CPMS GETTING STARTED GUIDE FOR "HOSPITALS"

OpenApp Consulting Ltd

CPMS Technical Requirements

May 2019

Author: OpenApp - System Administration

Document Revision

Revision	Modifications	Date
ver.7	Update the Recommended browsers	22/02/19
ver.8	Section 5 updated with whitelist & bandwidth information	07/05/19
Ver.9	Rule change in section 5.3	10/05/2019

Glossary

CPMS	Clinical Patient Management System
ERN	European Reference Networks
HCP	Health Care Provider (i.e Hospital, Care Institution)
HTTPS	Hyper Text Transfer Protocol Secured
WebRTC	Web browsers with Real-Time Communications
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
FTP	File Transfer Protocol
IHE	Integrating the Healthcare Enterprise

1   Introduction

Clinical Patient Management System known as CPMS is a secure web-based collaboration platform to support European Reference Networks in the diagnosis and treatment of rare or low prevalence complex diseases. The CPMS empowers experts and specialists to take part in multi-disciplinary cross-border virtual consultations.

This guide provides technical requirements to connect CPMS users to CPMS software services.

2   Overview

This document is intended for IT departments in hospitals participating in European Reference Networks for Rare Diseases. This is to provide the minimum technical requirements to facilitate using CPMS by health professionals working at your organization. More details about Web protocols used are provided in this document.

3   Access to CPMS

In order to allow health professionals benefit from CPMS, they should be able to access the URLs given below with their hospital networks via web browsers:

1. CPMS Live: https://cpms.ern-net.eu
2. CPMS Training: https://cpms-training.ern-net.eu

4   Recommended Browsers

The application can be accessed through web-browsers. For best experience, make sure you are using a supported browser. CPMS is supported to its full potentials on Google Chrome and Mozilla Firefox preferably latest version.

Please note that users on unsupported browsers, will **NOT** be able to benefit from the video conference facility in CPMS.

Note:
- Cameras and microphones have to be enabled for access through the browser.
- Users should **NOT** use private browsing modes such as "incognito" on chrome whilst using the CPMS
- In browser settings, turn on: JavaScript To be modified or explained (procedure ➔ to activate JavaScript in each supported browser)

For Google Chrome as the most recommended browser, please follow the following steps:
- Click the Chrome menu More in the top right hand corner of your browser
- Select Settings
- Click Show advanced settings
- Under the "Privacy" section, click the Content settings button
- In the "Javascript" section, select "Allow all sites to run JavaScript

5 Video Conferencing Requirements

5.1 Hardware Requirements

The minimum required hardware is to have a device with camera and microphone to enable you participate actively in video meetings on CPMS. Below are other requirements that potentially can affect the uptake of CPMS to run smoothly within your organization. WebRTC video technology incorporated into the CPMS can be TESTED on your machine via this link:
https://cpms-training.ern-net.eu/video-testing

Please note that for sharing screen using older versions of Google Chrome, users may need to enable an extension to run on the browser.

5.2 Conflicting video applications

Please make sure that you are **NOT** using another video conferencing applications (e.g. Skype, GoToMeeting, Zoom, etc.) or similar video stream through another browser or a tab in the same browser (e.g. when recording a webinar). This may cause difficulty to switch on your camera and microphone in diffferent applications.

5.3 IP Whitelisting

Video facility services require connection to specific IP ranges and ports. The connection is always initiated from the corporate network/client so it is **NOT** possible for an external entity to send malicious traffic in the opposite direction. You will need to open the following on your corporate firewall:

Protocol	Ports	Direction	IP Range Destinations
TCP	443	Outbound	See list in section 5.3.1
UDP	1025 - 65535	Outbound	See list in section 5.3.1

Opening only the outbound TCP Port 443 will allow TURN servers to send media traffic via TCP as well as TCP/TLS.

Opening outbound UDP port range 1025-65535, will allow direct media transmission from client to media servers and back, as media servers accept one connection per port (and UDP port 3478 will allow TURN servers to send media traffic).

5.3.1 IP Whitelisting
The following IP ranges are used for the video conferencing services:

IP Network/Mask	
13.251.158.0/28	54.233.127.224/29
34.218.216.144/28	54.250.250.208/28
35.158.127.224/28	64.95.96.0/25
52.41.63.240/28	72.251.224.0/25
52.51.63.16/28	72.251.228.0/25
52.65.127.192/27	74.201.205.0/25

52.66.255.192/27	95.172.84.0/25
52.200.60.16/28	117.20.41.128/25
52.213.63.176/28	203.190.122.112/29
54.89.253.64/28	

5.4 Bandwidth Requirements

Video conferencing uses a variable amount of bandwidth, this variation may affect the quality displayed to the user. This may result in low quality or dropped video connections if the available bandwidth falls below a reasonable threshold. The user is informed of this as clearly as possible.

Video quality dynamically adjusts based on the strength of a user's network connectivity.

The following table provides bandwidth requirement per media:

Media Type	Acceptable	Excellent
Audio Only	Minimum dedicated **50 kbps** down per downloaded stream, as well as **50 kbps** uploaded stream to maintain a stable audio connection. For example, in a meeting with 5 participants, the minimum bandwidth should be around **250 kbps** per each participant.	Minimum dedicated **100 kbps** down per downloaded stream, as well as **100 kbps** uploaded stream to maintain a stable audio connection. For example, in a meeting with 5 participants, the minimum bandwidth should be around **500 kbps** per each participant.
Video + Audio	Minimum dedicated **350 kbps** down per downloaded stream, as well as **350 kbps** uploaded stream to maintain a stable video connection. For example, in a meeting with 5 participants, the minimum bandwidth should be around **2 mbps** per each participant.	Minimum dedicated **600 kbps** down per downloaded stream, as well as **600 kbps** uploaded stream to maintain a stable video connection. For example, in a meeting with 5 participants, the minimum bandwidth should be around **3 mbps** per each participant.
Screen Sharing	**1 mbps** on average as it depends on screen motion and number of participants	

6 Large File Upload Requirements

6.1 FTP batch upload

Using the FTP functionality may require higher technical competences that require prior experience. Please ask the IT department at your organization if you experience any difficulty in using the FTP client software.

IT departments can install FTP clients such as FileZilla and WinSCP for health professionals and administrators who might be involved in supporting CPMS operations in hospitals. FTP can be suitable in case of large file uploads exceeding 100 mb.

If health professionals do not have access to medical documents and materials of interest to upload, they may request IT personnel in their organization to upload specific documents to a particular panel.

All the instructions are provided in the pop-up modal to guide users to feed the right information into the FTP client software. Below is a definitive list of file formats that can be uploaded to the CPMS. Please pay attention that the format extensions are case sensitive.

PDF	pdf					
Excel	xml	csv	xls	xlsx	xlsm	
PowerPoint	ppt		pptx		pptm	
Word	doc		docx		docm	
Open Doc	odt	ods	odp	odc	odi	
Medical Images	dcm	jpg	jpeg	bmp	tiff	png
Video	avi	flv	wmv	mov	mp4	
Sound	pcm	wav	ogg	flac	mp3	

6.2 IHE option for integration

CPMS is capable of exchanging documents with other Health Information Systems using specific profiles. If your institution can participate in connecting to external IHE systems, then please contact CPMS support desk for further details SANTE-ERN-CPMS-ITSUPPORT@ec.europa.eu