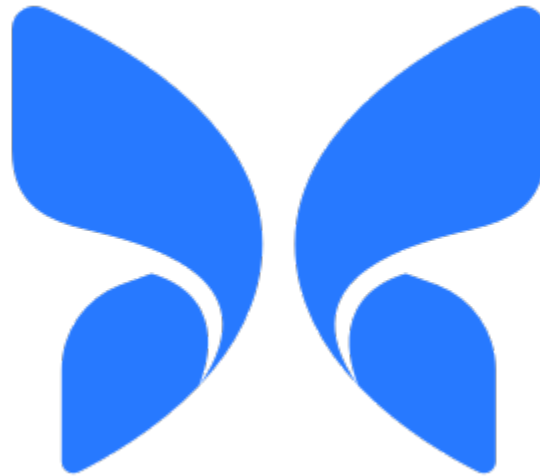


Whitepaper zur Sicherheit und Technologie von Butterfly Network

Verstehen, Einführen und Absichern von Butterfly iQ in Ihrer Organisation



Inhaltsverzeichnis

Einführung	3
Medizinische Bildgebung mit Ultraschall	3
Butterfly iQ und das Produkt-Ökosystem von Butterfly Network	3
Produkt-Ökosystem des Butterfly Network	4
Butterfly iQ-Schallkopf	5
Butterfly iQ-App	5
Butterfly Cloud	5
Butterfly Cloud Krankenhaus-Verbindung (Link oder TLS)	5
Sicherheit durch Design – Unser Ansatz für Sicherheit	6
Sicherheitsprogramm und Organisation	6
Sicherheitsrichtlinien, -prozesse und -verfahren	6
Sicherer Entwicklungslebenszyklus (Secure Development Lifecycle, SDLC)	6
Zugriffskontrollen	6
Anwendungsschicht	6
Infrastrukturschicht	7
Datenschutzkontrollen	7
Notfallwiederherstellung und Betriebskontinuität	7
Compliance und Zertifizierungen	7
Optionen zur Integrationsbereitstellung	8
Option 1 – Standardkonnektivität: iQ Mobile App zur Butterfly Cloud	8
Option 2 – Butterfly Link: DICOM-Endpunkte, EMR und Geräte von Drittanbietern zur Butterfly Cloud	9
Option 3: Butterfly Cloud zu PACS/Worklist über DICOM TLS	10
Option 4: Butterfly Cloud zu PACS/WORKLIST über demilitarisierte Zone (DMZ)	11
Zusammenfassung	12

Einführung

Dieses Whitepaper richtet sich an bestehende und potenzielle Kunden, die daran interessiert sind, das Produkt-Ökosystem von Butterfly Network in die IT-Umgebung ihres Krankenhauses zu integrieren, oder dies derzeit tun.

Wir bieten einen Überblick über die Technologie, Infrastruktur, Netzwerkarchitektur und Sicherheitskontrollen von Butterfly Network. Der erfolgreichen Integration steht mit diesen Informationen nichts im Weg. Darüber hinaus bietet dieses Whitepaper einen Überblick über die Bereitstellungsoptionen, um Ihrer Organisation die Auswahl einer geeigneten Konfiguration zu erleichtern.

Dieses Dokument richtet sich an Fachkräfte in den Bereichen Klinik, IT und Sicherheit. Teile dieses Dokuments erfordern Kenntnisse über Netzwerkarchitekturen, Betriebssysteme, Verschlüsselung und Sicherheitskontrollen.

Medizinische Bildgebung mit Ultraschall

Ultraschall ist eine lebensrettende Methode der medizinischen Bildgebung, die es Ärzten ermöglicht, die Anatomie ihrer Patienten auf sichere und nichtinvasive Weise zu visualisieren.

Im Gegensatz zu anderen wichtigen bildgebenden Verfahren wie dem Röntgen oder der Computertomographie (CT), die potenziell schädliche ionisierende Strahlung abgeben, erzeugt Ultraschall nur hochfrequenten Schall. Auch wenn Ultraschall viele Vorteile hat, ist eine breite Abdeckung aufgrund der hohen Kosten und der Größe der traditionellen Geräte nur eingeschränkt möglich.

Beim herkömmlichen Ultraschall wird ein elektrischer Strom durch einen Kristallverbundstoff namens PZT (Blei-Zirkonat-Titanat) geschickt. Dieses Material agiert als Wandler, der elektrische Energie in Schallwellen umwandelt, die an den Strukturen im Inneren des Körpers reflektiert werden. Bei ihrer Rückkehr zu den Kristallen im Schallkopf werden diese Echos wieder in elektrische Signale umgewandelt und von einem Computer zu einem bewegten Bild verarbeitet.

Dieser Prozess erfordert in der Regel sperrige, leistungsstarke, teure, auf einem Wagen montierte Computer, die für die Schwerfälligkeit traditioneller Systeme verantwortlich sind. Darüber hinaus erfordern herkömmliche Ultraschallsysteme aufgrund der inhärenten Grenzen von Schallwandlern mit Kristallen mehrere teure, empfindliche Schallköpfe (auch Sonden genannt), die jeweils speziell für die Abbildung eines bestimmten Körperteils ausgelegt sind.

Butterfly iQ und das Produkt-Ökosystem von Butterfly Network

Die grundlegende Innovation von Butterfly Network ermöglicht die Entwicklung eines Ultraschallgeräts auf einem Chip, ohne dass dafür sperrige Computer oder Schallköpfe mit Kristallen erforderlich sind. Dies ist vergleichbar mit dem Wandel in der Fotografie vom Film zur Digitalkamera. Unser chipbasierter Ansatz bietet den Anwendern von Ultraschallgeräten drei wesentliche Vorteile:

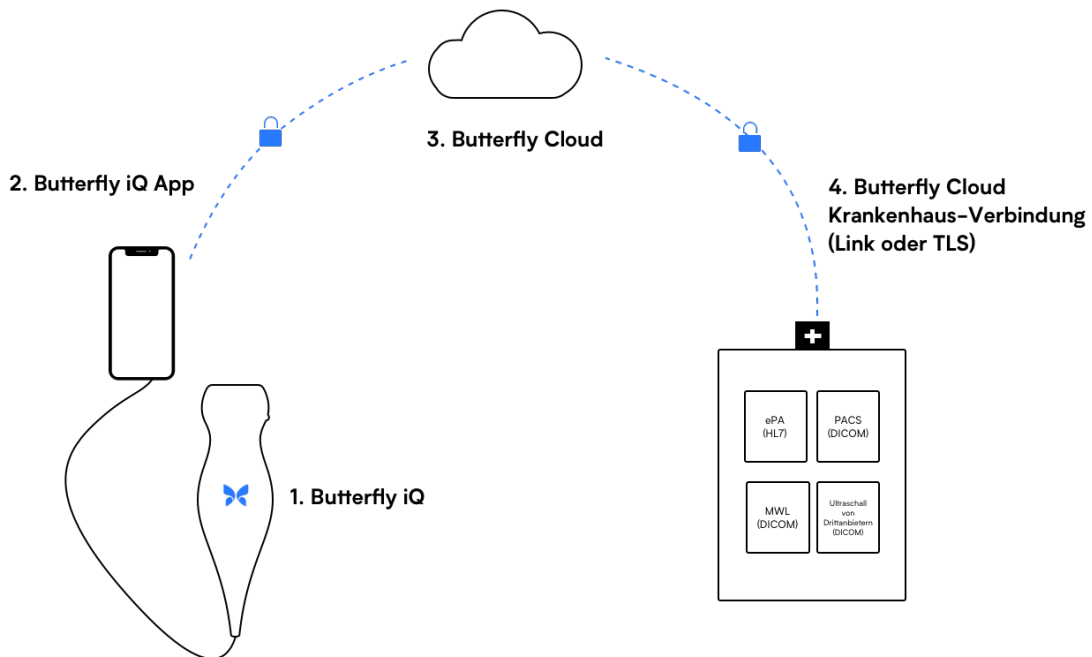
1. **Preiswert** – Butterfly iQ kostet 40-mal weniger als herkömmliche Ultraschallgeräte.
2. **Vielseitig** – Butterfly iQ kann den gesamten Körper mit einer einzigen Sonde scannen.
3. **Tragbar** – Butterfly iQ passt in die Kitteltasche.

Produkt-Ökosystem des Butterfly Network

Das Produkt-Ökosystem von Butterfly Network besteht aus vier Komponenten:

1. Butterfly iQ-Schallkopf
2. Butterfly iQ-App
3. Butterfly Cloud
4. Butterfly Cloud Krankenhaus-Verbindung (Link oder TLS)

Abbildung 1. Produkt-Ökosystem des Butterfly Network



Datenfluss im Produkt-Ökosystem von Butterfly Network. Alle übertragenen und aufbewahrten Daten werden verschlüsselt.

Butterfly iQ-Schallkopf

Butterfly iQ ist das weltweit einzige Ganzkörper-Ultraschallgerät. Bei einem Preis von weniger als 2.000 USD erreicht Butterfly iQ die klinische Vielseitigkeit und Leistung traditioneller Maschinen, die 40-mal mehr kosten.

Butterfly iQ kann den Körper mit einem einzigen Chip scannen. Butterfly Network ersetzt herkömmliche piezoelektrische Kristalle durch die Ultrasound-on-Chip-Technologie, bei der 9.000 kapazitive Ultraschallwandler mit Mikrotechnik Schallwellen von 1–10 MHz erzeugen und empfangen.

Butterfly iQ-App

Der Butterfly iQ-Schallkopf stellt eine Verbindung zu einem mobilen Gerät her, auf dem die mobile Butterfly iQ-App läuft. Diese kann im entsprechenden App-Store heruntergeladen werden. Die mobile App streamt in Echtzeit Ultraschallbilder vom Schallkopf und ermöglicht es dem Benutzer, Scan-Parameter wie Bildverstärkung und -tiefe zu regeln.

Nach Abschluss einer Untersuchung ermöglicht die mobile Butterfly iQ-App die nahtlose Archivierung und gemeinsame Nutzung von Ultraschallstudien mithilfe der Integration in die Butterfly Cloud. Die in der Butterfly Cloud gespeicherten Daten entsprechen den länderspezifischen Datenschutzgesetzen, einschließlich, aber nicht beschränkt auf HIPAA, DSGVO, APP und PIPEDA. Zusammen bieten die Butterfly Cloud, die mobile Butterfly iQ-App und die Butterfly iQ-Schallsonde die Funktionalität, Leistung und Vielseitigkeit eines herkömmlichen Ultraschallgeräts.

Butterfly Cloud

Die Butterfly Cloud bietet allen Benutzern unbegrenzten und verschlüsselten Speicherplatz für Bilder. Ein Zugriff auf diese Untersuchungen ist über die mobile Butterfly iQ App oder über jeden Webbrowser möglich. Benutzer können ihre Cloud in getrennte „Archive“ (d. h. Ordner) unterteilen, die zur Organisation der über die mobile Butterfly iQ App hochgeladenen Untersuchungen verwendet werden. Untersuchungen können mit anderen ausgetauscht werden. Dies erfolgt über anonymisierte Untersuchungslinks, die von der mobilen App oder dem Webbrowser generiert werden.

Kunden, die eine Team-Mitgliedschaft von Butterfly iQ erwerben, können außerdem die sichere Zusammenarbeit zwischen mehreren Anwendern garantieren, Bilder teilen und die Echtzeit-Kommentarfunktionen nutzen. Diese Funktionen ermöglichen eine Zusammenarbeit zwischen Pflegeteams, die sowohl HIPAA als auch andere internationale Datenschutzstandards wie DSGVO/APP erfüllt, und erleichtern die Verwaltung von abteilungsweiten, patientennahen (point of care, POC) Ultraschallprogrammen.

Und nicht zuletzt ermöglicht die Butterfly Cloud den sicheren Datenaustausch zwischen Endanwendern und dem Krankenhausinformationssystem, das zur Unterstützung der Rechnungsstellung für Ultraschalluntersuchungen und der Kontinuität der Versorgung durch die Integration mit dem Butterfly DICOM-Anschluss erforderlich ist.

Butterfly Cloud Krankenhaus-Verbindung (Link oder TLS)

Der Krankenhausanschluss von Butterfly iQ erstellt eine verschlüsselte Verbindung zwischen den DICOM-Endpunkten Ihres Krankenhauses, der elektronischen Krankenakte (EMR), den Ultraschallgeräten von Drittanbietern und dem Produkt-Ökosystem von Butterfly Network. Der Krankenhausanschluss von Butterfly Cloud kann mit einer vor Ort ausführbaren Datei namens Butterfly Link oder unter Verwendung von DICOM TLS (Transport Layer Security, V. 1.2) konfiguriert werden. Jede Option ermöglicht eine verschlüsselte Punkt-zu-Punkt-Kommunikation zwischen Ihrer Organisation und Butterfly Cloud, sodass kein VPN-Tunnel benötigt wird.

Der Krankenhausanschluss von Butterfly Cloud kann auch verwendet werden, um Benutzern den Zugriff auf den DICOM Modality Worklist-Server der Einrichtung zu ermöglichen, wodurch die langsame und fehleranfällige manuelle Dateneingabe überflüssig wird.

Sicherheit durch Design – Unser Ansatz für Sicherheit

Wir bei Butterfly Network glauben, dass es in unserer Verantwortung liegt, Geräte und Software zu entwickeln, die von vornherein sicher sind und dem Schutz der Privatsphäre der Patienten besondere Priorität einräumen. Wir wissen, dass unseren Kunden Patientendaten sehr wichtig sind. Durch die Nutzung der Butterfly Cloud können Sie unsere Sicherheits- und Konformitätskontrollen, z. B. die Datenlokalisierung, übernehmen und trotzdem gewährleisten, dass die Patientendaten weiterhin in Ihrem Besitz bleiben.

Dieser Abschnitt gibt einen umfassenden Überblick darüber, wie wir die wichtigsten Ebenen unserer Infrastruktur, unsere Cloud und unsere gehosteten Datenzentren sichern. Weitere Informationen darüber, wer wir sind, wie wir personenbezogene Daten sammeln und verwenden und wie Sie Ihre Datenschutzrechte ausüben können, finden Sie in unseren Datenschutzhinweisen <https://butterflynetwork.com/privacy-notice>. Antworten auf Fragen zu unserem umfassenden Datenschutzprogramm finden Sie auch in den häufig gestellten Fragen bezüglich des Globalen Datenschutzes <https://www.butterflynetwork.com/global-privacy>. Unsere Datenschutzerklärung für Patienten <https://www.butterflynetwork.com/patient-privacy> erklärt, wie wir Patientendaten nach der Verwendung des Butterfly iQ-Geräts durch unsere Kunden und darüber hinaus sammeln und verwenden.

Sicherheitsprogramm und Organisation

Das Sicherheitsprogramm von Butterfly nutzt branchenführende, risikobasierte Frameworks und Standards. Butterfly verfügt über ein Sicherheitsteam unter einem leitenden Informationssicherheitsbeauftragten (Chief Information Security Officer, CISO), der für die Entwicklung und Aufrechterhaltung von Sicherheitsrichtlinien, die Durchsetzung von Sicherheitsmaßnahmen und die Überwachung der technischen Sicherheit im Unternehmen und verbundenen Dritten verantwortlich ist.

Sicherheitsrichtlinien, -prozesse und -verfahren

Bei Butterfly verstehen wir, dass die Förderung einer funktionierenden Sicherheitskultur damit beginnt unseren Mitarbeitern Sicherheitsrichtlinien, -prozesse und -verfahren zur Verfügung zu stellen, die ihnen helfen, gute Entscheidungen beim Aufbau unserer Produkte und der Verwaltung sensibler Kundendaten zu treffen.

Sicherer Entwicklungslebenszyklus (Secure Development Lifecycle, SDLC)

Butterfly verfolgt den Ansatz „Secure by Design“ (Sicherheit durch Design), wobei die Sicherheit auf allen Stufen der Produkt- sowie Anwendungsentwicklung die höchste Priorität hat. Wir implementieren Kontrollmaßnahmen, wie z. B. Bedrohungsmodelle für neue Funktionen, Codeüberprüfung, Regressionstests, Bereitstellungskontrollen, Schwachstellenüberprüfung und Penetrationstests.

Zugriffskontrollen

Anwendungsschicht

Die mobilen und Internetanwendungen von Butterfly iQ erfordern eine strenge Benutzerauthentifizierung. Die mobile Butterfly iQ-App erfordert, dass die Hardware-Geräteverschlüsselung aktiviert ist, bevor Sie sich anmelden und scannen können.

Alle übertragenen und aufbewahrten Daten werden verschlüsselt. Administratoren einer Butterfly Cloud-Team-Mitgliedschaft behalten die volle Kontrolle darüber, welche Benutzer Zugriff auf ihre persönlichen Daten haben.

Butterfly hat für seine Unternehmenskunden drei zusätzliche Ebenen mit erweiterter, defensiver Sicherheit entwickelt: einmaliges Anmelden (Single Sign On), Einschränkungen der Mobilitätsverwaltung bei Unternehmenskunden

(Enterprise Mobility Management Restrictions) und individuelle Zeitüberschreitung bei Inaktivität (Custom Inactivity Timeout).

Infrastrukturschicht

Die Butterfly Cloud ist ein mandantenfähiges, dezentralisiertes System, das mit einer hochgradig redundanten Architektur entwickelt wurde. Butterfly Cloud nutzt die Infrastruktur der Amazon Web Services (AWS) und umfasst mehrere Ebenen von physischen, politischen und technischen Sicherheitsvorkehrungen.

Datenschutzkontrollen

Kundendaten in der Butterfly Cloud werden außerdem durch eine Container-Orchestrierungsplattform (Aptible Enclave) geschützt, die Best Practices und Kontrollen für den Einsatz von Gesundheitsanwendungen implementiert, z. B. AES 256-Bit-Verschlüsselung für ruhende Daten, Überwachung und Protokollierung, Schwachstellenmanagement und Systemhärtung.

Notfallwiederherstellung und Betriebskontinuität

Butterfly Network nutzt eine Kombination aus dezentralen Cloud-Verfügbarkeitszonen sowie tägliche Backups auf AWS-Servern, um im Katastrophenfall eine problemlose Wiederherstellung von Kundendaten zu gewährleisten. Es wurden Datensicherungs- und Notfallpläne etabliert, die vierteljährlich getestet werden.

Compliance und Zertifizierungen

Butterfly Network ist SOC 2 (Typ 1) zertifiziert, was die Einhaltung der Kriterien für Datenschutz, Sicherheit, Vertraulichkeit und Verfügbarkeit sowie der HIPAA- und HITECH-Vorschriften bestätigt. Darüber hinaus verfügt Butterfly über ein globales Datenschutzprogramm, das den Anforderungen der Datenschutzbestimmungen, wie z. B. der Datenschutz-Grundverordnung der EU entspricht.

Unsere Sicherheitskontrollen werden ständig weiterentwickelt, um mit der dynamischen Bedrohungslandschaft Schritt zu halten. Bitte informieren Sie sich regelmäßig auf unserer Webseite über unsere neuesten Kontrollen.

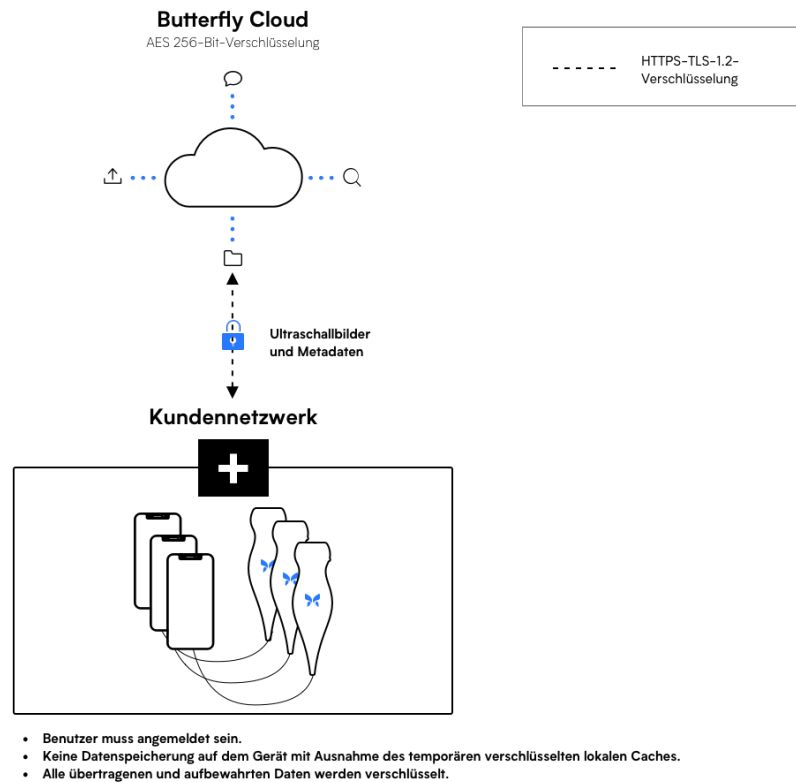
Optionen zur Integrationsbereitstellung

Butterfly Network unterstützt vier Bereitstellungskonfigurationen zur Integration in die IT-Umgebung der Kunden.

Option 1 – Standardkonnektivität: iQ Mobile App zur Butterfly Cloud

Die sichere Übertragung der Ultraschall-Bilddaten von der mobilen Butterfly iQ-App zur Butterfly Cloud erfolgt über HTTPS mit TLS 1.2-Verschlüsselung. Die mobile Butterfly iQ-App und die Butterfly Cloud erfordern die Verschlüsselung von Patienten-/Kundendaten während des Transports und im Ruhezustand. Bei dieser Konfiguration sind keine Änderungen an den IT-Systemen der Kunden erforderlich.

Abbildung 2. Butterfly iQ zur Butterfly Cloud

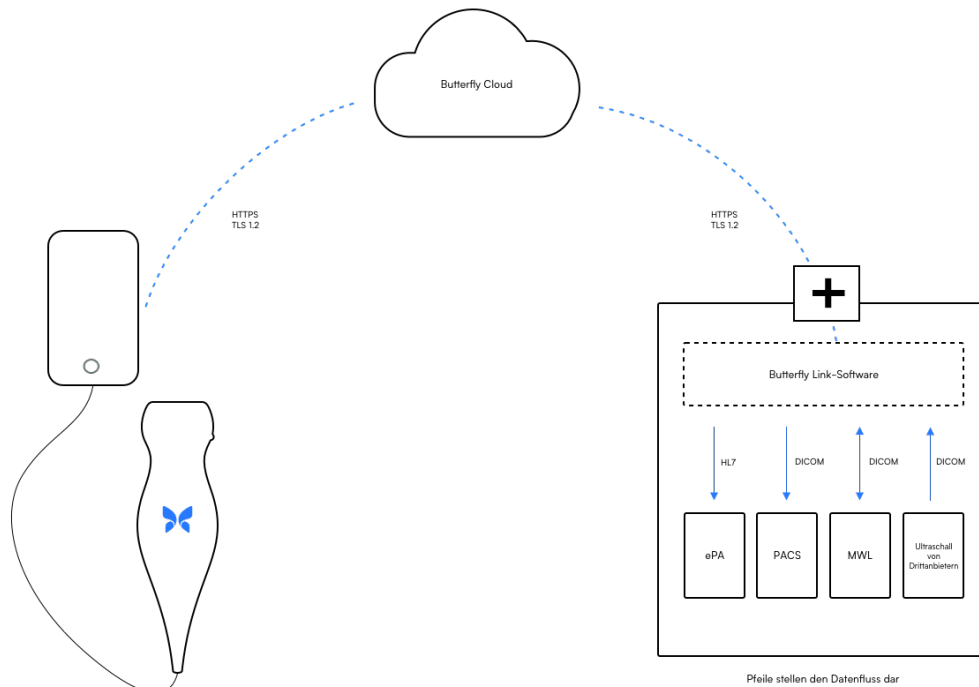


Standardkonnektivität: Datenfluss von der mobilen Butterfly iQ-App zur Butterfly Cloud.

Option 2 – Butterfly Link: DICOM-Endpunkte, EMR und Geräte von Drittanbietern zur Butterfly Cloud

Die sichere Übertragung der Ultraschall-Bilddaten von der mobilen Butterfly iQ-App zur Butterfly Cloud erfolgt über HTTPS mit TLS 1.2-Verschlüsselung. Die mobile Butterfly iQ-App und die Cloud erfordern die Verschlüsselung von Patienten-/Kundendaten während des Transports und im Ruhezustand. Bei dieser Konfiguration sind keine Änderungen an den IT-Systemen der Kunden erforderlich.

Abbildung 3. Butterfly Link: Hausinterner Client

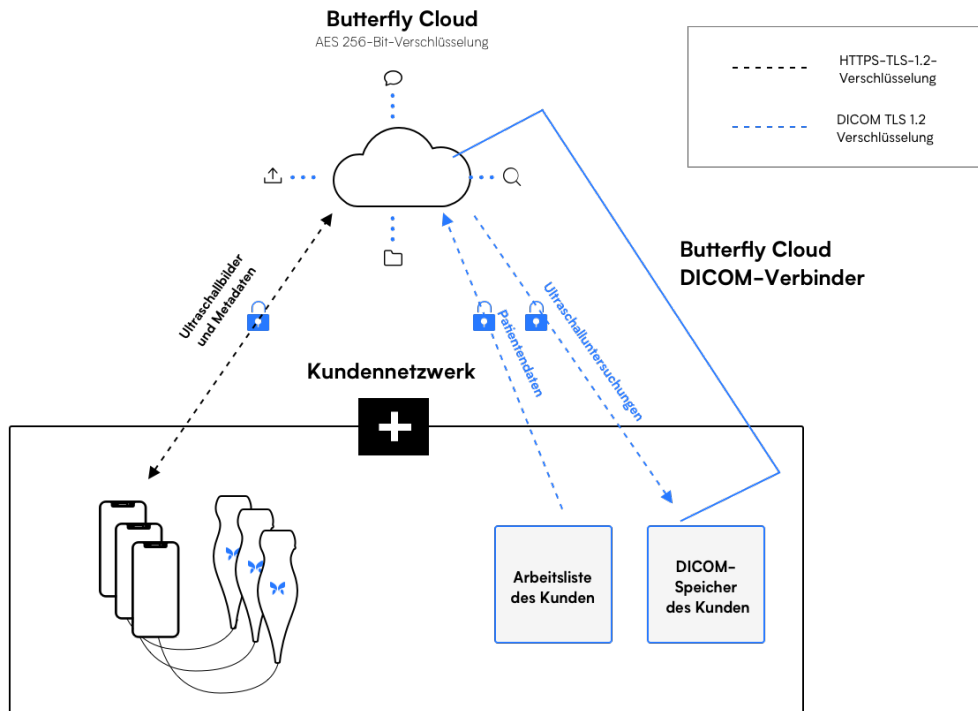


Butterfly Link: Ausführbares Programm, das DICOM-Endpunkte, EMR und Ultraschallgeräte von Drittanbietern sicher in die Butterfly Cloud integriert.

Option 3: Butterfly Cloud zu PACS/Worklist über DICOM TLS

Die Butterfly Cloud kann so konfiguriert werden, dass Untersuchungen sicher an ein PACS übertragen und/oder eine Modality Worklist (MWL) abgefragt werden können. Die Verschlüsselung der Kommunikation erfolgt mit TLS 1.2.

Abbildung 4. Butterfly Cloud zu PACS/Worklist über DICOM TLS



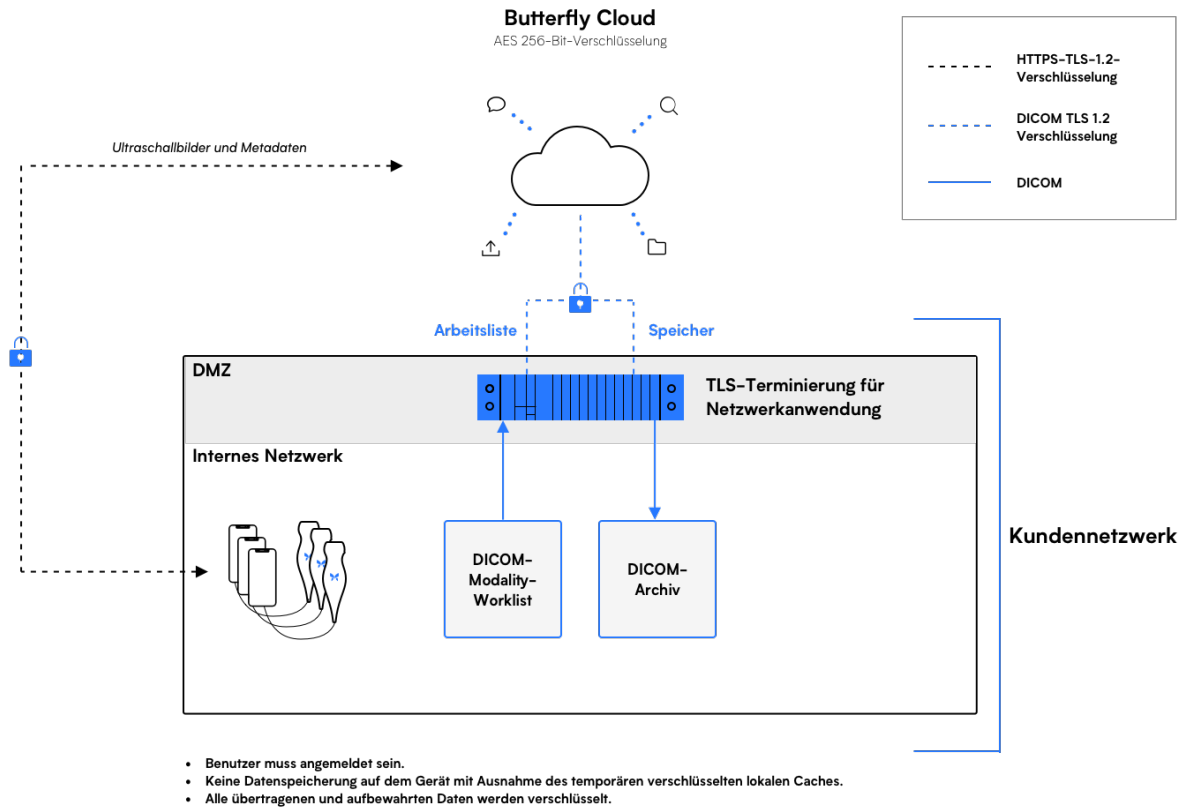
- Benutzer muss angemeldet sein.
- Keine Datenspeicherung auf dem Gerät mit Ausnahme des temporären verschlüsselten lokalen Caches.
- Alle übertragenen und aufbewahrten Daten werden verschlüsselt.

Datenfluss von der Butterfly Cloud zu PACS/Worklist über DICOM TLS

Option 4: Butterfly Cloud zu PACS/WORKLIST über demilitarisierte Zone (DMZ)

Die Butterfly Cloud kann so konfiguriert werden, dass Untersuchungen sicher an ein PACS übertragen und/oder eine Modality Worklist (MWL) abgefragt werden können, deren Verbindung durch eine Krankenhaus-DMZ erfolgt. Die TLS-Verbindung kann an der DMZ oder direkt an den DICOM-Endpunkten (wie in Option 2) beendet werden.

Abbildung 5. Butterfly Cloud zu PACS/Worklist über demilitarisierte Zone (DMZ)



Datenfluss von der Butterfly Cloud zu PACS/Worklist über demilitarisierte Zone (DMZ)

Zusammenfassung

Die Sicherheit von Kunden- und Patientendaten hat für uns oberste Priorität. Bitte kontaktieren Sie uns bei Fragen zu diesen Richtlinien oder für Hilfe bei der Integration unter support@butterflynetwork.com oder besuchen Sie unsere Wissensdatenbank unter support.butterflynetwork.com.