Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

Manufacturer or Representative Contact Information	Company Name Butterfly Network, Inc.	Manufacturer Contact Information Phone: (203) 458-7100 Email: support@butterflynetwork.com Web: https://butterflynetwork.com/contact
	Representative Name/Position Allan Bottemiller Medical Informatics Manager	

Intended use of **device** in network-connected environment:

Butterfly Network, Inc. (BNI) develops and manufactures point of care ultrasound (POCUS) products. Butterfly iQ, the POCUS device, has been cleared by FDA as a Class II medical device. Butterfly Network iQ Ultrasound is a single-probe, whole-body ultrasound device that plugs into a smartphone or tablet. Ultrasound studies are conducted using the Butterfly iQ connected to a smart mobile device. The Butterfly iQ mobile app is used to capture image/cine, associate patient information, and document exam findings. Upon completion of the study the provider can save the ultrasound study to the Butterfly Cloud. The Butterfly Cloud is used for the storage and quality assurance of ultrasound exams, as well as user provisioning, SSO/MDM integrations, and configuring DICOM or HL7 interfaces. Optional Telemedicine calls can be initiated between two Butterfly members. A trained ultrasound user can guide another novice user through tools in the web interface of the Butterfly Cloud.

MANAGEMENT OF PRIVATE DATA

		Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A		Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information**	Yes	1
B		Types of **private data** elements that can be maintained by the **device**:		
	B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	__
	B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	Yes	__
	B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	__
	B.4	Open, unstructured text entered by **device user/operator**?	Yes	__
	B.5	**Biometric data**?	No	__
	B.6	Personal financial information?	No	__
C		Maintaining **private data** - Can the **device**:		
	C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	2
	C.2	Store **private data** persistently on local media?	See Note	3
	C.3	Import/export **private data** with other systems?	Yes	4
	C.4	Maintain **private data** during power service interruptions?	Yes	__
D		Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1	Display private data (e.g., video display, etc.)?	Yes	__
	D.2	Generate hardcopy reports or images containing **private data**?	No	__
	D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	No	__
	D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	No	__
	D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	No	__
	D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared,	Yes	__
	D.7	Import **private data** via scanning?	Yes	__
	D.8	Other?	______	__

Management of Private Data notes:

1. Butterfly iQ provides the ability for users to enter PHI or pull data from a DICOM Modality Worklist (MWL).
2. Ultrasound exams that may include PHI are cached within the Butterfly mobile app until successfully uploaded to the Butterfly Cloud.
3. Data is stored encrypted in the application cache until the user uploads the study to the Butterfly Cloud, at which time the local data is deleted.
4. The Butterfly Cloud utilizes TLS 1.2 encryption for hospital system connections, such as PACS for archiving and Modality Worklist to pull patient demographics to the Butterfly iQ mobile app. A configurable option can be enabled to allow system administrators to export data to their local systems.

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

SECURITY CAPABILITIES

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
1	**AUTOMATIC LOGOFF (ALOF)** The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	1
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	Yes	2
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	Yes	1, 2
ALOF notes:	1. The inactivity timer is set within the mobile device configuration. The Butterfly mobile app forces users to apply a security PIN, password, etc. to their mobile device. This can be enforced by the use of a Mobile Device Management (MDM) software as well. Removing the device lock will result in the user being automatically logged out of the Butterfly app. The user will be unable to log back into the Butterfly mobile app until a device lock has been re-enabled. 2. The Butterfly Cloud provides a customizable inactivity timer that can be set by an administrator between 15 minutes and 24 hours.		
2	**AUDIT CONTROLS (AUDT)** The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	Yes	1
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	See Note	2
2-2.2	Display/presentation of data	See Note	3
2-2.3	Creation/modification/deletion of data	Yes	__
2-2.4	Import/export of data from **removable media**	N/A	__
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	Yes	__
2-2.5.1	**Remote service** activity	N/A	4
2-2.6	Other events? (describe in the notes section)	See Note	5
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1	**User** ID	Yes	__
2-3.2	Date/time	Yes	__
AUDT notes:	1. Any data accessed on the Butterfly Cloud and transmitted to the Butterfly Cloud is logged. 2. Login is logged, logout is not. Session keys are issuds for 24 hours and automatically expire, or are closed manually by user initiated logout. 3. User activity is logged, including which ultrasounds studies have been accessed. 4. There is no remote access to the device through the Butterfly mobile app. 5. All user activity (logging in, screens viewed, date/time of uploads, deletions, , captures and archives) is logged.		
3	**AUTHORIZATION (AUTH)** The ability of the device to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	Yes	1, 2
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	__
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	__
AUTH notes:	1. The Butterfly mobile app requires a device lock (password, pin, etc.) to be enabled. SSO/SAML integration can be implemented to enforce user login and password requirements. 2. Mobile device restrictions can be enforced through the use of the Mobile Device Management (MDM) feature on the Butterfly Cloud to prevent users from logging into the Butterfly mobile app on personal devices.		

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)** The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/operator reconfigure product **security capabilities**?	See Note	1
CNFS notes:	1. The device owner/operator can only configure security capabilities local to the mobile device, such as Auto Lock and password. The Butterfly Cloud and user profiles are controlled by a designated Butterfly Cloud administrator.		
5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)** The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	Yes	__
5-1.1	Can security patches or other software be installed remotely?	See Note	1
CSUP notes:	1. The Butterfly mobile app does not impact mobile device security patches from being applied/installed. Butterfly Network security patches are delivered thorugh the Butterfly mobile app and available through the Apple App Store or Android Play Store.		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)** The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	Yes	1
DIDT notes:	1. Users have the ability to share de-idenfitied study links from the Butterfly Cloud and Butterfly mobile app.		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)** The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	Yes	1
DTBK notes:	1. Ultrasound exams acquired on the Butterfly iQ are securely uploaded to the Butterfly Cloud, which is backed up daily and prior to updates.		
8	**EMERGENCY ACCESS (EMRG)** The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	No	__
EMRG notes:	N/A		
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)** How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	Yes	1
IGAU notes:	1. Data at rest is encrypted with AES 256-bit and data in transit is encrypted with TLS 1.2.		

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
10	**MALWARE DETECTION/PROTECTION (MLDP)** The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	See Note	1
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	Yes	__
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	See Note	1
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	1
10-2	Can the device owner install or update **anti-virus software**?	Yes	__
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	N/A	__
MLDP notes:	1. Installing anti-malware software on the mobile device will not impact the Butterfly mobile app. Anti-malware notifications may appear on the device user interface, but not from within the Butterfly mobile app.		
11	**NODE AUTHENTICATION (NAUT)** The ability of the **device** to authenticate communication partners/nodes.		
11-1	Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	Yes	1
NAUT notes:	1. Transmission of data between the Butterfly mobile app and Butterfly Cloud solution is performed using HTTPS with TLS 1.2 encryption. DICOM Store (PACS/VNA) and Modality Worklist (MWL) connections are performed via Butterfly Link software using HTTPS with TLS 1.2 encryption or DICOM-TLS (TLS 1.2).		
12	**PERSON AUTHENTICATION (PAUT)** Ability of the **device** to authenticate **users**		
12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	Yes	1
12-1.1	Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	Yes	2
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	Yes	__
12-4	Can default passwords be changed at/prior to installation?	N/A	3
12-5	Are any shared **user** IDs used in this system?	No	__
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	2
12-7	Can the **device** be configured so that account passwords expire periodically?	Yes	2
PAUT notes:	1. Butterfly Network user accounts are managed by a designated Butterfly Cloud administrator. 2. SSO/SAML integration is available to enforce corporate user login and password requirements. 3. There are no default passwords.		
13	**PHYSICAL LOCKS (PLOK)** Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.		
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	Yes	__
PLOK notes:	N/A		

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)** Manufacturer's plans for security support of 3rd party components within **device** life cycle.		
14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	See Note	1, 2
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	__
RDMP notes:	1. A list of supported mobile devices can be found at https://www.butterflynetwork.com/specs 2. The Butterfly Cloud solution is compatible with the latest two versions of Google Chrome, Mozilla Firefox, Safari and Microsoft Edge.		
15	**SYSTEM AND APPLICATION HARDENING (SAHD)** The **device**'s resistance to cyber attacks and **malware**.		
15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	See Note	1
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	Yes	2
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes	3
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	No	__
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	Yes	4
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	No	5
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	__
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	Yes	__
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	No	5
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	No	__
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No	__
SAHD notes:	1. Butterfly Network follows ISO 27001 standards and is built under the Butterfly QMS. 2. Software and firmware updates are only available through the Butterfly mobile app. 3. Cellular and WiFi are supported. 4. There are no default accounts. Access to the Butterfly app and Butterly Cloud is restricted to active user accounts, which are managed by a designated Butterfly Cloud administrator for each organization. 5. The Butterfly mobile app allows the mobile device to function normally, however, the app itself only utilizes specified ports and communcation protocols when in use.		
16	**SECURITY GUIDANCE (SGUD)** The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the **device user**?	Yes	__
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	Yes	1
SGUD notes:	1. Data is only cached securely within the Butterfly mobile app until uploaded to the Butterfly Cloud. The Butterfly mobile app requires the device to have a lock mechanism enabled before the app can be used. Removing the device lock will result in the user being automatically logged out of the Butterfly app, which will permanently delete any iQ data that has not been uploaded to the Butterfly Cloud. The user will be unable to log back into the Butterfly mobile app until a device lock has been re-enabled.		

Device Category Ultrasound	Manufacturer Butterfly Network, Inc.	Document ID 950-20007-00 v04	Document Release Date June, 2020
Device Model iQ	Software Revision 1.19		Software Release Date May, 2020

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)** The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.		
17-1	Can the **device** encrypt data at rest?	Yes	1
STCF notes:	1. Data cached within the Butterfly mobile app is encrypted with AES 256-bit.		
18	**TRANSMISSION CONFIDENTIALITY (TXCF)** The ability of the **device** to ensure the confidentiality of transmitted **private data**.		
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	No	__
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	Yes	1, 2
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	Yes	2
TXCF notes:	1. Transmission of data between Butterfly mobile app and the Butterfly Cloud solution is performed using HTTPS with TLS 1.2 encryption. Telemedicine Only: Data streams are encrypted using Datagram Transport Layer Security (DTLS) and media streams are encrypted using Secure Real-time Transport Protocol (SRTP). 2. DICOM Store (PACS/VNA) and Modality Worklist (MWL) connections are performed via Butterfly Link software using HTTPS with TLS 1.2 encryption or DICOM-TLS (TLS 1.2).		
19	**TRANSMISSION INTEGRITY (TXIG)** The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	Yes	1
TXIG notes:	1. Transmission of data between Butterfly mobile app and the Butterfly Cloud solution is performed using HTTPS with TLS 1.2 encryption.		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	No	__
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	N/A	__
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	N/A	__
OTHR notes:	N/A		