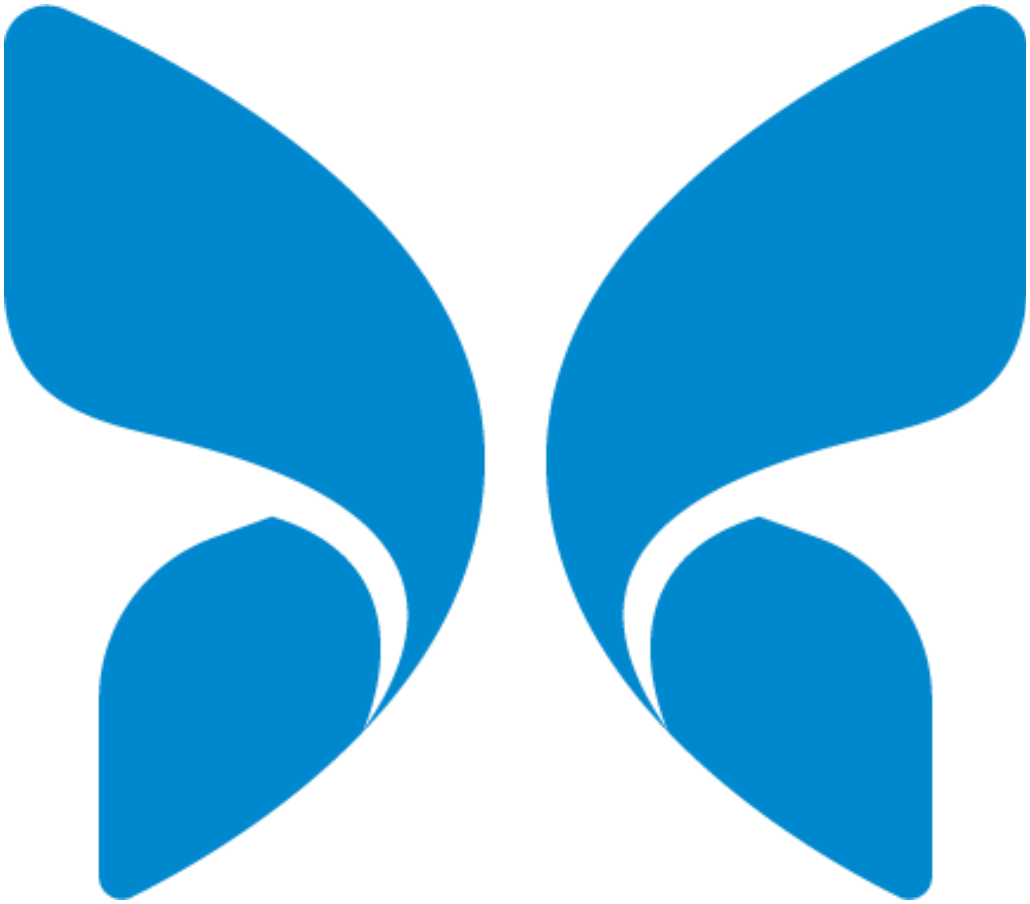
Butterfly Network
Technology and Security White Paper



Understanding, Implementing and Securing Butterfly iQ at Your Organization

950-20009-00 rev C

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 whitepaper 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 Mobile App
3. Butterfly Cloud
4. Butterfly DICOM Connector

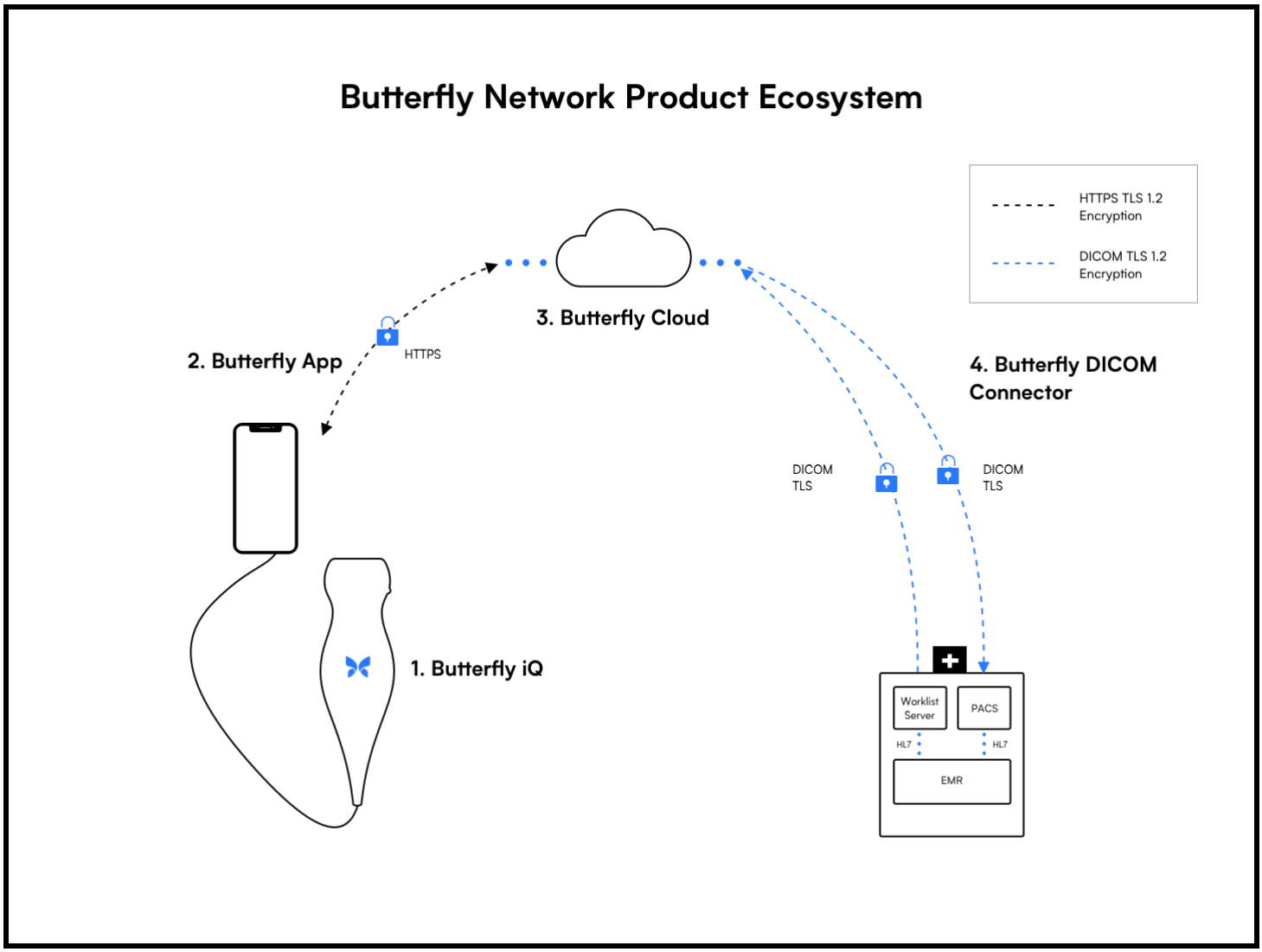


Figure 1: The Butterfly Network product ecosystem data flow. All data is encrypted in transit and at rest.

1. Butterfly iQ Transducer

The Butterfly iQ transducer is the world's only whole-body ultrasound imager. Priced under $2000, 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.

2. Butterfly Mobile App

The Butterfly iQ Transducer connects to an iPhone (or iPad) running the Butterfly iQ Mobile App, which can be downloaded from the Apple App Store. The Mobile App streams real-time ultrasound imagery from the iQ Transducer and enables the user to control scanning parameters like image gain and depth.

Upon completion of an examination, the Butterfly Mobile App enables archiving and HIPAA-compliant sharing of ultrasound studies via integration with the Butterfly Cloud. Together, the Butterfly Mobile App and iQ Transducer deliver the functionality, performance, and versatility of a traditional ultrasound machine.

3. Butterfly Cloud

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

Customers who purchase a Butterfly Cloud team subscription also enjoy multi-user 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, and make it easy to manage a department-wide point of care ultrasound (POCUS) program.

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.

4. Butterfly DICOM Connector

The Butterfly DICOM Connector creates an encrypted connection between your hospital's DICOM endpoints and the Butterfly Network product ecosystem. This enables secure transmission of ultrasound studies captured with Butterfly iQ to a hospital's internal PACS or other middleware systems. The Butterfly DICOM Connector utilizes "DICOM TLS" (Transport Layer Security, v 1.2) to facilitate point-to-point encrypted communication so a VPN tunnel is not required.

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

Defense in Depth – Our Approach to Security

At Butterfly Network the security of your data is our highest priority. In this section, we describe how we secure the key layers of our infrastructure, our Cloud, and our hosted data centers.

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.

Butterfly conducts comprehensive background checks for all new hires. In addition, all new hires are trained and tested in principles pertaining to security, confidentiality, ethics and the details of our Quality Management System (QMS).

Employees who work with sensitive customer data or Protected Health Information (PHI) are further required to undergo specialized privacy training that meets both HIPAA and other international privacy standards such as GDPR.

The Butterfly security team also runs a security awareness program and routinely retrains employees to avoid common security threats.

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.

Butterfly's code is stored in a central repository where both current and past versions of the software are subject to routine audit. The infrastructure is configured to ensure all service binaries are built from specific reviewed, source code.

All software deployment requires review, inspection, and approval from multiple expert engineers. These processes ensure that all changes to our code base are both authorized and appropriate.

Butterfly's experienced application security team conducts manual and automated testing of our products and applications using industry standard frameworks such as OWASP Top 10. In addition, we conduct regular application penetration testing by independent third parties to maintain constant vigilance.

Production code deployments for the Butterfly Cloud occur during periods of low network traffic and occur with no downtime to users. In the rare event of an outage, the core imaging function of Butterfly iQ will not be impacted. Any studies pending upload will remain encrypted and cached in the Butterfly Mobile App until Cloud service is restored.

Access Controls

Application Layer

The Butterfly iOS and Web applications enforce strict user authentication. The Butterfly iOS 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 subscription maintain full control over which users have access to their private data.

Additional Enterprise Access Controls

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.

Single Sign-On (SSO)

Butterfly Single Sign On, or SSO, enables institutions to delegate Butterfly authentication to an existing SAML-compliant identity provider, such as Active Directory. With SSO, users only have to remember a single password and administrators can enforce enhanced identification, like two-factor authentication. SSO also enables centralized account management for secure, simple offboarding.

Enterprise Mobility Management (EMM) Restrictions

The Butterfly Mobile Device Management Restrictions feature allows administrators to prevent access to Butterfly from devices that aren't enrolled in a corporate Mobile Device Management program. Administrators can restrict Butterfly access to managed devices if needed. Users will be able to login to view Cloud archives and capture new images when using devices enrolled in the corporate mobile device management program. When using a personal device, or other unmanaged hardware, access will be blocked.

Custom Inactivity Timeout

Butterfly Custom Inactivity Timeout allows enterprise administrators full control over session length for secure use on shared workstations. With Custom Inactivity Timeout, administrators can configure the cloud to log out after 15 minutes to 10 hours of user inactivity.

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. Butterfly maintains a Business Associates Agreement (BAA) with Amazon ensuring a clear delineation of roles and responsibilities for storing PHI in AWS data centers.

Physical Access to AWS data centers is strictly controlled. Amazon uses multiple physical security layers to protect its data center floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and intrusion detection systems. Additional information on physical precautions can be found in Amazon's Web Services System and Organization Controls (SOC) reports website.

Customer Data Protection

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, monitoring and logging, vulnerability management and system hardening.

Customer Data Privacy

Butterfly Network takes the privacy and the security of its users very seriously and adheres to international privacy standards including HIPAA and GDPR. PHI is maintained in compliance with these rules and our

contractual obligations with healthcare providers. For more on our privacy policy please visit https://www.butterflynetwork.com/privacy-policy.

Disaster Recovery and Business Continuity

Butterfly Network conducts daily backups to Amazon's East and West USA data centers to ensure customer data is easily recoverable in the event of a disaster. Backup plans and disaster plans are in place and tested quarterly.

Compliance

Butterfly Network is SOC 2 (Part 1) certified, which attests to our compliance with both HIPAA and HITECH.

Integration Deployment Options

Butterfly Network supports three 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 mobile app to the Butterfly Cloud using HTTPS with TLS 1.2 encryption. The Butterfly 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.*

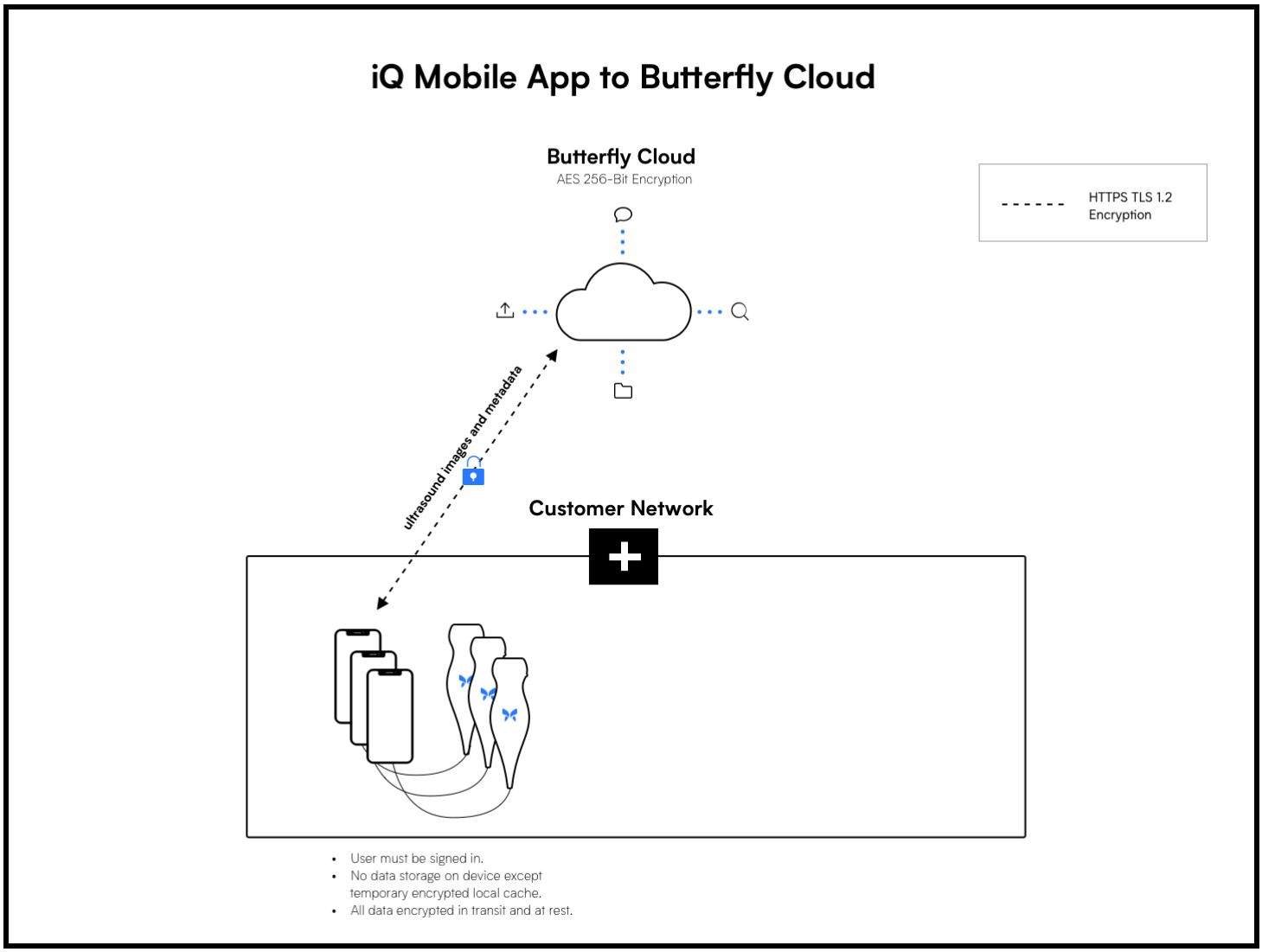


Figure 2: Default connectivity: iQ mobile app to Butterfly Cloud data flow.

Option 2: Butterfly Cloud to PACS/Worklist via DICOM TLS

The 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.

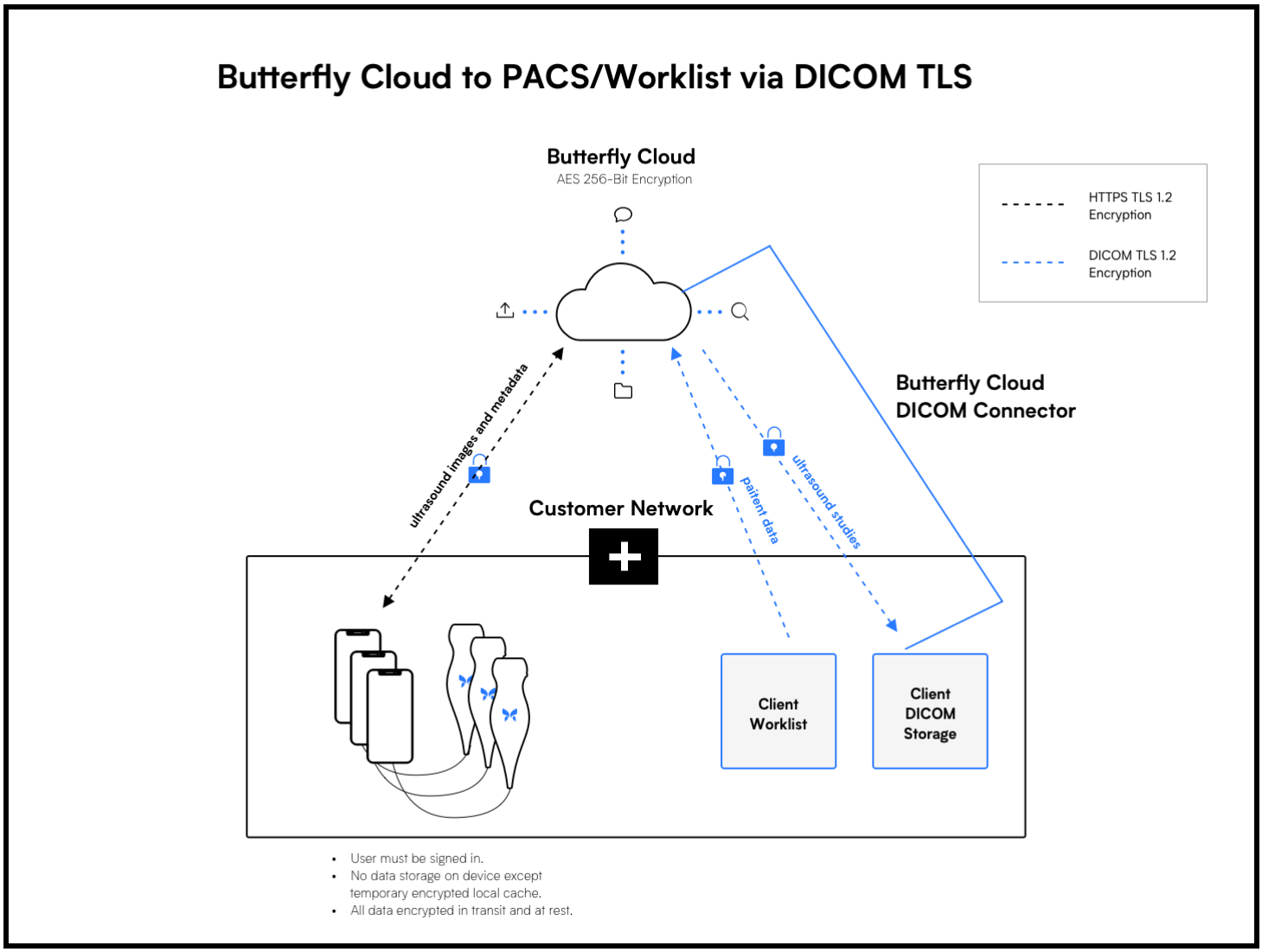


Figure 3: Butterfly Cloud to PACS/Worklist via DICOM TLS data flow.

Option 3: Butterfly Cloud to PACS/WORKLIST via DMZ (Demilitarized Zone)

The 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).

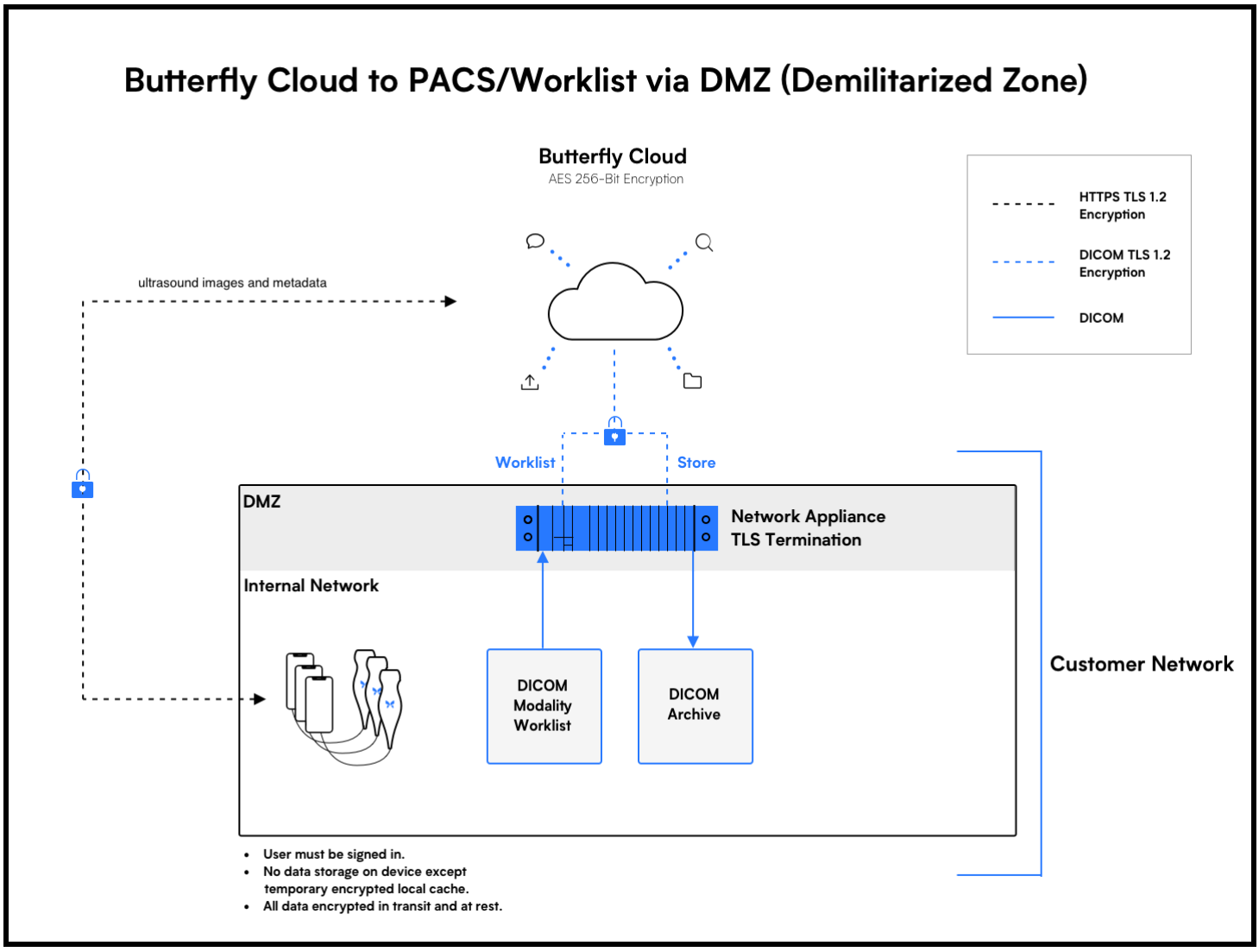


Figure 4: Butterfly Cloud to PACS/Worklist via DMZ (Demilitarized Zone) data flow.

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.