



## Telehealth vs. Non-Telehealth Tools

Privacy / Security / Legislation Considerations

### Telehealth Tools (Tools specifically designed for patient care)

- Designed-for-telehealth tools (Jane Video Visits, Clinicmaster Telehealth, Doxy.me, Zoom Healthcare, LiveCare, others) considers ease of use, access, medical features, privacy legislation for their jurisdiction, security and other medical considerations in their design.
- These solutions are more likely to have transparent architecture / privacy / security measures and some have independent reviews certificates (TrustArc or similar) for best-practice security and Canadian legislation.
- Some of these tools meet privacy legislation requirements in different ways - some by not storing any patient information at all, and some by handling the patient data they do store appropriately.
- Many have been evaluated for PIPEDA (Canada) and PHIPA (Ontario) compliance and from a computer / technical standpoint should give you and your patient a high degree of confidence. JaneApp is the first tool we have seen claiming local PIPA (BC) compliance.
- Some basic versions of designed-for-telehealth tools are not typically prohibitive in cost or usability. Many are free at this time. They can and should be considered by physiotherapists.
- You should be aware that funders (e.g. ICBC) may and do request that you use a formal telehealth tool designed for patient care.
- WorkSafeBC will require that your tool does not allow patient information storage across borders. Generally, only the formal telehealth tools ensure this.

### Non-Telehealth Tools

#### Consumer / Social Media Tools

- There are many also non-telehealth / social media type tools (FaceTime / Skype / Google Hangouts).
- We do know multiple physiotherapists have been using non-telehealth / social media tools for many years and we are unaware of privacy breaches. The actual risk for this appears to be low.
- In most cases, the servers for these tools are likely not in Canada, so they are still a concern if you are treating WorkSafeBC patients.
- The telehealth literature typically advises us not to use the non-telehealth / social media platforms for patient interaction. *It is not so much that they don't have some security measures (encryption), but how they handle data is generally not as transparent as telehealth platforms and security expectations in the context of healthcare.*

## Business Tools

- Business tools (Zoom (standard), GotoMeeting, Skype for Business) are also non-telehealth tools, but their security tends to be more robust than the social media tools.
- Generally, you can feel more secure about the business tools security than the social media tools.
- Data residency (does personal information cross borders?) is still a concern from WorkSafeBC perspective.

## Recommendations in Choosing a Tool:

- Choose a telehealth tool if you can – many are not prohibitive from either a cost or usability perspective.
  - The current need for rapid implementation may require that you use non-telehealth solutions in order to facilitate ease of use for you and your patients – access should trump what appear to be low privacy and security risks.
  - If you are using a non-telehealth solution (Skype, Facetime, etc.), you should advise your patient of this and obtain their consent to continue.
-