



BUTTERFLY iQ +

MDS2

Manufacturer Disclosure Statement for Medical Device Security

Question ID	Question	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
DOC-1	Manufacturer Name	Butterfly Network, Inc.				
DOC-2	Device Description	Handheld ultrasound and workflow management solution				
DOC-3	Device Model	iQ+				
DOC-4	Document ID	950-20007-00				
DOC-5	Manufacturer Contact Information	Technical Support https://support.butterflynetwork.com/ 855-296-6188				
DOC-6	Intended use of device in network-connected environment:	Yes	Network connectivity is only required if saving images to the Butterfly Cloud, or to any connected hospital system.			
DOC-7	Document Release Date		3/29/21			
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes				
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	No				
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	https://support.butterflynetwork.com/hc/en-us/articles/360027865792-Technology-and-Security-White-Paper			
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No				
DOC-11.1	Does the SaMD contain an operating system?	N/A				
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A				
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A				
DOC-11.4	Is the SaMD hosted by the customer?	N/A				

Question ID	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	Yes			AR-2	A.15.1.4
MPII-2	Does the device maintain personally identifiable information?	No			AR-2	A.15.1.4
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	Ultrasound exams are briefly cached in the Butterfly iQ mobile app encrypted using AES 256 bit encryption until uploaded to the Butterfly Cloud.		AR-2	A.15.1.4
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	No				
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	No				
MPII-2.4	Does the device store personally identifiable information in a database?	Yes	Butterfly mobile app can securely transmit data to the Butterfly Cloud where it is stored in a database long term.			
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	Yes	Local data is deleted once successfully received by the Butterfly Cloud.		AR-2	A.15.1.4
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	Yes	Our Customers determine and control what Customer Data is uploaded to the Butterfly Cloud, but such data typically includes: the patient's full name, DOB, gender, accession #, as well as the MRN scans captured through the iQ Device. It may also include the Customer's clinical notes on the patient and their scans.		AR-2	A.15.1.4
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes	Ultrasound exams not uploaded to the Butterfly Cloud will maintain in the cache of the Butterfly iQ mobile app until uploaded to the Butterfly Cloud, or the user is logged out of the application.		AR-2	A.15.1.4
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	N/A	Internal media is part of the smart device being used in conjunction with the Butterfly iQ mobile app. No data is saved to the smart device's media.			
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	Yes	Butterfly mobile app can securely transmit data to the Butterfly Cloud where it is stored in a database long term. Butterfly Cloud can also be integrated with a hospital's PACS/VNA or EHR.		AR-2	A.15.1.4
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	Yes	Data is transmitted to the Butterfly Cloud using HTTPS with TLS 1.2 (SHA-256) encryption		AR-2	A.15.1.4
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes			AR-2	A.15.1.4
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	Yes	Butterfly Cloud has the ability to download a patient study as a PDF.		AR-2	A.15.1.4
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)?	No			AR-2	A.15.1.4
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	No			AR-2	A.15.1.4
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	No			AR-2	A.15.1.4
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., Wi-Fi, Bluetooth, NFC, infrared, cellular, etc.)?	Yes	Internet connectivity is required for access to hospital Modality Worklist, or to upload studies from the Butterfly iQ mobile app to the Butterfly Cloud.		AR-2	A.15.1.4
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	Yes	Data is transmitted to the Butterfly Cloud using HTTPS with TLS 1.2 (SHA-256) encryption using the internet connectivity of the smart device used in conjunction with the Butterfly iQ mobile app.		AR-2	A.15.1.4
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No				
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No				
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	Yes	DICOM or HL7 is used to send or receive data from connected hospital systems.		AR-2	A.15.1.4

Question ID	AUTOMATIC LOGOFF (ALOF) <i>The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logout, session lock, password protected screen saver)?	Yes	Butterfly iQ mobile app session time-out is enabled through our MDM integration.	Section 5.1, ALOF	AC-12	None
ALOF-2	Is the length of inactivity time before auto-logout/screen lock user or administrator configurable?	Yes		Section 5.1, ALOF	AC-11	A.11.2.8, A.11.2.9
Question ID	AUDIT CONTROLS (AUDT) <i>The ability to reliably audit activity on the device.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	Audit logs can be requested from Butterfly Technical Support.	Section 5.2, AUDT	AU-1	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AUDT-1.1	Does the audit log record a USER ID?	Yes				
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	No		Section 5.2, AUDT	AU-2	None
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.1	Successful login/logout attempts?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.2	Unsuccessful login/logout attempts?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.3	Modification of user privileges?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.4	Creation/modification/deletion of users?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.6	Creation/modification/deletion of data?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	No		Section 5.2, AUDT	AU-2	None
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-2.8.1	Remote or on-site support?	Yes	Butterfly Support is remote, however no remote access is needed by Butterfly Technical Support.	Section 5.2, AUDT	AU-2	None
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes	There are several internal only APIs used in the development of the Butterfly. There is no API available to customers.	Section 5.2, AUDT	AU-2	None
AUDT-2.9	Emergency access?	No		Section 5.2, AUDT	AU-2	None
AUDT-2.10	Other events (e.g., software updates)?	Yes	Butterfly Cloud is a SaaS with continuous delivery. Updates are deployed during periods of low cloud usage using non-breaking changes with no impact to the end user. Butterfly iQ mobile app and Butterfly iQ firmware upgrades and security patches are provided automatically using Over the Air (OTA) updates. Updates are not generally required, however, major updates, such as those affecting safety or data security, could be mandatory. For Enterprise customers, mobile app upgrades can also be pushed to end-users through MDM integration. Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.	Section 5.2, AUDT	AU-2	None
AUDT-2.11	Is the audit capability documented in more detail?	Yes	All events are logged and retained for 6 years at minimum. No end-user can delete the audit log.	Section 5.2, AUDT	AU-2	None
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No		Section 5.2, AUDT	AU-2	None
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	Yes	All activities below are logged by User ID and date/time to the millisecond: Logon Failed login attempts Image create/view/modify/delete Modification of study details User account create/delete/modification Administrator changes	Section 5.2, AUDT	AU-2	None
AUDT-4.1	Does the audit log record date/time?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-5	Can audit log content be exported?	No	To request a customized audit log email butterfly Support at support@butterflynetwork.com.	Section 5.2, AUDT	AU-2	None
AUDT-5.1	Via physical media?	No				
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No				
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No				
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	N/A				
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	To request a customized audit log email butterfly Support at support@butterflynetwork.com.			
AUDT-7	Are audit logs protected from modification?	Yes		Section 5.2, AUDT	AU-2	None
AUDT-7.1	Are audit logs protected from access?	Yes				
AUDT-8	Can audit logs be analyzed by the device?	No		Section 5.2, AUDT	AU-2	None
Question ID	AUTHORIZATION (AUTH) <i>The ability of the device to determine the authorization of users.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	Yes		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	Two user types are available: 1. Administrator: User is able to create ultrasound studies, associate patient information, send to the Butterfly Cloud, perform QA, move/delete studies, configure DICOM, HL7, SSO, and MDM integrations. 2. Regular: User is able to create ultrasound studies, associate patient information, and send to the Butterfly Cloud.	Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	No		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-4	Does the device authorize or control all API access requests?	N/A		Section 5.3, AUTH	IA-2	A.9.2.1
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	No	Butterfly iQ mobile app can be run in kiosk mode.			

Question ID	CYBER SECURITY PRODUCT UPGRADES (CSUP) <i>The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	Butterfly Cloud is a SaaS with continuous delivery. Updates are deployed during periods of low cloud usage using non-breaking changes with no impact to the end user. Butterfly IQ mobile app and Butterfly IQ firmware upgrades and security patches are provided automatically using Over the Air (OTA) updates. Updates are not generally required, however, major updates, such as those affecting safety or data security, could be mandatory. For Enterprise customers, mobile app upgrades can also be pushed to end-users through MDM integration. Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.			
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	No	Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.			
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	https://manual.butterflynetwork.com/butterfly-iq-user-manual_rev-aa-en.pdf			
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No				
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes				
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes				
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes				
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	https://manual.butterflynetwork.com/butterfly-iq-user-manual_rev-aa-en.pdf			
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No				
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes				
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes				
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	No				
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A				
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A				
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	No				
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A				
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A				
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No				
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A				
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A				
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A				
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A				
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	N/A	Butterfly Cloud is a SaaS with continuous delivery. Updates are deployed during periods of low cloud usage using non-breaking changes with no impact to the end user. Butterfly IQ mobile app and Butterfly IQ firmware upgrades and security patches are provided automatically using Over the Air (OTA) updates. Updates are not generally required, however, major updates, such as those affecting safety or data security, could be mandatory. For Enterprise customers, mobile app upgrades can also be pushed to end-users through MDM integration. Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.			
CSUP-8	Does the device perform automatic installation of software updates?	Yes				
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.			
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	N/A				
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	N/A				
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes				
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	Butterfly IQ mobile app and Butterfly IQ firmware upgrades and security patches are provided automatically using Over the Air (OTA) updates. Updates are not generally required, however, major updates, such as those affecting safety or data security, could be mandatory.			
CSUP-11.2	Is there an update review cycle for the device?	Yes	Generally updates are released through the Appstore monthly.			

Question ID	HEALTH DATA DE-IDENTIFICATION (DIDT) <i>The ability of the device to directly remove information that allows identification of a person.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	Yes		Section 5.6, DIDT	None	ISO 27038
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	Yes		Section 5.6, DIDT	None	ISO 27038

Question ID DATA BACKUP AND DISASTER RECOVERY (DTBK)

The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.

IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

ISO 27002:2013

DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	Yes	Butterfly Cloud can also be integrated with a hospitals PACS/VNA or EHR.			
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	Yes		Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-3	Does the device have an integral data backup capability to removable media?	No		Section 5.7, DTBK	CP-9	A.12.3.1
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes	Backups of all Butterfly Cloud system data are stored in Amazon Web Services and managed by Aptible (a secure container platform) where they are encrypted with AES 256-bit encryption. Backups are automatically performed daily and prior to application upgrades, but can also be performed on demand. The format of the backups are snapshots of the encrypted Amazon Elastic Block Store volume. Backups are maintained for 8 days prior to being deleted. For specific data center disaster recovery details, please refer to the AWS SOC III report. https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf			
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	No				
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	Backups of all Butterfly Cloud system data are stored in Amazon Web Services and managed by Aptible.	Section 5.7, DTBK	CP-9	A.12.3.1

Question ID EMERGENCY ACCESS (EMRG)

The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.

Response

Comment

IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

ISO 27002:2013

EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	No		Section 5.8, EMRG	SI-17	None
--------	---	----	--	-------------------	-------	------

Question ID HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)

How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.

Response

Comment

IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

ISO 27002:2013

IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes		Section 5.9, IGAU	SC-28	A.18.1.3
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes		Section 5.9, IGAU	SC-28	A.18.1.3

Question ID MALWARE DETECTION/PROTECTION (MLDP)

The ability of the device to effectively prevent, detect and remove malicious software (malware).

Response

Comment

IEC TR 80001-2-2:2012

NIST SP 800-53 Rev. 4

ISO 27002:2013

MLDP-1	Is the device capable of hosting executable software?	No		Section 5.10, MLDP		
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-2.1	Does the device include anti-malware software by default?	No	Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.	Section 5.10, MLDP	CM-5	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
MLDP-2.2	Does the device have anti-malware software available as an option?	No		Section 5.10, MLDP	AU-6	A.12.4.1, A.16.1.2, A.16.1.4
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	N/A		Section 5.10, MLDP	CP-10	A.17.1.2
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	Yes		Section 5.10, MLDP	AU-2	None
MLDP-2.5	Does notification of malware detection occur in the device user interface?	No				
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	N/A				
MLDP-2.7	Are malware notifications written to a log?	N/A				
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	No				
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	N/A		Section 5.10, MLDP	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	Yes	For Butterfly Cloud: Enclave host operating systems are hardened based on the Center for Internet Security's Security Configuration Benchmark for the OS and version in use. For all operating systems: Operating systems are installed on hosts only from bare images, and only via automated configuration management. Services installed can be enumerated upon request. Aptible internal workforce user access is configured only on a per-user basis, and only when necessary to provide customer support. Swap is disabled to avoid writing in-memory secrets to unencrypted volumes. Password-based services (such as PostgreSQL) are provisioned only with unique, per-resource, Aptible-generated passphrases. Additional hardening: - Host password logins are disabled - SSH root keys are not permitted - No user SSH keys are permitted on hosts by default - Command history for shell sessions is disabled - Non-default SSH ports are used - No password-based services are installed Aptible HIDS is utilized for host intrusion detection and prevention on the Butterfly Cloud. See: https://www.aptible.com/documentation/deploy/reference/managed-host-intrusion-detection.html	Section 5.10, MLDP	SI-3	A.12.2.1
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	Yes	Aptible HIDS is utilized for host intrusion detection and prevention on the Butterfly Cloud. See: https://www.aptible.com/documentation/deploy/reference/managed-host-intrusion-detection.html	Section 5.10, MLDP	SI-4	None
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	No		Section 5.10, MLDP	CM-7	A.12.5.1
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Yes		Section 5.10, MLDP		

Question ID	NODE AUTHENTICATION (NAUT) <i>The ability of the device to authenticate communication partners/nodes.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
NAUT-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 (e.g. Web APIs, SMTP, SNMP)?	Yes	HTTPS with TLS 1.2 encryption.	Section 5.11, NAUT	SC-23	None
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	Yes	Butterfly Cloud utilizes three firewalls. AWS Shield and CloudFront (maintained by Aptible) and ModSecurity (firewall at the application level). Web application traffic is secured with TLS 1.2. Butterfly Network utilizes a secure container platform (Aptible Endave) that provides Network and Host Variability Scanning as well as a Web Application Firewall (WAF). The Butterfly Cloud uses a multi-tenant cloud architecture that ensures data separation through organization specific metadata tags.	Section 5.11, NAUT	SC-7	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
NAUT-2.1	Is the firewall ruleset documented and available for review?	No	These are reviewed by our 3rd party auditor. Report is available for review.			
NAUT-3	Does the device use certificate-based network connection authentication?	Yes				

Question ID	CONNECTIVITY CAPABILITIES (CONN) <i>All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
CONN-1	Does the device have hardware connectivity capabilities?	No				
CONN-1.1	Does the device support wireless connections?	No				
CONN-1.1.1	Does the device support Wi-Fi?	Yes				
CONN-1.1.2	Does the device support Bluetooth?	No				
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	Yes	Butterfly IQ mobile app uses the internet connectivity of the smart device being used in conjunction with the app.			
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	No				
CONN-1.2	Does the device support physical connections?	Yes	Butterfly IQ+ plugs into a smart device using a lightning or USB-C cable.			
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	No				
CONN-1.2.2	Does the device have available USB ports?	No				
CONN-1.2.3	Does the device require, use, or support removable memory devices?	No				
CONN-1.2.4	Does the device support other physical connectivity?	No				
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	N/A				
CONN-3	Can the device communicate with other systems within the customer environment?	Yes	Butterfly Cloud can be integrated with a hospital's DICOM or HL7 systems.			
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes	Butterfly IQ mobile app securely connects to the Butterfly Cloud hosted in AWS.			
CONN-5	Does the device make or receive API calls?	Yes				
CONN-6	Does the device require an internet connection for its intended use?	Yes				
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes		1.2		
CONN-7.1	Is TLS configurable?	No				
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	Yes	Telemedicine is a feature of the Butterfly Platform and can be used between two authorized users of the same customer domain.			

Question ID	PERSON AUTHENTICATION (PAUT) <i>The ability to configure the device to authenticate users.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes		Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes	Enterprise memberships may be integrated with customer's SSO via SAML 2.0 to enforce authentication.	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc)?	Yes	Enterprise memberships may be integrated with customer's SSO via SAML 2.0.	Section 5.12, PAUT	IA-5	A.9.2.1
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	Yes	Butterfly user ID's lock after 10 failed attempts. Alternatively, lock will follow your SSO rules.	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	N/A	No default accounts.	Section 5.12, PAUT	SA-4(5)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
PAUT-5	Can all passwords be changed?	Yes		Section 5.12, PAUT		
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	Yes	Enterprise memberships may be integrated with customer's SSO via SAML 2.0 to meet complexity requirements.	Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-7	Does the device support account passwords that expire periodically?	Yes	Enterprise memberships may be integrated with customer's SSO via SAML 2.0 to meet expiration requirements.			
PAUT-8	Does the device support multi-factor authentication?	Yes	Enterprise memberships may be integrated with customer's SSO via SAML 2.0 to meet MFA requirements.			
PAUT-9	Does the device support single sign-on (SSO)?	Yes		Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-10	Can user accounts be disabled/locked on the device?	Yes		Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-11	Does the device support biometric controls?	No		Section 5.12, PAUT	IA-2	A.9.2.1
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No				
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No				
PAUT-14	Does the application or device store or manage authentication credentials?	Yes				
PAUT-14.1	Are credentials stored using a secure method?	Yes	Passwords are hashed using Bcrypt. Bcrypt is based on the Blowfish cipher.			

Question ID	PHYSICAL LOCKS (PLOK) <i>Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	No		Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes		Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	Yes		Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	Yes		Section 5.13, PLOK	PE-3(4)	A.11.1.1, A.11.1.2, A.11.1.3

Question ID	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) <i>Manufacturer's plans for security support of third-party components within the device's life cycle.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	Yes		Section 5.14, RDMP	CM-2	None
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes		Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes		Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes		Section 5.14, RDMP	CM-8	A.8.1.1, A.8.1.2

Question ID	SOFTWARE BILL OF MATERIALS (SBOM) <i>A Software Bill of Material (SBOM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
SBOM-1	Is the SBOM for this product available?	Yes	Available under NDA.			
SBOM-2	Does the SBOM follow a standard or common method in describing software components?	Yes				
SBOM-2.1	Are the software components identified?	Yes				
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes				
SBOM-2.3	Are the major version numbers of the software components identified?	No				
SBOM-2.4	Are any additional descriptive elements identified?	Yes				
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No				
SBOM-4	Is there an update process for the SBOM?	Yes				
Question ID	SYSTEM AND APPLICATION HARDENING (SAHD) <i>The device's inherent resistance to cyber attacks and malware.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
SAHD-1	Is the device hardened in accordance with any industry standards?	Yes		Section 5.15, SAHD	CM-7 AC-17(2)/IA-3	A.12.5.1* A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/None
SAHD-2	Has the device received any cybersecurity certifications?	Yes	SOC II Type 1 (2020) HIPAA and HITECH compliant (2020) GDPR Ready Freedom of Information and Protection of Privacy Act (FOIPPA) Ready Personal Information International Disclosure Protection Act (PIIDPA) Ready ISO 13485	Section 5.15, SAHD	SA-12(10)	A.6.2.1, A.6.2.2, A.13.1.1, A.14.1.2, A.15.1.1, A.15.1.2, A.15.1.3
SAHD-3	Does the device employ any mechanisms for software integrity checking?	Yes	s3 is used for file storage and integrity monitoring https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-compliance.html			
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	Yes				
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes		Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No		Section 5.15, SAHD	AC-3	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No		Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-5.1	Does the device provide role-based access controls?	Yes	Two user types are available: 1. Administrator: User is able to create ultrasound studies, associate patient information, send to the Butterfly Cloud, perform QA, move/delete studies, configure DICOM, HL7, SSO, and MDM integrations. 2. Regulator: User is able to create ultrasound studies, associate patient information, and send to the Butterfly Cloud.	Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	Yes		Section 5.15, SAHD	CM-8	A.8.1.1, A.8.1.2
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No		Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	N/A		Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	Yes		Section 5.15, SAHD	CM-7	A.12.5.1*
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	Yes		Section 5.15, SAHD	SA-18	None
SAHD-9	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		Section 5.15, SAHD	CM-6	None
SAHD-10	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?	Yes		Section 5.15, SAHD	SI-2	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes				
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	No				
SAHD-13	Does the product documentation include information on operational network security scanning by users?	Yes	Mobile devices, Server and Workstation maintenance, upgrades, patches, and anti-virus software are the responsibility of the customer.			
SAHD-14	Can the device be hardened beyond the default provided state?	No				
SAHD-14.1	Are instructions available from vendor for increased hardening?	N/A				
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes				
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	Yes	Enclave host operating systems are hardened based on the Center for Internet Security's Security Configuration Benchmark for the OS and version in use. For all operating systems: Operating systems are installed on hosts only from bare images, and only via automated configuration management. Services installed can be enumerated upon request. Aptible internal workforce user access is configured only on a per-user basis, and only when necessary to provide customer support. Swap is disabled to avoid writing in-memory secrets to unencrypted volumes. Password-based services (such as PostgreSQL) are provisioned only with unique, Additional hardening: - Host password logins are disabled - SSH root keys are not permitted - No user SSH keys are permitted on hosts - Command history for shell sessions is disabled - Non-default SSH ports are used - No password-based services are installed - No default passwords are permitted - Host security updates are automated - All host ports are opened only via whitelist			

Question ID	SECURITY GUIDANCE (SGUD) <i>Availability of security guidance for operator and administrator of the device and manufacturer sales and service.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
SGUD-1	Does the device include security documentation for the owner/operator?	Yes		Section 5.16, SGUD	AT-2/PL-2	A.7.2.2, A.12.2.1/A.14.1.1
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	Yes		Section 5.16, SGUD	MP-6	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
SGUD-3	Are all access accounts documented?	N/A	All service accounts have been disabled.	Section 5.16, SGUD	AC-6,IA-2	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5/A.9.2.1
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes				
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	Yes				

Question ID	HEALTH DATA STORAGE CONFIDENTIALITY (STCF) <i>The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
STCF-1	Can the device encrypt data at rest?	Yes	Data at rest is encrypted with AES 256-bit within the Butterfly IQ mobile app and on the Butterfly Cloud.	Section 5.17, STCF	SC-28	A.8.2.3
STCF-1.1	Is all data encrypted or otherwise protected?	Yes				
STCF-1.2	Is the data encryption capability configured by default?	Yes				
STCF-1.3	Are instructions available to the customer to configure encryption?	No				
STCF-2	Can the encryption keys be changed or configured?	No	Encryption keys are managed by AWS and Aptible. AWS KMS (Key Management Services) are tightly integrated with the AWS product portfolio to provide leading security controls, auditability, management and compliance for encryption keys. The service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of the keys. TLS certificates expire every 90 days and are rotated before-hand. No Butterfly employees can access them directly by any means. Encryption keys are customer specific for Butterfly Cloud-to-Customer network communications.	Section 5.17, STCF	SC-28	A.8.2.3
STCF-3	Is the data stored in a database located on the device?	No				
STCF-4	Is the data stored in a database external to the device?	Yes	Butterfly Cloud			

Question ID	TRANSMISSION CONFIDENTIALITY (TXCF) <i>The ability of the device to ensure the confidentiality of transmitted personally identifiable information.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No		Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	Yes	Data in transit is secured with HTTPS and TLS 1.2 encryption.	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	N/A	Data is encrypted by default.			
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	Butterfly IQ mobile app will only connect with the Butterfly Cloud. Additionally, the Butterfly Cloud can be pre-configured to send to hospital end points like PACS/VNA/EHR.	Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-4	Are connections limited to authenticated systems?	Yes		Section 5.18, TXCF	CM-7	A.12.5.1
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	Yes	Data in transit is secured with HTTPS and TLS 1.2 encryption. Additional transmission modes include DICOM-TLS and HL7.			

Question ID	TRANSMISSION INTEGRITY (TXIG) <i>The ability of the device to ensure the integrity of transmitted data.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	Yes	Data is transmitted to the Butterfly Cloud using HTTPS with TLS 1.2 (SHA-256) encryption.	Section 5.19, TXIG	SC-8	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
TXIG-2	Does the device include multiple sub-components connected by external cables?	No				

Question ID	REMOTE SERVICE (RMOT) <i>Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.</i>	Response	Comment	IEC TR 80001-2-2:2012	NIST SP 800-53 Rev. 4	ISO 27002:2013
RMOT-1	Does the device permit remote service connections for device analysis or repair?	No			AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
RMOT-1.1	Does the device allow the owner/operator to initiate remote service sessions for device analysis or repair?	No				
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A				
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	N/A			AC-17	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No				
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	No				