Accelerating
the digital transformation
of the Health sector in the Américas

ALL-IN-ONE

Telehealth platform primary health care with a focus on non-communicable diseases

Basic security and connectivity requirements

PAHO
Pan American Health Organization
World Health Organization
Americas Region

ALL-IN-ONE

Telehealth platform for primary health care with a focus on non-communicable diseases

Basic security and connectivity requirements

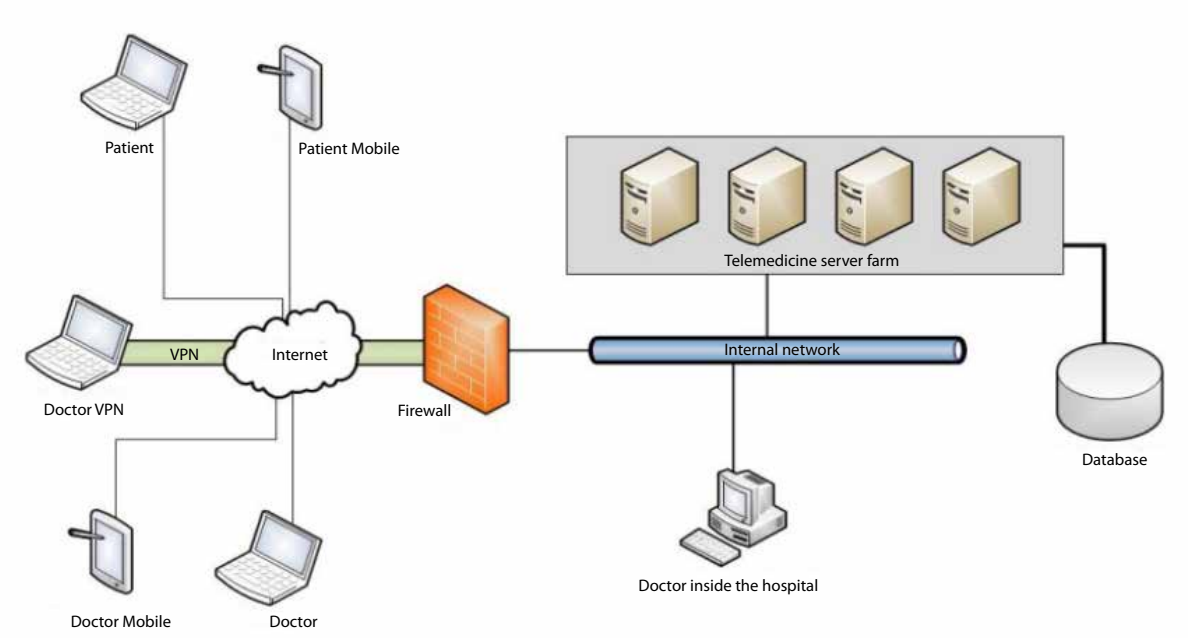
PAHO Pan American Health Organization World Health Organization Americas Region

Contents

Basic security and connectivity requirements

The telehealth is based on the concept of service, so it is necessary to take into account both: the quality of the service and the security of the data, offering the best performance and placing special focus on the security of the infrastructure.

Image 1. Overview of telemedicine



Different use cases must be considered so that telehealth is a flexible service, that is, there are no physical locations, but people can have their virtual consultation from anywhere, including doctors, who no longer need to be in an office within the hospital.

In the general telehealth scheme, all connections from the Internet (unsafe zone) must go through firewalls and the connection is analyzed at all times, thus avoiding the exploitation of vulnerabilities in the platform.

Analyzing the complexity of this type of service, it is evident that most of the connections come from the unsafe zone (internet) because this service breaks with the paradigm that the doctor must be within a hospital (and therefore in its secure network), locating both doctor and patient anywhere in the world.

To achieve a correct balance between security and performance, it is recommended to install a server that works simultaneously within the network to ensure high availability, and a firewall scheme in charge of analyzing incoming and outgoing connections, configured with strict security profiles according to the application published on the Internet.

It analyzes the application in search of vulnerabilities or attacks, blocking any attempt at intrusion or exploitation of vulnerability.

In all cases, connections from the Internet are treated as insecure without exception, even those in which a doctor may be connected via VPN, because we cannot determine the security level of the devices (level of operating system updates, security patches, antivirus, etc.).

Within the LAN, a doctor can perform teleconsultations from the desktop PCs that exist in the offices. Here, security is complemented by updated operating systems, up-to-date security patches, antivirus support, a scheduled update scheme, and policies for using both the PC and the Internet.

There is also the possibility that a patient who is in the hospital may perform teleconsultations (e.g. a visit from an inpatient who has a scheduled consultation), due to a guest Wi-Fi system, which, by not having contact with the LAN, can treat the patient's device in the same way as in the cases described above.

A typical data volume is on average 680 Gbit of daily traffic taking the service period from 08:00 am to 20:00 pm, with an average traffic of more than 15 Mbit/s dedicated only to this service.

It is recommended that the Internet links be redundant and contingent, as well as the Firewalls and the internal infrastructure, in order to minimize downtime, even in the case of software, firmware, etc.

Privacy Policy

It is recommended that the Internet links be redundant and contingent, as well as the Firewalls and the internal infrastructure, in order to minimize downtime, even in the case of software, firmware, etc.

OpenEMR

It is an open-source electronic medical record and medical practice management software. OpenEMR's privacy policy highlights its commitment to privacy protection and compliance with privacy regulations such as HIPAA. It focuses on the security of patient information and describes how data is handled within the system. It is licensed under CC 3.0 BY1. For a detailed evaluation of privacy and HIPAA compliance.

Jitsi (meet.jit.si)

is an open-source video conferencing solution. The meet.jit.si privacy policy, last updated on August 21, 2023, describes how 8x8, Inc., the main contributor to the Jitsi.org video conferencing solution, processes personal information to provide the meet.jit.si service. This policy covers what personal information is processed and why, how this information is used, and how to contact 8x8's data protection officer. It also ensures that they are not in the business of selling personal information to third parties and that they use the information to deliver and improve the meet.jit.si service.

Security and Encryption

About encryption and security points each of the software includes the following features:

OpenEMR provides several security measures to protect patient data and comply with regulations such as HIPAA. Some of the security features include:

- **Document Encryption:** OpenEMR uses the PHP mcrypt library for document encryption and decryption.
- **Strong Passwords:** Using strong and unique passwords as well as password expiration is recommended.
- **Multi-factor authentication:** For an added layer of security.
- **Network and server settings:** It is suggested to only open port 443 (https) and consider a firewall that only allows traffic through this port.
- **Apache hardening:** It is recommended to only allow https and disable direct access to certain directories.

Jitsi Meet is a video conferencing solution that also focuses on the security and privacy of its users. Security features include:

- **End-to-end encryption (E2EE):** Jitsi Meet offers E2EE as an added layer of security over always-present transport encryption3.
- **Ephemeral rooms:** Meeting rooms only exist while the meeting is active, meaning there is no connection to previous meetings that may have had the same name.
- **Room Name Generator:** To prevent unwanted access, randomly generated room names are used that are difficult to guess.
- **Browser Support:** End-to-end encryption is available in certain browsers, but not all.

PAHO
Pan American Health Organization
World Health Organization
Americas Region

www.paho.org