied to the platform that the LIFENET PC gateway resides on could inadvertently affect system operation.	Identify a person responsible for tracking security updates. Have a process in place for monitoring for and applying updates on an ongoing basis. Use the system test features to ensure the LIFENET Alert, LIFENET Care or Care Client destinations are functional and can receive data following any virus detection or security updates or application changes on the PC that the clients reside on. Use the system test features to ensure the LIFENET gateway is functional and can transmit device data following any virus detection, security updates or application changes to the gateway platform.

For further information, please contact Stryker at 800 442 1142 or visit our website at stryker.com

Emergency Care

02/2024
M0000018089 REV AA

Distributed by:

Physio-Control, Inc.
11811 Willows Road NE
Redmond, WA, 98052 U.S.A.
Toll free 800 442 1142
stryker.com