Australian Government

Australian Digital Health Agency

USING ONLINE CONFERENCING TECHNOLOGIES SECURELY

A guide for

healthcare organisations

– 'Connected, secure consultations.'

This guide is intended to assist healthcare organisations assess their online conferencing technology solutions. The guidance is general and relates to Information Technology (IT) security. It is not intended to be comprehensive, and includes some of the benefits and implications of implementing online conferencing technologies. This guidance should not take the place of conducting other due diligence processes such as conducting risk assessments, obtaining legal advice and assessing the financial viability of vendors.

As healthcare organisations adopt online conferencing technologies at an increasing rate, these systems are becoming an essential component of healthcare service delivery. Used properly, online conferencing technologies can be a trusted and valuable tool. Conversely, insecure online conferencing technologies or practices can lead to loss of confidential data.

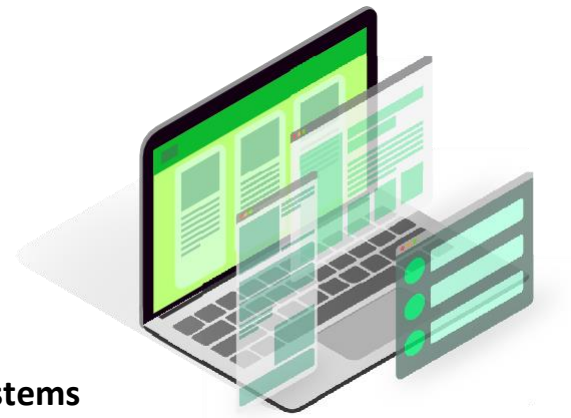
This guide has been developed by the Australian Digital Health Agency (the Agency) and CyberCX. The Agency promotes the use of safe and secure digital health services and systems to improve health outcomes. CyberCX is Australia's largest dedicated cyber security company, providing end-to-end cyber security services to Australian businesses and government.

1. Online conferencing technologies guide for healthcare organisations

The process of selecting an online conferencing technology platform will vary between healthcare organisations of different sizes. The following principles can help you identify a solution that meets your needs. Please also refer to advice from your local jurisdictions, as applicable.

- **Consider your existing systems**

  Your healthcare organisation may already have a suitable online conferencing platform. This may have been included as part of an existing software implementation, such as an enterprise productivity suite. If this system has been deployed and configured securely already, you can avoid many of the issues associated with configuring new software and integrating it with other systems.



- **Selecting new online conferencing technology systems**

  In selecting a new system, a good starting point would be reviewing the Agency's toolkit for selecting secure IT products and services. Please view the guide titled ***Selecting secure IT products and services*** at https://www.digitalhealth.gov.au/healthcare-providers/cyber-security.

- **A note on cloud solutions**

  Online conferencing technologies tend to be hosted in a cloud-based solution for scalability. A common misconception is that cloud-based solutions are inherently insecure as they rely on the use of hardware in external datacentres rather than on-premises. This is understandable but not correct; a properly configured cloud service can offer an acceptable degree of security, among other benefits. To learn more about cloud solutions, please view the guide titled ***Managing cloud-based services*** at https://www.digitalhealth.gov.au/healthcare-providers/cyber-security.

- **Securing your systems and software**

  Security vulnerabilities on your computer can undermine the security of your online conferencing solution, potentially leading to the exposure of confidential information. Maintain appropriate cyber security through activities like using the latest operating system version and installing updates as soon as they are available. For more information on securing your systems please refer to the briefing paper titled ***Patching for senior managers*** at https://www.digitalhealth.gov.au/healthcare-providers/cyber-security.

Before making any decision on an online conferencing solution, it is recommended you consider performing a risk assessment incorporating the topics below. Undertaking a risk assessment can provide you with an informed approach when selecting an online conferencing platform.

2. What to look for in an online conferencing technology platform

The following features can assist you in choosing a secure online conferencing technology platform. It's important to note that cloud solutions, such as video conferencing platforms, operate under a "shared responsibility model". That is, generally the service provider is responsible for security of the cloud, while the end user is responsible for security in the cloud.

The following features can assist you in choosing a secure online conferencing technology platform for your organisation. In addition, beyond the scope of this advice, you should also consider your functionality and compatibility requirements, as well as the clinical appropriateness of your chosen solution.

- **Secure configuration**

  Ideally, an online conferencing technology platform should offer a good level of security by default. This means, with minimal configuration requirements for end users. These types of applications help reduce the potential for error, and have fewer requirements for specialist technical knowledge.

  One should look at the configuration settings of your chosen solution and apply higher security settings as required. Consider having this performed by specialist IT providers where needed.

- **Well-implemented encryption**

  The primary mechanism for maintaining confidentiality is encryption. Some online conferencing technology services offer end-to-end encryption (E2E encryption), which means that data is encrypted on one side of the conversation and remains encrypted through each stage of the transmission process until it is decrypted by the recipient on the other side.

  For example, the message below would appear to the sender and recipient just as you see it in the plain text, while any system collecting the traffic between them would only see the encrypted ciphertext. In a properly configured system, it is essentially impossible to decrypt the ciphertext without having the correct decryption key.

Plain text: *Mary Smith presented with symptoms of influenza, including elevated temperature, joint pain, headaches and lethargy.*

Encrypted ciphertext: *CYa+bbrJSKFvQZXaJcLD5rkrX/6oMg7s7MYV80yPzP7jph2goRJLqz5SjgNEH31izcBUQooLdQtJltzTkW9f5l72SHP7/QaN6j1nfVQ7H9lalpbP8Jgv8tKHpBqo6LxGgr3lQ//W5rNz8uGQsvjTTcWtjVwabJWPLctCSsQ=*

However, a lack of E2E encryption does not necessarily make a service insecure. E2E encryption can be very demanding on online conferencing technology's resources, particularly when used for large group calls. To improve performance and functionality, online conferencing services may encrypt connections in segments, with some steps of the communication (typically within the online conferencing technology provider's servers) in plain text before being re-encrypted and sent onward.

While it is possible to design such systems to minimise the potential for exposure, a lack of E2E encryption makes it even more important to understand the way your data is being managed and stored by the software vendor. Reading the online conferencing solution's terms and conditions will assist in understanding how your data is handled.

Even in the absence of E2E encryption, the use of strong encryption standards is recommended, preferably NIST-approved algorithms and current IETF secure protocol standards.

To understand encryption in detail you can visit:
https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography/

- ## Access control and Multi-Factor Authentication (MFA)

Another key requirement for a secure online conferencing technology platform is having control over who has access to the online conferencing system, its configuration settings, and any confidential data it may store. This is especially important for cloud-based online conferencing platforms as their login pages are often available to anyone on the internet to try to gain access.

Access to system components and functionality should be assigned based on giving users the minimal access they require to perform their role. Organisations with an IT team, for example, may allow their system administrators to have access to configuration settings, while online conference participants only have access to the functionality required to perform consultations.

Effective access control also relies on making sure that users are authenticated securely. Using Multi-Factor Authentication (MFA) provides a far higher level of assurance compared to simply using a username and password or passphrase.

MFA adds another form of identification, known as a "factor", to the authentication process.

MFA consists of **two or more** of the following factors:

- ✓ Something you **know** – such as your password or passphrase
- ✓ Something you **have** – such as a code from a token or mobile app
- ✓ Something you **are** – such as your fingerprint or a facial scan.

A good platform should have this option and MFA should be enabled wherever possible to ensure a higher level of security and assurance.

- **Ability to identify participants**

  A good practice for healthcare consultations is to enable the identification and verification of all participants prior to commencing. While obvious in the context of an in-person consultation, the presence of unidentified or unwanted parties can be less apparent when using online conferencing technologies.

  To reduce the likelihood of breaches arising from uninvited attendees, the online conferencing technology solution should limit access to only those who are invited to join the meeting - and it should also be easy to see who is participating in the conference at any given time.

3. Privacy practices and policies that support confidentiality

Many applications, including online conferencing technology platforms, need to collect certain types of data and metadata in order to function. Some software providers choose to collect data as a source of additional revenue. Information sharing arrangements should be clearly identified in the privacy policy of the online conferencing provider. As it is difficult to determine how data may be used or stored once sent to third parties, the more secure option is to avoid online conferencing technology solutions that engage in such practices.

- **Hosting in countries with compatible privacy laws**

  Some countries have laws which are not consistent with Australian privacy laws. If your data is stored in or transmitted through another country, it will be subject to the laws of that country.

  In some cases, data offshore may be subject to lawful and covert data collection requests. For example, a conversation between a healthcare provider and a healthcare recipient in Australia may be accessed in its entirety if the platform does not use end-to-end encryption and any data transits through a country where such a request can be made.

  Take the time to review whether the online conferencing platforms retains all data within Australia, as this will help offset risks associated with data stored or transmitted offshore. Storing data in Australia will provide consistency of legal protections and will help Australian authorities assist you if necessary.

In all cases, Australian healthcare organisations are required to ensure Australian privacy laws are adhered to. This can be more challenging if data is stored in another country, particularly where the country has fewer legal protections in place.

Consult the Office of the Australian Information Commissioner's (OAIC) guidelines to understand your obligations and interpreting the Privacy Act. The OAIC guide to health privacy can be found here: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/

The OAIC guide to securing your personal information can be found here: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/

Further information is available from the Department of Health's "Privacy Checklist for Telehealth Services". This provides a summary of key steps to enable confidentiality of personal and health information while conducting telehealth consultations. It can be found here: http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/Content/Factsheet-TelehealthPrivChecklist

- **Ability to comply with Australian privacy requirements**

  Overall, it is important to consider how well the platform will enable your organisation to protect sensitive information and comply with its legislative and professional requirements. Review the online conferencing provider's privacy policy, terms and conditions, and other contractual arrangements to determine how these align to the requirements and risks that apply to your organisation.

  In addition, you will need to check what happens to your data when you discontinue using the online conferencing platform. It is important to ensure that:

  - transferability provisions are in place for your data to make sure you receive a full copy of your data on contract termination
  - all copies of your data are deleted (to comply with data retention and disposal requirements).

  If the online conferencing platform will be holding significant amounts of personal healthcare information on behalf of your organisation, you should seek legal advice.

4. Technical assessment of online conferencing providers platforms

In November 2020, the United States' National Security Agency (NSA) updated guidance regarding several commonly used online conferencing solutions. While it is important that each organisation undertakes its own assessment of the technology solutions it uses, Australian healthcare organisations may find the NSA's assessment a helpful starting point.

It is important to note this advice has been provided to US teleworkers, and in this context the

table illustrates the crucial security control areas which are important considerations when selecting an online conferencing platform.

If your jurisdiction has provided specific advice regarding secure online conferencing solutions, the information provided in this table is to be viewed as supplementary information only.

Table 1: National Security Agency (NSA) assessments of online conferencing technologies

Service	E2E Encryption	Testable Encryption	MFA	Invitation Controls	Minimal 3rd Party Sharing	Certified Service (FedRAMP)
Amazon Chime™	✗	✓	✓	✓	✗	✗
Cisco Webex®	Configurable	✓	Configurable, Paid version only	Configurable	✓	✓
Google G Suite™	✗	✓	Configurable	Configurable	✓	✓
GoToMeeting®	Configurable	✓	✗	Configurable	✓	✗
Jitsi Meet®	Partial	✓	✗	✓	✗	✗
Mattermost™	✗	✓	Paid version only	✓	✗	✓
Microsoft Teams®	✗	✓	✓	✓	✓	✓
Signal®	✓	✓	✓	✓	✓	✗
Skype for Business™	Partial	Partial	✓	✓	✗	✗
Slack®	✗	✓	✓	✓	Configurable	✓
WhatsApp®	✓	✓	✓	✓	✓	✗
Wickr®	✓	✓	✓	✓	✓	✗
Zoom®	Configurable, Partial	✓	Configurable	✓	✓	✓

* FedRAMP is the United States' Federal Risk and Authorization Management Program, that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services (ref: https://www.fedramp.gov/about).

Table 2: CyberCX assessments of additional online conferencing platforms utilised by healthcare organisations

Service	E2E Encryption	Testable Encryption	MFA	Invitation Controls	Minimal 3rd Party Sharing	Certified Service (FedRAMP)
FaceTime®	✓	✓	Configurable	✓	✗[1]	✗
Facebook Messenger™	✗	✗[2]	Configurable	✓	✗[1,2]	✗
Instagram Messenger™	✗	✗[2]	Configurable	✓	✗[1]	✗
Telegram®	✗	✓	Configurable	✓	✓	✗

[1] While collaboration services must often collect certain basic information needed to operate, they should protect sensitive data such as contact details and content. Collaboration information and conversations should not be shared with third parties. This could include metadata associated with user identities, device information, collaboration session history, or various other information that may put your organization at risk. Information sharing should be spelled out clearly in the privacy policy – NSA.
[2] No Published Details

5. Practising secure online conferencing consultations

In addition to selecting and configuring a secure platform, you will need to consider your computer hardware, your environment and your procedures for setting up secure online meetings.

- **Setting up the consultation**

  The booking process that a healthcare organisation uses to set up a telehealth consultation can also support the security of the meeting. Some of the processes that are already in place for booking and conducting face-to-face consultations can be adapted, such as identifying the healthcare recipient by validating full name, date of birth and address.

  It is important to consider the most secure way to share the link to the consultation. Sending the link via email and code to log in to the consultation by different channels will make it far harder for someone to gain unauthorised access to the call. For example, you may consider using email to send the link and providing the code over SMS or phone call when booking the appointment.

  Preparing healthcare recipients and carers for their telehealth consultation will assist in conducting a beneficial meeting. Further information regarding consultations from your recipient's or carer's perspective is available at the Digital Health CRC Telehealth Hub https://digitalhealthcrc.com/telehealth/.

- **Selecting a suitable consultation space**

  You will require a space that allows for privacy. Consider whether conversation, including audio from your computer as well as your own voice, could be heard by others outside of the consultation space. Also be aware of your screen's location and orientation to avoid others seeing sensitive personal information.

  If working from home or in other shared spaces, put systems in place (such as a "do not disturb" sign) to prevent interruption during consultations. Once you are online, some online conferencing technologies have the option to blur the background or load a background image that protects your privacy and the risk of inadvertently sharing confidential information that may be in the background. For example, information on a whiteboard, or other people's healthcare records.

- **Managing attendees**

  Just as you would in a face-to-face context, confirm your healthcare recipient's identity before the consultation commences. Details of how to join the meeting should be treated as if they are as sensitive as the meeting itself. Many platforms include a lobby functionality to allow the host to review attendees before admitting them.

- **Conducting consultations**

  When commencing the consultation, explain the format of the meeting, for example whether the contents of the meeting are to be recorded, and address any concerns before starting the consultation. This extends to the sharing of screen content for your meeting. Only share the information that is required for that meeting. If your desktop includes other sensitive work documents, it is a good practice to share an individual application instead of the entire desktop. It may help to exit all other applications prior to your meeting.

  Finalising your consultation - once your meeting has concluded, remember to leave the meeting and close down any associated meeting material, in preparation for your next consultation.

6. For additional information

1. Australian Cyber Security Centre, Web Conferencing Security (https://www.cyber.gov.au/acsc/view-all-content/publications/web-conferencing-security)
2. Australian Digital Health Agency, Cyber Security Centre (https://www.digitalhealth.gov.au/healthcare-providers/cyber-security)
3. Department of Health, Privacy checklist for telehealth services - fact sheet (http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/Content/Factsheet-TelehealthPrivChecklist)
4. Department of Industry, Science, Energy and Resources, Business Co-operative Research Centres Program – Digital Health Co-operative Research Centre Telehealth Hub (https://digitalhealthcrc.com/telehealth/)
5. National Cyber Security Centre, Video conferencing services: security guidance for organisations (https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations)
6. National Institute of Standards and Technology, National Cybersecurity Centre of Excellence, Cybersecurity for the Healthcare Sector – Securing Telehealth remote patient monitoring ecosystem (https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf)
7. National Security Agency Central Security Service, Selecting and Safely Using Collaboration services for Telework (https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/Collaboration_Services_UOO13459820_Full.PDF)
8. Royal Australian College of General Practitioners, Telehealth video consultations guide (https://www.racgp.org.au/running-a-practice/technology/clinical-technology/telehealth/telehealth-video-consultations-guide/introduction)
9. Royal Australian College of General Practitioners, Telephone and video consultations in general practice flow chart (https://www.racgp.org.au/FSDEDEV/media/documents/Clinical%20Resources/Guidelines/Telephone-and-video-consultations-in-general-practice-Flowcharts.pdf)
10. Royal Australian College of Physicians, Telehealth guidelines and practical tips for physicians (http://www.racptelehealth.com.au/guidelines/)

7. A secure telehealth checklist

USING ONLINE CONFERENCING TECHNOLOGIES SECURELY

A secure telehealth checklist for healthcare providers

Set up your digital consultation room

- Close doors and windows if required
- Set up a “do not disturb” sign to avoid interruption
- Check for confidential information, such as healthcare data that may be visible

When starting an appointment

- Check for unauthorised participants on the call
- Confirm each person’s identity
- Request a phone number to call if the connection drops

Maintain a secure system

- Use reputable and secure online conferencing technologies
- Keep your operating system and software up to date
- Where possible, use different computers for work and general browsing
- Keep up to date and secure backups

For more information:

Digital Health Cyber Security Centre:
https://www.digitalhealth.gov.au/healthcare-providers/cyber-security
CyberCX:
www.cybercx.com.au

Disclaimer
The creators of this guide are Australian Digital Health Agency and CyberCX Pty Ltd.

This guide is of a general nature and should not be regarded as professional advice or relied on for assistance in any particular circumstance. Readers should seek appropriate independent professional advice in relation to their situation.

No representations are given about the accuracy, completeness or suitability of this guide. The creators do not accept any responsibility or liability for any damage, loss or expense incurred as result of any reliance on information contained in this guide.

Second Edition

ISBN.....978-0-9876434-6-9 (print)
ISBN..... 978-0-9876434-7-6 (online)

The attribution for this guide is:

Australian Digital Health Agency and CyberCX Pty Ltd, Using Online Conferencing Technologies Securely. A guide for healthcare organisations, v2.0, 2021, available at http://www.digitalhealth.gov.au

Copyright © 2021 Australian Digital Health Agency

The material in this guide is licensed under a Creative Commons Attribution ¬4.0 International (CC BY 4.0) licence, with the exception of:

- the Australian Digital Health Agency logo which is subject to the Guidelines for Using the Commonwealth Coat of Arms at https://www.pmc.gov.au/government/commonwealth-coat-arms,
- the CyberCX logos and trade marks, and
- any third party material, any material protected by a trademark, and any images and/or photographs.

The Creative Commons legal code is at https://creativecommons.org/licenses/by/4.0/legalcode.

Enquiries about this licence and any other use of this guide can be sent to:

Australian Digital Health Agency
Scarborough House
Level 7, 1 Atlantic Street
Woden ACT 2606

Email: help@digitalhealth.gov.au
Phone: 1300 901 001

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au