Video-Conferencing & Privacy: how to choose a VC solution for your Practice

Are you new to video-conferencing (VC) or looking to expand the use of VC to deliver more Medicare telehealth consultations? A VC consultation is part of the patient record and subject to all the privacy, Medicare, continuity of care, and other record keeping requirements of any consultation.

This checklist outlines some of the data privacy matters that you should consider when selecting, or expanding, a VC solution for your practice.

Essential Minimum Steps (The 'Must Do' List)

CHECKLIST *Consider each of the following …*	**YES**	**NO**	**ACTION** *Suggestions for managing risks & meeting privacy requirements*
Know what you want (and need) from a VC solution. • A bit of planning will help you choose the best VC option for you, your practice and your patients. • Think about the kinds of features that are important to you, in order to deliver a smooth telehealth consultation. ***Tip**: Trial or select a VC solution that has features (default or customised settings) that help you to comply with your obligations under Australian privacy law.* *Features that pose a privacy compliance risk, or have a negative impact on data privacy (real or perceived) will require some effort/ intervention to mitigate the risk.*			There's no substitute for doing some sensible and practical 'due diligence'. You (or a trusted adviser) should: • Consider & review the suitability of the features of the proposed VC solution (see our suggestions below); • Review the product's terms & conditions (T&Cs) of use; and • Review the product's or supplier's Privacy Policy.
Do your due diligence (see above). • Here are some of the issues, features and functionality that you should think about.			
Who 'hosts' & manages the VC session? • Can anyone initiate and/ or join the VC call? • Can you control who initiates and/or joins a VC call as the 'host'?? • Can meetings/ consultations be 'locked-down' by the 'host'?			• Consider related features such as a virtual 'waiting room' or 'lobby' that helps you to manage back-to-back VC consultations & lock down VC sessions to the right participants. • Make sure the feature limits attendees to *invited* participants and successfully blocks invited participants from *automatically joining* a VC session, based on the scheduled meeting/consultation start time. • VC sessions should always be 'locked-down' or operate on an 'invite-only' basis. • Consider whether usernames will be publicly visible, or only visible to invited meeting participants. ***Tip**: Only practitioners should 'host' VC meetings for the purposes of performing telehealth consultations.* *Practitioners should be the ones to initiate the call and permit participants to 'join' the call.*
Does the VC solution have file sharing or screen sharing capabilities?			• Disable file sharing & screen sharing, at least to begin with.

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Suggestions for managing risks & meeting privacy requirements*
• Do you know how to restrict access to intended recipients, and prevent unauthorised access, use, copying or distribution?			***Tip**: Unless you are a seasoned VC user or recently completed an online tutorial etc. for the VC product and confident with the settings, we recommend that you disable this feature.*
Does the VC solution provide end-to-end encryption? • Is encryption a default/ standard setting? • Is encryption available as an upgrade/ licensed version of the VC product? • If file-sharing is important to you, is that part of an encrypted transmission?			• A product that has encryption will help you to demonstrate that you've taken reasonable steps to keep personal information secure.
What records are generated in connection with the VC session? • Do the records relate to the *manner* in which the VC service was utilised, and can individual users be identified from those record? • Do the records include the *content* of the VC? If yes, are those records automatically generated or an optional extra? • If records are automatically generated (and the feature cannot be disabled) can you easily access those records? • How long will the records be kept? Can the retention period be modified/ customised? • Are there costs associated with accessing the record?			• Carefully consider the types of records generated and ask yourself, are those records necessary? Do they provide value to your practice? • Records generated from a telehealth consultation are part of the medical record of the patient and subject to the same recordkeeping requirements. • Some products generate records such as: ○ Details about who was invited to a call, the device(s) used and network information; and ○ Transcripts of the VC call. ***Tip**: Are these records necessary, or of value, to your practice? Think about the medico-legal implications of having those records.* ***Tip**: If your VC solution has the capacity to generate a transcript, consider flagging this in your privacy policy. It's not the kind of collection and record of personal information that patients might reasonably expect.*
Does the VC solution permit audio/ video recording? • Can that capability be easily enabled/ disabled, and if so, by whom?			• Generating an audio or video recording of a telehealth consultation raises a number of additional issues: ○ Consent of the participants & transparency through privacy policies and notices; ○ Retention period for the recording; ○ Secure storage of the recording; and ○ Accessibility of the record. ***Tip**: Obtain legal advice before using this function.*
How do patients join the VC session? • Are participants issued with a single-use secure link, password or PIN to join the VC?			• Think about your workflow, consultation booking procedure, confirming patient identity and preferred device for conducting telehealth consultations. Is one option better suited to your practice?
Have you reviewed *your own* privacy policy lately? • Does it adequately cover the management of personal information in the context of telehealth consultations?			• Consider reviewing/ updating your privacy policy to ensure it reflects the collection, use, management and disclosure of personal information (especially sensitive health information) in connection with the provision of telehealth consultations.

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Suggestions for managing risks & meeting privacy requirements*
			• The policy should address the extent to which data might be handled differently in a telehealth context compared to a face-to-face consultation. • Ensure that your privacy policy is accessible and available, free of charge.
Will data be sent or stored off shore? • Will the introduction/ expansion of telehealth services via VC mean that personal information is routed or stored overseas?			Identify and consider: • The extent to which the VC solution involves off shore data movements or off shore data storage; and • Whether cloud-based solutions are supported locally or overseas? As a secondary step, consider whether your workflow practices or privacy policy needs to specifically deal with off shore data movements.
Do you need additional equipment? • Will you need a webcam, microphone or headset to use the VC platform or product?			• Does the platform/ service provider recommend any equipment to enhance the user experience? • Consider whether the success or performance of certain features will require additional equipment. • What are the minimum equipment requirements from *the patient side* of the consultation? ***Tip**: Remember, Medicare telehealth items require a visual and audio connection for VC consultations, for the entirety of the service. How good is your kit? What about the patient?*
Is your hardware and software up-to-date? • Does your computer, mobile or tablet have the latest software/ operating systems? • Is your kit up to the task?			• Update/ upgrade your kit as and when required. • Consider enabling notifications or routine checking alerts so you know when new updates are available. • Keep antivirus software up-to-date & operational at all times. Antivirus software should also scan incoming files. • Make sure smart devices regularly receive the latest security updates and patches. ***Tip**: Doing these things will help you meet your obligation to take reasonable steps to protect personal information from loss, unauthorised access or disclosure. Privacy requirements include keeping data secure.*
Where will the telehealth consultation take place? • Do you have a suitable physical location from which to conduct telehealth consultations?			If working remotely, and delivering telehealth services from home, choose a location that ensures the privacy & confidentiality of the consultation.
What role might staff play in terms of planning/ preparation for telehealth consultations? • Will staff (e.g. practice nurses, receptionists or practice managers) assist you to triage patients and screen patient suitability to participate in a telehealth service?			• Are work/ office areas suitable for staff to have conversations for the purposes of screening patients in order to ascertain: ○ Patients' willingness/ capability to participate in a telehealth service (e.g. available technology, familiarity with platforms); and

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Suggestions for managing risks & meeting privacy requirements*
			○ Potential suitability for a telehealth consultation, having regard to the nature of the patient's request/ medical issue. ***Tip**: Whether a service can, and should, be delivered as a telehealth consultation is ultimately a decision for the practitioner. But, if the practitioner is supported by staff in terms of offering telehealth consultations & preparing patients for that channel of communication, it would be prudent to document the practitioner's expectations in terms of appointments made for telehealth consultations.*
How is your connectivity and network coverage? • Are telehealth (VC) services a practical option for you and your patients?			• Is connectivity, coverage, data or speed already a challenge? • Consider the extent to which you might need to upgrade, or select VC solutions, based on available infrastructure and hardware.
How good is your password hygiene?			It's important to choose a secure password to manage your VC account access & operation. • Use a strong, unique password & change it regularly. • Don't use the same passwords across multiple products/ portals. • Don't share your VC password with staff. • Look for VC solutions that permit a team/ nominated group to perform certain administrative tasks. This will allow each user to have their own password.

Weigh the risks & benefits (The 'be careful' list)

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Some suggestions for managing risks & meeting privacy requirements*
Here are some additional features and functionality that may warrant some risk mitigation steps, expectation management and transparency in terms of privacy practices.			
File sharing			• Consider whether file-sharing functionality will deliver tangible or measurable benefits for you, your practice and/ or patients. • Consider whether encrypted or password protected files sent to patients via email (or direct to third parties such as pharmacists or specialists) is a more appropriate option, in the short term, having regard to: ○ Privacy & security considerations; ○ VC participants' confidence/ familiarity with the platform. ***Tip**: Consider delaying the use of file-sharing functionality until you've satisfied yourself that VC (and your chosen VC solution) is a good fit.*

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Some suggestions for managing risks & meeting privacy requirements*
			***Tip**: Approach your telehealth consultations as a 'proof-of-concept' exercise if you are new to VC. In addition to meeting legal & regulatory requirements, focus on whether VC is providing a good 'user experience' for practitioner & patient. Start with the basics & scale up with additional features, over time.*
Will telehealth consultations be delivered across a range of devices? • Does the VC solution need to be used on desktop, mobile phone and/or tablet?			Does the choice of device materially impact: • Useability of the VC solution, for practitioners or for patients? • The features/ capabilities of the chosen VC solution? For example, are some features only available (or successful) on certain devices? • The risk mitigation & workflow processes that you may need to observe. For example: ○ Will telehealth consultations conducted by VC only be offered to patients who agree to use a certain product that you have reviewed, risk assessed and are comfortable using? ○ Can the patient use any device?
More on 'locking-down' your VC session • Is there a realistic chance that the VC session may be gate-crashed, tapped into or highjacked by another person?			Consider whether the VC platform: • Has a continuity feature, where a user (or third party) can make, pick up or join a call from another device using the same account; or • Is on a public domain where third parties can join a VC session without being invited. ***Tip**: Avoid conducting telehealth consultations in a public domain/ open environment.*
Notifications			• Does the VC platform automatically issue real-time notices to a user's contact list that will alert them to the user being online? • Does the VC platform allow a user's contacts to see who the user is talking to (i.e. practitioner and patient)? If yes: ○ Choose a user name wisely; and below) ○ Check whether users (practitioners & patients) can disable this feature? ***Tip**: Consider developing a notice or information sheet for patients participating in telehealth consultations.* *Depending on the VC solution(s) you use, it may be prudent to highlight these kinds of issues & suggest patients customise settings/ features in order to protect their privacy.*
Select & use a username wisely			Where will your VC username be visible, and to whom?

CHECKLIST *Consider each of the following …*	YES	NO	ACTION *Some suggestions for managing risks & meeting privacy requirements*
Permissions & Data Sharing • What permissions (access to information via your device) does the VC platform require?			• Review the T&Cs. • Does the VC platform/ service require permission to any of the following? ○ Contacts; ○ Location (GPS and network based). Does it share location with contacts? ○ Emails; ○ SMS, to verify your phone number and identity; or ○ Photos, Media & File. • Can users opt-out or modify those permissions/ settings? ***Tip**: Consider developing a notice or information sheet for patients participating in telehealth consultations.*

For further information, or to discuss whether your practice is a candidate for a privacy impact assessment in relation to the integration or expansion of VC to support the delivery of telehealth consultations, please contact us.

Louise Cantrill
Partner
T: +61 2 8289 5846
M: +61 417 454 299
E: lcantrill@millsoakley.com.au

Natalie Butler
Special Counsel
T: +61 2 6196 5223
E: nbutler@millsoakley.com.au

Alec Christie
Partner
T: +61 2 8035 7959
M: +61 439 557 768
E: achristie@millsoakley.com.au

Vince Sharma
Partner
T: +61 2 6196 5202
M: +61 419 802 870
E: vsharma@millsoakley.com.au

Teresa Nicoletti
Partner
T: +61 2 8035 7860
M: +61 431 075 182
E: tnicoletti@millsoakley.com.au