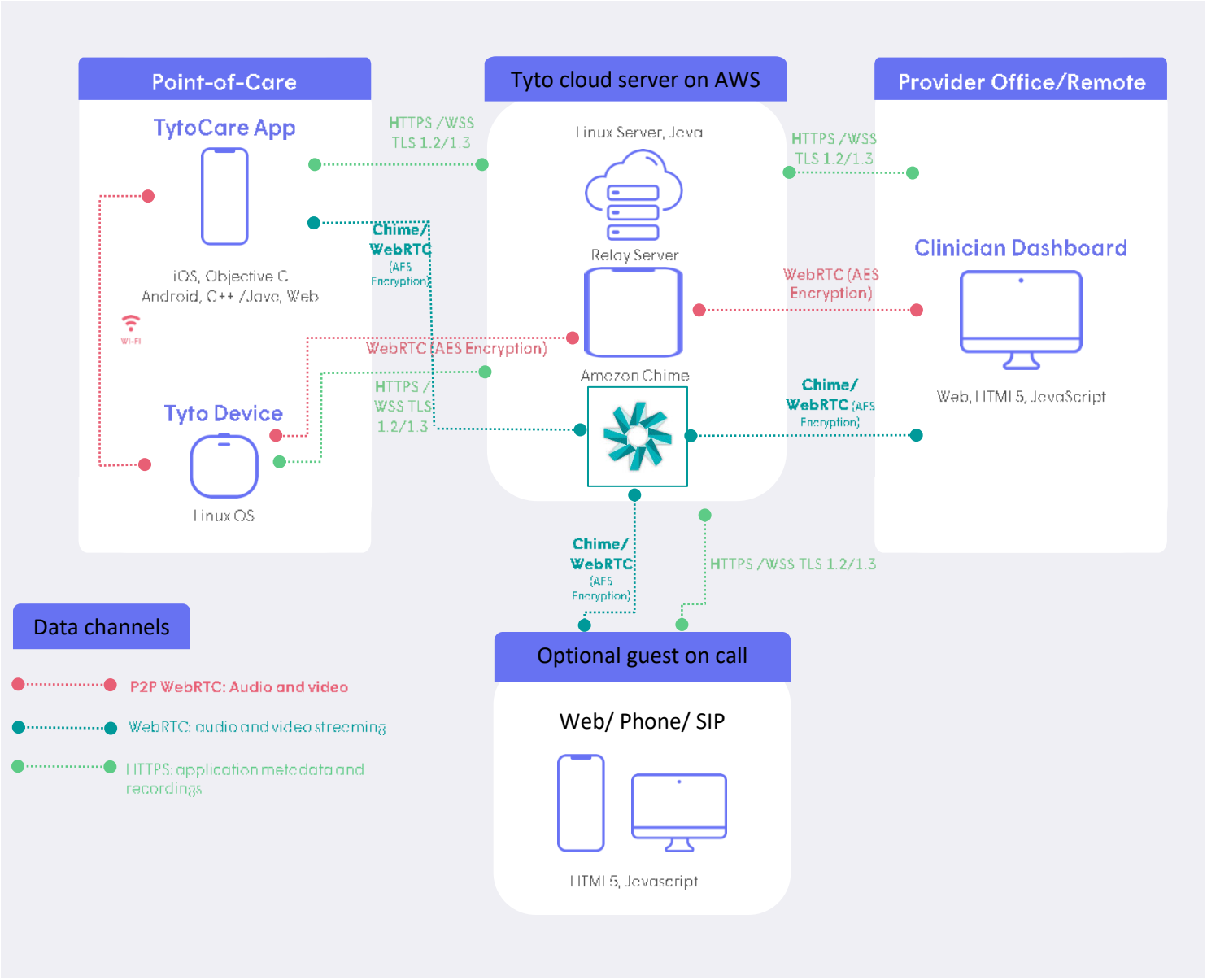
TytoCare IT Platform Overview

TytoCare Architecture & Data Flow

This document provides an overview of the TytoCare platform IT elements. It addresses the data flow architecture, connectivity, and security of the TytoCare platform.

TytoCare platform architecture with Amazon Chime as the communications service



Wi-Fi Network Requirements

The TytoCare platform works with wireless networks utilizing the WPA2 Personal (PSK) or Enterprise (IEEE 802.1X) security protocol and transmitting over the 2.4 GHz and 5 GHz* frequency bands. Supported WPA2 Enterprise protocols are PEAP-MSCHAPv2 and EAP-TLS.

The Wi-Fi network must:

- Support ICMP protocol to allow the Tyto App and Tyto Device to communicate and complete the pairing process successfully.
- Support WebSocket protocol (WSS) on TCP ports 443 (required for the Tyto Device and Tyto App's communication with the Tyto Platform).
- Allow communication between Tyto App and Tyto Device on ports 49152- 65534 UDP.

* Supported on TytoCare G2 devices only

The following configurations are not supported:

- Networks with a proxy server or those that require a secondary sign in
- 802.11w

Wireless connection speed requirements:

Latency: < 350 ms

Bandwidth

Recommended:
- Download: 20 Mbps
- Upload: 5 Mbps

Minimum:
- Download: 2 Mbps
- Upload: 2 Mbps

Network Firewall Requirements

The TytoCare solution requires the following TCP/UDP ports to function properly:

- Outbound TCP ports 443, 3478
- Outbound UDP ports 443, 3478, 49152-65534

The following are components of the Tyto Platform that need to be accessed from clinicians' computers that are on the organization's network:

Role	Region	IP / Destination	Ports	Protocol
Application server & API	USA Canada EU Australia	app-cloud.tytocare.com app-cloudca.mnt.tytocare.com app-cloudeu.tytocare.com app-cloudanz.sdn.tytocare.com	443	TCP
Amazon Chime	All	99.77.128.0/18 *.chime.aws chime.aws	443	TCP
Amazon Chime	All	99.77.128.0/18 *.chime.aws chime.aws	3478	UDP
WebRTC Signaling	All	websync-cloud.tytocare.com websync-prod.tytocare.com websync-prod.irl.tytocare.com	443	TCP
WebRTC Stun/Turn	All	141.226.185.1 141.226.185.7 141.226.185.8 141.226.185.11 141.226.185.21 141.226.187.2 141.226.187.3 141.226.187.4 141.226.187.14 141.226.187.15 3.230.86.251 34.205.83.16 54.152.40.26 3.232.47.201 54.151.0.39	443, 3478, 49152-65534	UDP

		54.176.56.132 3.251.32.233 54.155.101.137 13.244.184.123 13.245.173.222 51.17.177.94 51.17.180.53 51.17.188.156 51.17.197.203		
Twilio Stun/Turn	All	13.210.2.128 - 13.210.2.159 54.252.254.64 - 54.252.254.127 3.25.42.128 - 3.25.42.255 18.231.105.32 - 18.231.105.63 177.71.206.192 - 177.71.206.255 18.230.125.0 -18.230.125.127, 52.59.186.0 - 52.59.186.31 18.195.48.224 - 18.195.48.255 18.156.18.128 - 18.156.18.255 52.66.193.96 - 52.66.193.127 52.66.194.0 - 52.66.194.63 3.7.35.128 - 3.7.35.255 52.215.253.0 - 52.215.253.63 54.171.127.192 - 54.171.127.255 52.215.127.0 - 52.215.127.255 3.249.63.128 - 3.249.63.255 13.115.244.0 - 13.115.244.31 54.65.63.192 - 54.65.63.255 18.180.220.128 - 18.180.220.255 13.229.255.0 - 13.229.255.31 54.169.127.128 - 54.169.127.191 18.141.157.128 - 18.141.157.255 34.203.254.0 - 34.203.254.255 54.172.60.0 - 54.172.61.255 34.203.250.0 - 34.203.251.255 3.235.111.128 - 3.235.111.255 34.216.110.128 - 34.216.110.159 54.244.51.0 - 54.244.51.255 44.234.69.0 - 44.234.69.127 *.turn.twilio.com *.stun.twilio.com	443, 3478	TCP, UDP
Web server	USA Canada EU Australia	cloud.tytocare.com cloudca.mnt.tytocare.com cloudeu.tytocare.com cloudanz.sdn.tytocare.com	443	TCP

Content server	All	static-cloud.tytocare.com	443	TCP

UDP ports 443, 3478, 49152-65534: Required for TytoCare Device traffic, suboptimal videoconferencing performance with Amazon Chime over UDP, and Twilio Network Traversal Service.

HTTPS port 443: The TytoCare servers are hosted in the AWS cloud and located behind a web application firewall (WAF). Cloud WAF assigns an IP within the following ranges that can be safelisted in the organization's firewall:

- 199.83.128.1 - 199.83.135.254
- 198.143.32.1 - 198.143.63.254
- 149.126.72.1 - 149.126.79.254
- 103.28.248.1 - 103.28.251.254
- 185.11.124.1 - 185.11.127.254
- 45.64.64.0 - 45.64.67.255
- 192.230.64.1 - 192.230.127.254
- 107.154.0.0 - 107.154.255.254
- 45.60.0.1 -45.60.255.254
- 45.223.0.1 - 45.223.255.254
- 131.125.128.1-131.125.255.254
- 2a02:e980:0:0:0:0:0:0 - 2a02:e987:ffff:ffff:ffff:ffff:ffff:ffff

The updated list of the Twilio IP ranges is available at: https://www.twilio.com/docs/stun-turn/regions

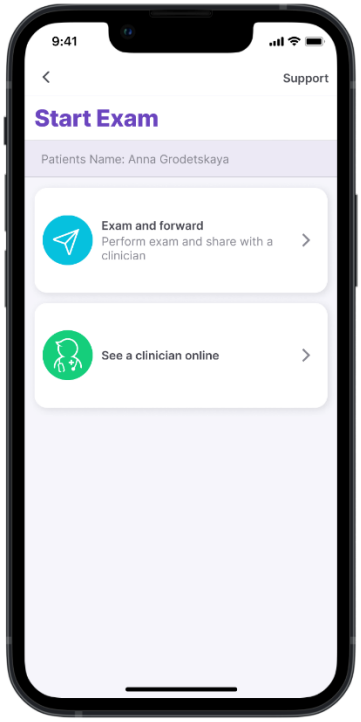
The updated list of the Cloud WAF IP ranges is available at: https://docs.imperva.com/howto/c85245b7

The TytoCare platform calls the following domains upon requirement. All the domains on this list **must** be safelisted for TCP.

Domain	Port	Role
*.tytocare.com	443	Platform Infrastructure
*.cloudfront.net	443	Static web files
*.incapdns.net *.impervadns.net	443	Web Application Firewall (Incapsula/Imperva)
*.amazon.com *.amazonaws.com	443	Amazon Web Services
accounts.google.com	443	Multi-factor authentication services using Google Authenticator
redbend.com	443	Tyto Device remote upgrade management
in-addr.arpa	443	Reverse DNS lookup
*.logz.io	443 8071	Logs for analytics service
google-analytics.com	443	Platform usage statistics
*.crashlytics.com	443	Logs for TytoCare App crash events
*.firebaseio.com	443	Statistics about user interaction with TytoCare App
*.mixpanel.com	443	Platform usage analytics
wss://watchrtc.testrtc.com	443	Video conferencing quality monitoring service
*.walkme.com	443	Loads the WalkMe player for clinician tutorials
s3.walkmeusercontent.com	443	Displays images for WalkMe player clinician tutorials

System Description

TytoCare App



Free app downloadable from the Apple and Google Play app stores. The TytoCare App authenticates the user before providing access to the TytoCare App functionality.

The TytoCare App enables the following capabilities:

- Initiating an online exam with a clinician including videoconference and exam data (synchronous).
- Sending store-and-forward data to a clinician for review (asynchronous).
- Receiving notifications and responses from clinicians (inbox).

The TytoCare App immediately uploads examination data received from the Tyto Device to the Tyto Cloud Server. After confirmation that the data resides in the Tyto Cloud Server, it is erased locally. In any case of disconnection from the Tyto Cloud Server, the examination data is immediately purged locally (from the TytoCare App) until a reconnection is established with the Tyto Cloud Server.

TytoCare Device

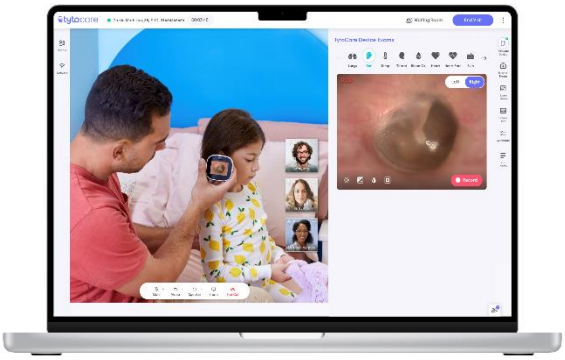
Used to perform the examinations, collect examination data, and transfer it (via the Tyto Cloud Server) to the TytoCare App using TLS 1.2/1.3 encryption. The TytoCare Device also streams the real-time data to the TytoCare App and transmits short-time recordings to the Clinician Dashboard App using a secured peer-to-peer protocol (WebRTC, utilizing DTLS).

Once the examination data has been securely transferred from the TytoCare App to the Tyto Cloud Server, the data is erased locally.

Pairing: TytoCare App and TytoCare Device

To establish a secure connection between the TytoCare App and the TytoCare Device, a pairing transaction must occur when connecting the Tyto solution to a new Wi-Fi network, or at any time a stored network's credentials (SSID or password) are modified. The TytoCare App initiates the pairing process, and the following parameters are transferred using UDP packets to the TytoCare Device via a QR code: SSID, password, time, pair ID, IP: Port.

TytoCare Clinician Dashboard



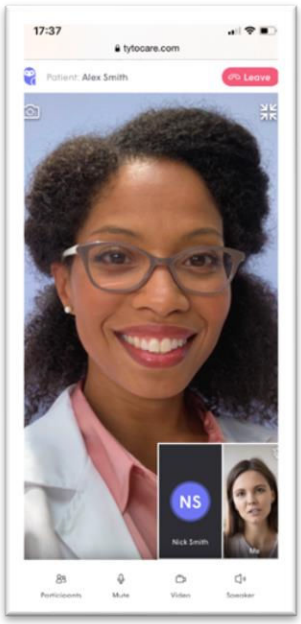
The TytoCare Clinician Dashboard is a secure browser-based HTML 5 web app. To fully utilize all the dashboard capabilities, it is required to use a device running on a supported operating system and browser. For Windows-based operating systems, we support the latest two versions of Google Chrome and Microsoft Edge (Chromium-based). On macOS, we support the latest two versions of Google Chrome and Safari. These browsers offer native support for WebRTC and in-browser audio playback.

The TytoCare Clinician Dashboard enables the following capabilities:

- Conduct online exams (synchronous).
- Respond to patient store-and-forward requests (asynchronous).
- Review exam history (inbox).

The TytoCare Clinician Dashboard does not store any data locally (browser), does not use cookies, and is deployed on a CDN (AWS Cloud Front) to enable fast and secure access.

TytoCare Guest App



The TytoCare Guest App is a secure browser-based video and web conferencing application. The app enables invited guests to join an in-progress TytoCare visit between a clinician and a patient, such as an interpreter or medical colleague.

The TytoCare Guest App enables the following capabilities:

1. Video conferencing service: Clinicians and patients can meet virtually, either via video or audio, or both.
2. Control over user permissions: Clinicians can invite guests to join a TytoCare visit. With the admit feature, clinicians can determine when guests are admitted into the visit.
3. Screen sharing: Screen sharing enables clinicians to share the content of their screen with the guests.

The conference is conducted over WebRTC and is facilitated by the Amazon Chime video conferencing and communications service.

Video Conference

The video conference is conducted over WebRTC via Selective Forwarding Unit (SFU) when the communications service is Amazon Chime. WebRTC is a secured protocol that utilizes SRTP, SCTP, and DTLS for the streams, control, and data channels.

A relayed connection is required via the TytoCare TURN servers if a symmetrical NAT is configured in the firewall. When a relayed connection is utilized, the TytoCare platform provides dedicated servers for media stream relay.

TytoCare Cloud

The Tyto Cloud is a fault-tolerant, stress-tested, and fully redundant environment running on Amazon Web Services (AWS) with the following topology:

- Dedicated VPC divided into three subnets.
- Completely managed by ACL and security groups and based on machine roles (access keys do not leave the VPC).
- Utilizing AWS elastic beanstalk – Linux-based machines running Tomcat that are monitored, updated and auto-scale automatically.

The TytoCare AWS account is secured via a two-factor authentication process:

- Server access requires an access token generated for the end-user only after authentication using a username and password.
- The Tyto Cloud Server manages patient information only via HIPAA/GDPR-compliant services such as RDS, S3, EC2 (running elastic beanstalk), and the elastic load balancer. The TytoCare Cloud database guarantees data/transaction completeness. AWS RDBMS (RDS) provides built-in mechanisms for availability, scalability, durability, and security.

User Authentication and Session Management

The following table describes the different authentication methods on the TytoCare Platform.

Component / Capabilities	TytoCare Mobile App	TytoCare Admin Console
Username and password	•	•
Biometric (Face ID or touch ID)	•	
SSO via third-party application	•	•
MFA		•

Password policy capabilities

The TytoCare platform can be configured to enforce password policy with the following capabilities:

- Password complexity with the ability to force uppercase, lowercase, digits, and special characters.
- Password expiration every X days (defaulted to 90 days)
- Minimal password length of X characters

Passwords are kept encrypted in the database with a salting mechanism.

Session Expiration

The TytoCare Platform can be configured to control the expiration of each session. The default setting is timeout after 15 minutes with automatic logout.

TytoPro

In a TytoPro setting the platform supports configuration of Enterprise Wi-Fi. Please see dedicated guide for details.

Data Encryption at Rest

TytoCare uses Advanced Encryption Standard (AES) 256-bit encryption on the recordings and metadata stored in AWS (Amazon Web Services.

Data Encryption in Transit

TytoCare uses encryption protocol TLS1.2 and TLS 1.3

Product Compliance

Security

TytoCare maintains certification in the following international standards for information security: ISO/IEC 27001:2013, ISO 27799: 2016, and SOC-2 (Type II) with mapping to HITRUST.

In addition, TytoCare conforms to the FDA cyber security guidance. In compliance with the FDA guidelines and the product design process, TytoCare has performed an in-depth threat analysis to identify cyber security risks in the platform. As part of the company's cyber security process, TytoCare has executed a penetration test and vulnerability assessment (on the entire platform), and the company policy defines that penetration tests shall be conducted routinely.

Privacy

TytoCare utilizes HIPAA and GDPR-compliant/certified AWS services. Additionally, TytoCare has implemented a technical safeguard review (HIPAA & GDPR) on the platform and has aligned its product features accordingly:

- Audit trail monitoring any access to PHI & PII.
- HIPAA, GDPR-compliant/certified user authentication mechanism, including password policies and session restrictions (e.g., auto log-off).
- PHI security and integrity mechanisms.

BAA & DPA

For HIPAA compliance of US customers TytoCare is willing to sign a BAA (Business Associate Agreement).

For GDPR compliance of EU customers TytoCare is willing to sign a DPA (Data Processing Agreement).

All TytoCare production environment-related subcontractors have a BAA & DPA agreement with TytoCare.

External Penetration Testing

TytoCare allows a third-party penetration test on a "test" environment in AWS, which is identical to the production environment.

Monitoring

TytoCare uses a suite of monitoring tools to monitor its service. This includes a SIEM/SOC solution using Elastic SIEM and a 24/7 SOC service through a 3rd party.

Data Repository Location & Security

The data collected by TytoCare is stored on AWS-dedicated & HIPAA-compliant services for storage (S3) and database (RDS). These AWS services guarantee that data-at-rest is kept encrypted. TytoCare maintains separate production environments in the following Amazon regions to support data privacy protection regulations:

- US East (North Virginia)
- Canada (Central)
- EU (Ireland)
- Australia (Sydney)

The TytoCare server topology within AWS keeps the application servers behind two levels of firewalls. In addition, the RDS (which holds the ePHI) is secured behind three levels of firewalls (2 subnets within a VPC).

File accessibility is managed by ad-hoc, time-limited policies, ensuring authorized users have access only to what they need when they need it.

Backup & Disaster Recovery

All repository data is backed up to an additional AWS account to enable recovery in case of root account hijack. Additionally, AWS has inherent capabilities in terms of disaster recovery, such as cloning data in up to three availability zones within the same region.

For more information visit us at:
www.tytocare.com

Contact us directly at:
sales@tytocare.com

Call us at:
+1-866-971-TYTO (8986)

tytocare™

Your On Demand Medical Exam