Butterfly Network Technology and Security White Paper

Understanding, Implementing and Securing Butterfly iQ at Your Organization

Table of Contents

Introduction

This white paper is intended for existing and potential customers who are interested in, or currently integrating the Butterfly Network product ecosystem into their hospital IT environment.

We provide an overview of Butterfly Network's technology, infrastructure, network architecture and security controls that will help your institution navigate a successful integration. This white paper also provides an overview of deployment options to help your organization select an appropriate configuration.

This document is targeted at clinical, IT, and security professionals. Portions of this document will assume familiarity with network architectures, operating systems, encryption, and security controls.

Medical Ultrasound Imaging

Ultrasound is a life-saving medical imaging modality which enables healthcare practitioners to safely and non-invasively visualize their patients' anatomy.

Unlike other dominant imaging modalities like X-Ray or Computed Tomography (CT) which emit potentially harmful ionizing radiation, ultrasound emits only high-frequency sound. While ultrasound has many benefits, broad access is limited by the high cost and bulk of traditional equipment.

Traditional ultrasound works by sending an electric current through a crystal composite called PZT (Lead Zirconate Titanate). This material acts as a transducer, converting electrical energy into sound waves that bounce off structures inside the body. On their return to the crystal transducer, these echoes are turned back into electrical signals and processed by a computer into a moving image.

Typically, this process requires bulky, powerful, expensive, cart-mounted computers which are responsible for the heft of traditional systems. Furthermore, traditional ultrasound systems, due to intrinsic limitations of crystal transducers, require multiple expensive, fragile, transducers (aka probes), each tailored to image a specific part of the body.

Butterfly iQ and the Butterfly Network Product Ecosystem

Butterfly Network's foundational innovation enables the construction of an ultrasound machine on a chip without the need for bulky computers or crystal transducers. This transformation is analogous to the transition in photography from film to digital cameras: our chip-based approach delivers three core benefits to ultrasound users:

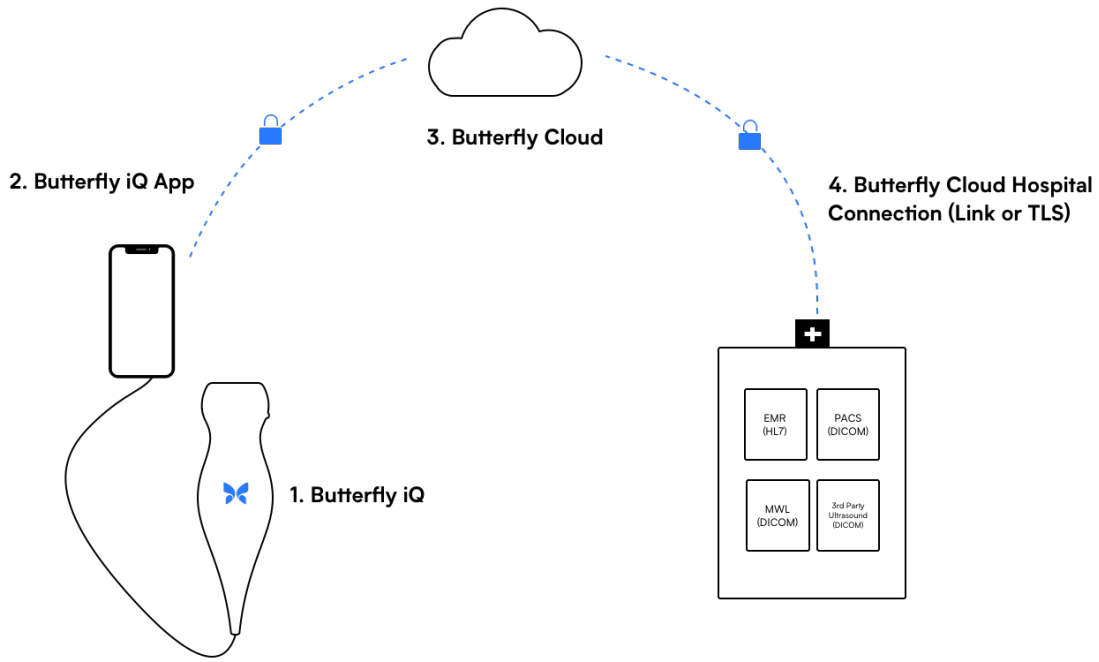
1. **Affordability** - Butterfly iQ costs 40 times less than traditional ultrasound machines.
2. **Versatility** - Butterfly iQ can scan the entire body with a single probe.
3. **Portability** - Butterfly iQ fits in a lab-coat pocket.

Butterfly Network Product Ecosystem

The Butterfly Network product ecosystem is comprised of four components:

1. Butterfly iQ Transducer
2. Butterfly iQ Mobile App
3. Butterfly Cloud
4. Butterfly Cloud Hospital Connection (Link or TLS)

Figure 1. Butterfly Network Product Ecosystem



Butterfly Network product ecosystem data flow. All data is encrypted in transit and at rest.

Butterfly iQ Transducer

Butterfly iQ is the world's only whole-body ultrasound imager. Priced under $2,000, Butterfly iQ matches the clinical versatility and performance of traditional machines costing 40x more.

Butterfly iQ can scan the body with a single chip because it replaces traditional piezoelectric crystals with Butterfly Network's ultrasound-on-a-chip technology wherein 9,000 capacitive micromachined ultrasound transducers create and receive sound from 1 - 10 MHz.

Butterfly iQ Mobile App

The Butterfly iQ Transducer connects to a mobile device running the Butterfly iQ Mobile App, which can be downloaded from the applicable app store. The Mobile App streams real-time ultrasound imagery from the transducer and enables the user to control scanning parameters like image gain and depth.

Upon completion of an examination, the Butterfly iQ Mobile App enables seamless archiving and sharing of ultrasound studies via integration with Butterfly Cloud. Data stored in Butterfly Cloud is compliant with country specific privacy laws including, but not limited to, HIPAA, GDPR, APP, and PIPEDA. Together, the Butterfly Cloud, Butterfly iQ Mobile App and Butterfly iQ Transducer deliver the functionality, performance, and versatility of a traditional ultrasound machine.

Butterfly Cloud

Butterfly Cloud provides all users with unlimited, encrypted image storage. Studies can be accessed from the Butterfly iQ Mobile App, or from any web browser. Users can segment their cloud into separate "Archives" (i.e. folders) used to organize studies uploaded via the Butterfly iQ Mobile App. Studies can be shared with others via de-identified study-links generated from the Mobile App or web browser.

Customers who purchase a Butterfly iQ Team membership also enjoy multi-user secure collaboration, image-sharing, and real-time commenting capabilities. These features enable collaboration across care teams that meets both HIPAA, and other international privacy standards such as GDPR/APP, and make it easier to manage governance of department-wide point of care ultrasound (POCUS) programs.

Lastly, Butterfly Cloud enables the secure interchange of data between end-users and the hospital information systems necessary to support ultrasound billing and continuity of care via integration with the Butterfly DICOM Connector.

Butterfly Cloud Hospital Connection (Link or TLS)

Butterfly iQ Hospital Connector creates an encrypted connection between your hospital's DICOM endpoints, Electronic Medical Record (EMR), third party ultrasound devices. and the Butterfly Network product ecosystem. Butterfly Cloud Hospital Connector can be configured with an on premise executable called Butterfly Link or utilizing DICOM TLS (Transport Layer Security, v 1.2). Each option facilitates a point-to-point encrypted communication between your organization and Butterfly Cloud so a VPN tunnel is not required.

Butterfly CloudHospital Connector can also be used to provide users with access to your institution's DICOM Modality Worklist server which eliminates the need for slow, error-prone manual data entry.

Secure by Design – Our Approach to Security

At Butterfly Network, we believe that it is our responsibility to design devices and software that are secure by design and prioritize patient privacy. We know our customers care deeply about patient data. Leveraging the Butterfly Cloud, allows you to inherit our security and regulatory compliance controls like data localization, while still maintaining ownership of patient data.

This section will provide a high-level overview of how we secure the key layers of our infrastructure, our cloud, and our hosted data centers. More information about who we are, how we collect, and use personal information about you and how you can exercise your privacy rights can be found in our Privacy Notice https://butterflynetwork.com/privacy-notice. Similarly, if you have questions about our comprehensive privacy program, please visit our Global Privacy FAQ https://www.butterflynetwork.com/global-privacy. And our Patient Privacy Notice https://www.butterflynetwork.com/patient-privacy explains how we collect and use patient data following the use, by our Customers, of the Butterfly iQ Device and beyond.

Security Program and Organization

Butterfly's Security Program utilizes industry leading, risk-based, frameworks and standards. Butterfly has a security team led by a Chief Information Security Officer (CISO) who is responsible for the development and maintenance of security policies, enforcing security operations and monitoring technical security within the company and associated third parties.

Security Policies, Processes, and Procedures

At Butterfly, we understand that fostering a healthy security culture begins by providing our employees with security policies, processes, and procedures to help make good decisions when building our products and managing sensitive customer data.

Secure Development Lifecycle (SDLC)

Butterfly follows a "secure by design" approach whereby security is treated as a top priority at all stages of product and application development. We implement controls such as threat modeling for new features, code review, regression testing, deployment controls, vulnerability scanning and penetration testing.

Access Controls

Application Layer

The Butterfly iQ Mobile and Web applications enforce strict user authentication. The Butterfly iQ mobile app requires that hardware device encryption is enabled before log-in and scanning is allowed.

All data is encrypted in transit and at rest. Administrators of a Butterfly Cloud Team membership maintain full control over which users have access to their private data.

For our enterprise customers, Butterfly has developed three additional layers of enhanced, defensive security: Single Sign On, Enterprise Mobility Management Restrictions, and Custom Inactivity Timeout.

Infrastructure Layer

Butterfly Cloud is a multi-tenant distributed system, built with a highly redundant architecture. Leveraging Amazon Web Services (AWS) infrastructure, Butterfly Cloud incorporates multiple layers of physical, policy, and technical safeguards.

Data Protection Controls

Customer data in Butterfly Cloud is further secured by a container orchestration platform (Aptible Enclave) that implements security best practices and controls for the deployment of healthcare applications such as AES 256-bit encryption for data at rest, monitoring and logging, vulnerability management and system hardening.

Disaster Recovery and Business Continuity

Butterfly Network leverages a combination of distributed cloud availability zones as well as daily backups in AWS servers to ensure customer data is easily recoverable in the event of a disaster. Backup and disaster plans are in place and tested quarterly.

Compliance and Certifications

Butterfly Network is SOC 2 (Type 1) certified, which attests to our compliance with Privacy, Security, Confidentiality and Availability criteria as well as HIPAA and HITECH regulations. Butterfly also has a global privacy program that meets the requirements of data protection regulations such as the EU General Data Protection Regulation (GDPR).

Our security controls are constantly evolving to keep up with the dynamic threat landscape, please check our webpage often to view our latest controls.

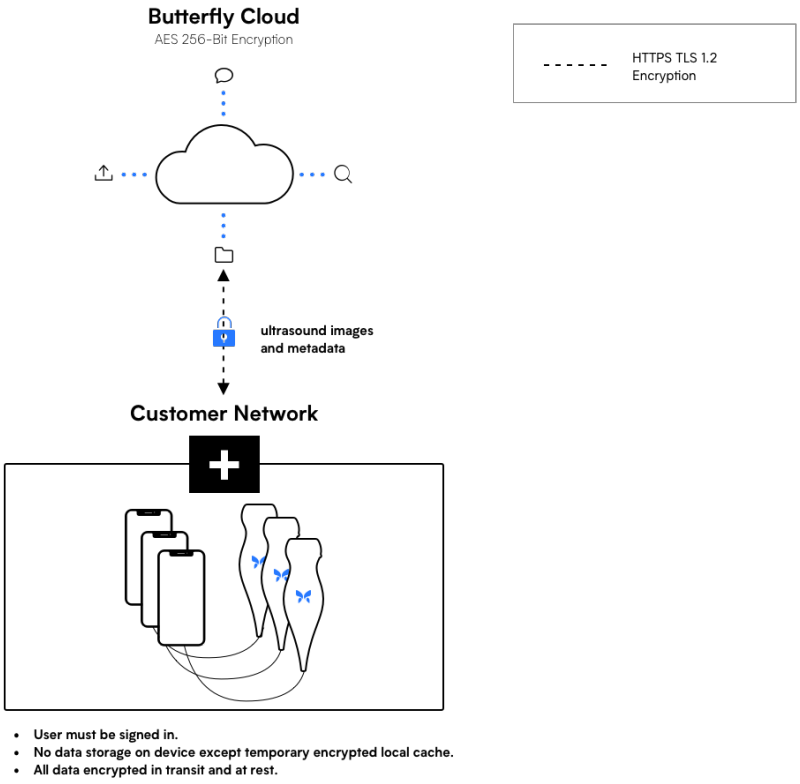
Integration Deployment Options

Butterfly Network supports four integration deployment configurations for integration with customer IT environments.

Option 1 - Default Connectivity: iQ Mobile App to Butterfly Cloud

Ultrasound image data is securely transmitted from the Butterfly iQ Mobile App to Butterfly Cloud using HTTPS with TLS 1.2 encryption. The Butterfly iQ Mobile App and Butterfly Cloud enforce encryption of patient/customer data in transit and at rest. In this configuration, no changes are required to customer IT systems.

Figure 2. Butterfly iQ to Butterfly Cloud

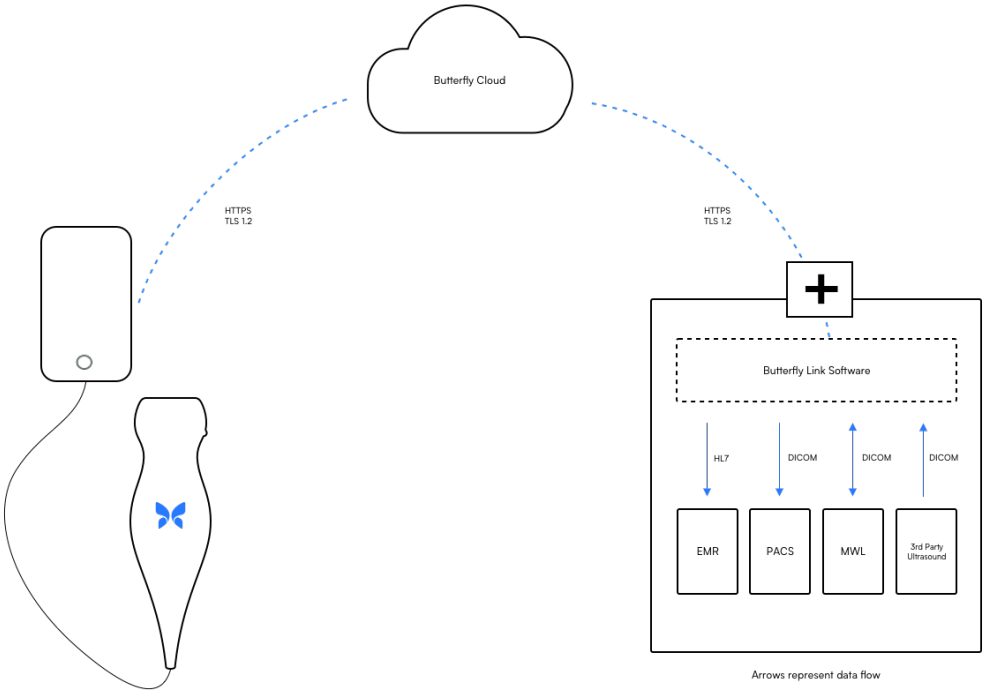


Default connectivity: Butterfly iQ Mobile App to Butterfly Cloud data flow.

Option 2 - Butterfly Link: DICOM Endpoints, EMR and Third Party Devices to Butterfly Cloud

Ultrasound image data is securely transmitted from the Butterfly mobile app to Butterfly Cloud using HTTPS with TLS 1.2 encryption. The Butterfly iQ Mobile App and Cloud enforce encryption of patient/customer data in transit and at rest. In this configuration, no changes are required to customer IT systems.

Figure 3. Butterfly Link: On Premise Client

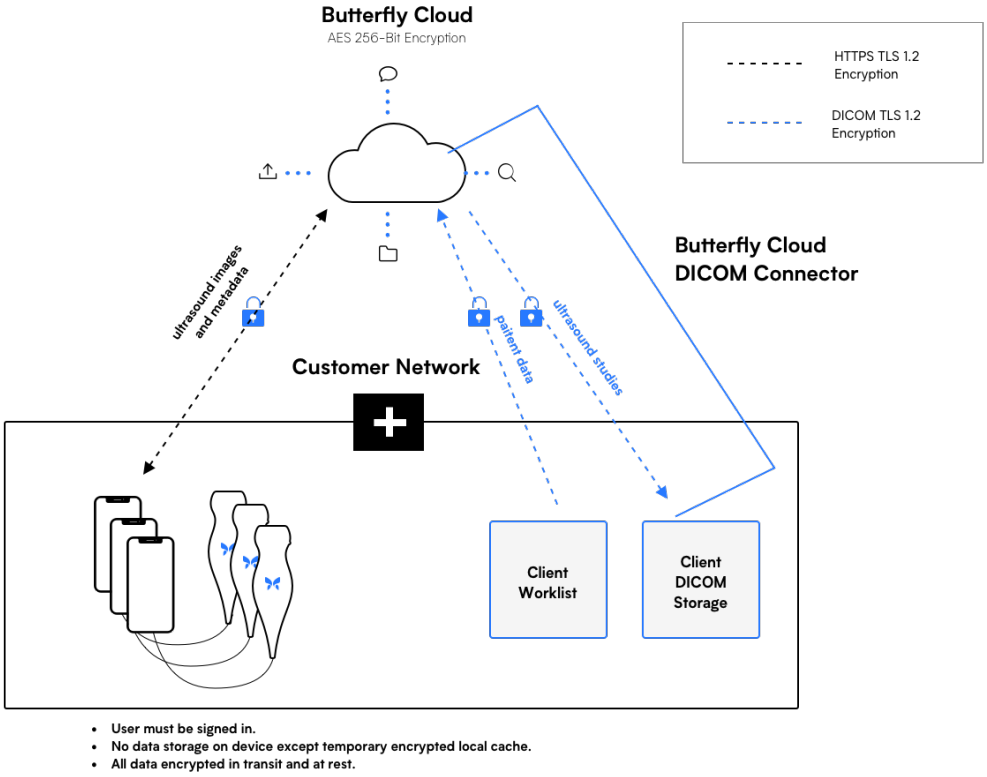


Butterfly Link: On premise executable that securely integrates DICOM endpoints, EMR, and third party ultrasound devices with Butterfly Cloud.

Option 3: Butterfly Cloud to PACS/Worklist via DICOM TLS

Butterfly Cloud can be configured to securely push studies to a PACS and/or query a Modality Worklist (MWL). Communication is encrypted using TLS 1.2.

Figure 4. Butterfly Cloud to PACS/Worklist via DICOM TLS

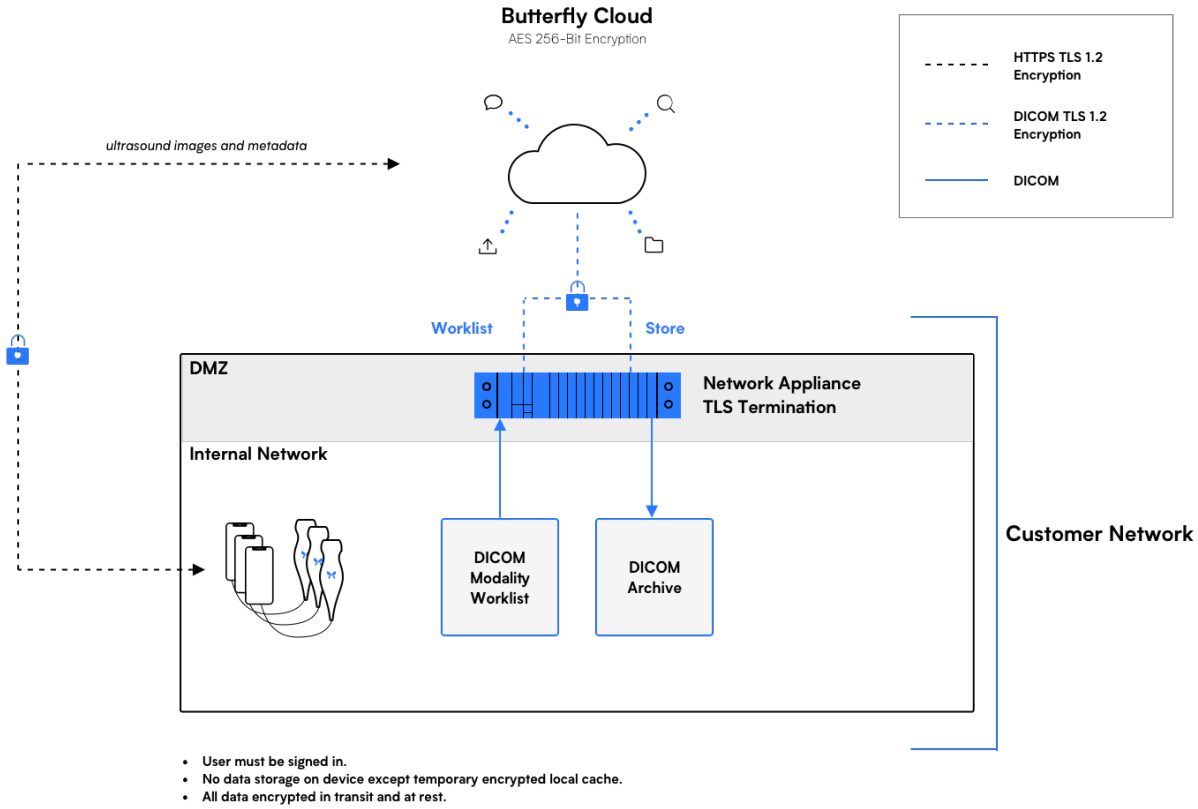


Butterfly Cloud to PACS/Worklist via DICOM TLS data flow.

Option 4: Butterfly Cloud to PACS/WORKLIST via DMZ (Demilitarized Zone)

Butterfly Cloud can be configured to securely push studies to a PACS and/or query a Modality Worklist (MWL) with connection facilitated by a hospital DMZ. The TLS connection can be terminated at the DMZ or directly at the DICOM endpoints (as in Option 2).

Figure 5. Butterfly Cloud to PACS/Worklist via DMZ (Demilitarized Zone)



Butterfly Cloud to PACS/Worklist via DMZ (Demilitarized Zone) data flow.

Conclusion

The security of customer and patient data is our number one priority. For questions on these policies, or for assistance with integration, contact us at support@butterflynetwork.com or visit our knowledge base at support.butterflynetwork.com.