Contents

Introduction

COVID-19 brought most businesses, **including medical clinics to shut down**. Patients were unable to visit the Clinic disrupting the patient's continuity of care. Clinics have since been trying a mix and mash of tools - Skype, Whatsapp, Zoom, emails and chats to offer consultations. **Such modes of communication are disorganized and unsecure**. They also do not have any concept of payment, further impacting the deteriorating financial health of the clinic.

In response to this we have launched **Curofic.** Curofic is a software platform for Medical Practitioners. It lets a brick and mortar clinic, **to setup a complete Virtual Clinic**.

A virtual Clinic enables

1. Patients to book online video consults with the Medical Practitioner.
2. Clinics to auto-collect payment for consultations.
3. Practitioners to conduct Hi-Definition video consults, issue online prescriptions and schedule recalls for chronic patients.

All of this works, without the need for the patient to download or login anywhere. Secure and Simple.

There is more, Curofic can also be enabled to become your **Virtual Assistant** by getting Patients to complete intake forms and sign digital consents. Additionally, it empowers patients by giving them unparalleled access to their health data - the kind which has not been seen till date in the healthcare industry.

Curofic Security

Security in software platforms is often an afterthought. At best, a feature. Both approaches are doomed to fail. **The rise and fall of the Zoom platform in medical community has lessons for all of us to learn from.**

A secure product is **"secure"** only when it was designed ground-up with security in mind. When **each component** was added to the platform after an evaluation of wherein lies its Achilles heel. Only when you evaluate for security, will you become aware of the fallibilities in your system. This rigorous process of evaluation, identification and only then development, should be the idealistic approach to software development. Idealistic because often time is of essence, elbowing out ideals along its way.

However, when dealing with Virtual Clinics, the bar is set much higher. The tele-consultations between a Medical Practitioner and a Patient are bound by confidentiality and protected by law in almost all countries across the globe. **Security cannot be an afterthought here**. **Medical practitioners who end up getting on such an unsecure platform at best will expose themselves to medico-legal issues. At worst, will destroy the reputation of their practice. Here are the security measures we have taken to ensure our Medical Practitioners remain immune from such risks:**

1. Enterprise Grade

Our clients have trusted us to make the right technology decisions for them. Hence we took a decision to opt out from free to use, non-commercial, open source video calling infrastructure. We **"only" use enterprise grade, dedicated commercial video calling servers, backed by a Service Level Agreement and monitored by dedicated Technical teams.** Such a service comes at a cost. We need to pay per minute of the video call to access this infrastructure, and in turn we charge you for the same.

2. Encryption & Secure Routing

All signals are encrypted. Encryption used is AES-128 bit. The entire video and audio track from the Patient, to you and back is encrypted. Media in transit cannot by decrypted by pass-through. Decryption is only possible via the application id and private certificate assigned to the project. This ensures the man-in-the-middle attack is no longer a possibility.

3. Tokens

We use a signalling server, that generates a token just before a call starts. Tokens are issued behind the scene for granting access to open a video track and an audio track into the tele-consult. Without a valid token, any attempts by the user to initiate a call will fail. **Tokens cannot be guessed like one tries with passwords. They are 32 character long MD5 Hex code signature** i.e. **4.294 billion combinations.**

4. Spoofing

Each tele-consult is **signed by Curofic's secure private key**. An unauthorised person trying to join the call with a spoofed token will result in failure as the digital certificate will not match.

5. TTL

Tokens are like tickets to enter a movie hall. Our algorithms determine a variable TTL (Time To Live) period for each token. Even a valid user, with a valid token can no longer join the call, once the TTL expires. **It ensures that simply copying a token, like one can with a password, will not work,** as tokens auto-expire around the time the appointment gets over.

6. De-Identification

No personal data, no demographic data, not even your name or that of your patient goes beyond our company's servers. This means even the dedicated video calling infrastructure which is handling your tele-consult, does not know who you are. They do not know if the user is a Medical practitioner or a Patient. All that the video calling servers see are operational health metrics. For them the 2 users involved in the call are a bunch of number and alphabets, something like this

User 1: *kl0o23b6wp324d15b80d8681f856ff03*
User 2: *90d925yu14d04454a199ca8bablkac7b*

7. DDoS Attacks

Servers involved in tele consult are regularly scanned for possible security vulnerabilities. An **anti-DDoS firewall is also implemented on each cloud data centre to protect core nodes from any attack**. Additionally redundant bandwidth is maintained for core servers to ensure there is sufficient capacity and resources to minimize the risk of DDoS attacks.

8. Recording

None of the Curofic servers involved in the Tele-Consult, or the back-end video call servers, allow any kind of video or audio recording of the visit. Not having the option to record, ensures, accidentally or otherwise you cannot end up storing the recording on an external hard disk / USB drive that gets misplaced, or put it in one of those cloud storage accounts that then get hacked. **You can sleep easy knowing there are no such recordings with us, or even possible at our end.**

9. Failovers

There is no single point of failure. Servers are deployed on edge, geographically. In the event of a catastrophic failure, systems are tested to recover within 30 minutes.

10. Compliance

The dedicated video calling infrastructure used for tele-consultation is **HIPAA compliant** in USA. The platform is also **GDPR Ready** for EU.

Curofic is integrated with a larger secure EMR platform, **Clinicea**. Security measures at place in Clinicea can be found here.

For questions please reach us at support@clinicea.com.