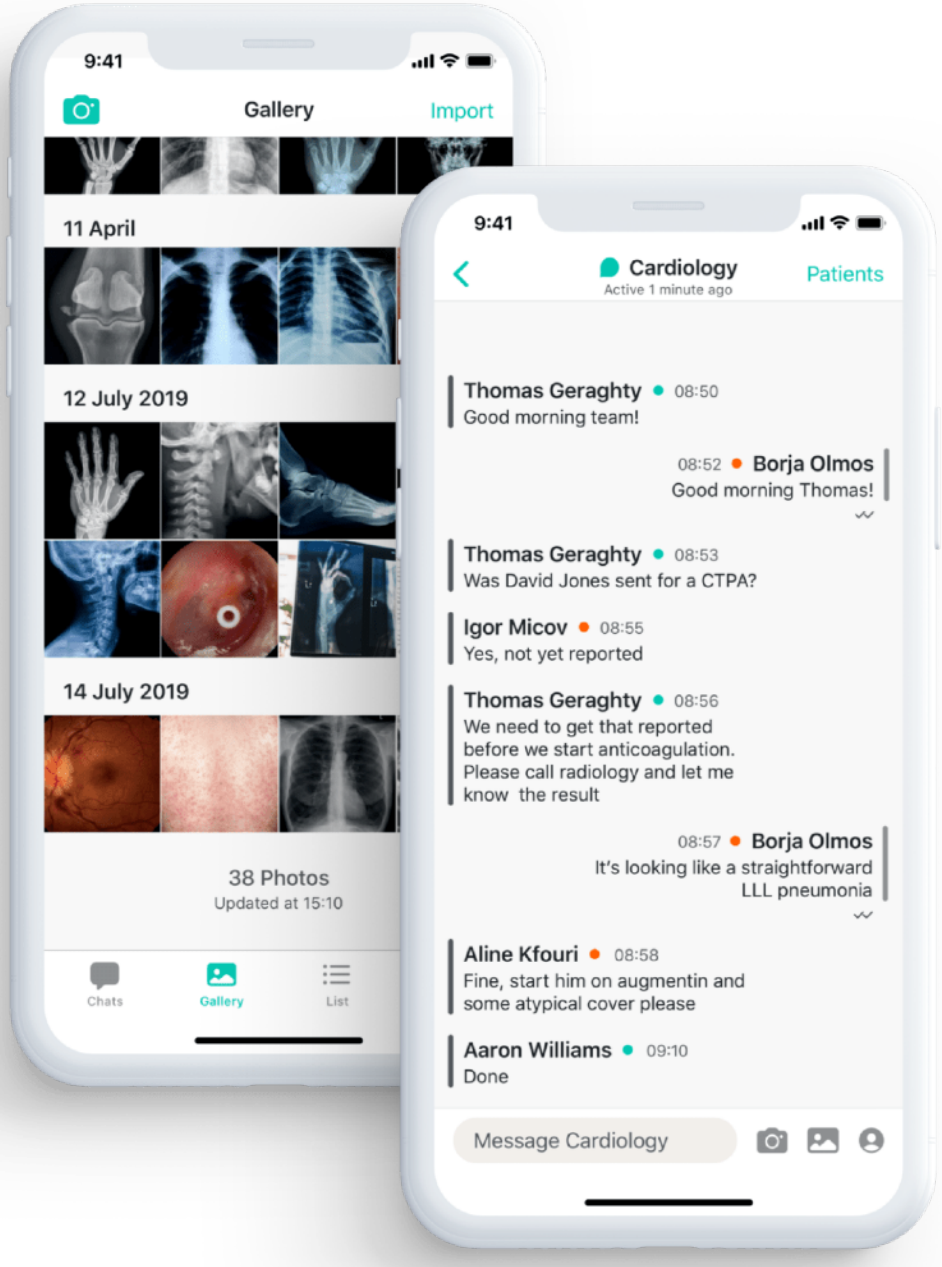
IT requirements.



pando

IT requirements

For the product to function as expected end-to-end the following requirements are needed for Trust firewall

Push Notification Service

Apple Push Notification Service
This address range is owned by Apple, in its entirety, for the delivery of Apple services. Pando uses APNS to notify users when they receive a message on the platform. This requires:

- Whitelisting the 17.0.0.0/8 address block (i.e. 17.0.0.0 to 17.255.255.254)
- Whitelisting ports 5223, 443, 2197 in this address range

Android Push Notification Service
Notification messages are delivered to the Android devices by Firebase Cloud Messaging ("FCM").
The ports to be open for incoming and outgoing messaging are: 5228, 5229, 5230

As stated by Google:
For outgoing connections, FCM doesn't provide specific IPs because our IP range changes too frequently and your firewall rules could get out of date, impacting your users' experience. Ideally, you will whitelist ports 5228-5230 with no IP restrictions. However, if you must have an IP restriction, you should whitelist all of the IP addresses in the IPv4 and IPv6 blocks listed in Google's ASN of 15169. This is a large list and you should plan to update your rules monthly. Problems caused by firewall IP restrictions are often intermittent and difficult to diagnose.

Pando Infrastructure

All port 443:

REST API	XMPP (STARTTLS)	XMPP (WSS)	XMPP (Immediate TLS)
13.248.211.177 (anycast) 76.223.90.244 (anycast)	52.56.108.139 52.56.182.79 3.9.224.170	3.11.52.145 3.11.31.42 3.11.148.249	18.130.159.61 3.11.92.146 3.11.7.214

Email

Please whitelist all email from **hellopando.com** and **app.hellopando.com**, subject to SPF/DKIM. Authentication codes to access the Pando service are sent via email; if these aren't delivered or are quarantined, users will not be able to use the service.