

TELEHEALTH CHECKLIST

7 Things to lookout for when choosing the right telehealth platform for you

Please note that this is not an exhaustive list and that it is, in our opinion, what one should look at as a start. There may be other factors to consider but these are what we believe to be primary considerations

Telehealth is the new buzz word. Whilst there has been some form of virtual consulting around for many years – think the last time you spoke to a patient on the telephone – today, telehealth has gone mainstream accelerated by advances in technology but also aggravated by worldwide economic lockdowns and quarantine. We have no need to remind you of that and just how it has changed the way we work in the now, and possibly, in the future.

Here are some tips to help you choose the right telehealth platform for you.

Does the telehealth platform meet the following requirements?

		YES	NO
1	<p>Data security - The first consideration has to be data security, and then the highest security that you can find. If you're in any doubt, simply don't use it. In our world, we look for PoPI and HIPPA (Health Insurance Portability and Accountability Act), compliance.</p> <p>To be fair, HIPPA is a piece of U.S regulation and we may not be subject to it, but this is about a genuine concern for patient data and avoiding litigation, rather than just complying with the law. Video and texting are only two of the many things that are vital to security in telehealth. Your patient's name, email address, phone number, address, and my other things, all fall under data that must be protected.</p> <p>Also consider who has access to the data. Before, we could store patient records in the backroom, we made very sure that access was strictly controlled, and you knew exactly who had access to your patient files. Can you say the same of your online storage today?</p> <ul style="list-style-type: none"> • MAP YOUR DATA: Know where your data is being held and if it is being stored in the cloud, you want to know where. • ASK and RECORD, who has access to the data, who should have access to the data and insist on seeing evidence of Business Partner agreements to ensure that all employees are kept at the same high standard as your solutions provider. • MONITOR all file access to your data. • SET UP ALERTS to notify you if anyone has access to your data. • ENSURE that the solution has encryption, server room security, and a two-factor authentication access. 	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<p>Public vs Private Chat Platforms – There are a host of online video and group chat platforms in the market at present. Nothing against Zoom, Google Hangouts, Microsoft Teams or WhatsApp or their counterparts, but in the healthcare environment, data security (as noted above), is paramount. The</p>		

	<p>overwhelming majority of these platforms were made for reasons other than telehealth and have therefore, been retrofitted to suit as opposed to a platform that has been specifically designed for healthcare practitioners on the go and operating in a modern world.</p> <p>Zoom, for example, has become the most popular business meeting software in use today. Its free version and ease-of-use has made it a quick choice for many practitioners, but the question remains as to its suitability for telehealth consultations. It's attractive as its' easy to use, has a waiting room, can screen share and has end-to-end encryption, so it should be fine, right?</p> <p>The answer is that the Zoom - free and paid versions - is NOT HIPPA compliant, and for this reason, they have recently introduced Zoom for Healthcare. You can expect to pay a starting rate of \$200 per month or about R3400 at today's rate, with a 12-month contract. You can't expect to get into a piece of software this advanced and compliant and remain on the platform for just a few weeks.</p> <p>Zoom was not originally developed for telehealth and therefore, it doesn't have the features that telehealth platforms have for online consultations or the storage of patient data. For this reason, Zoom was not originally created to be HIPPA compliant.</p> <p>There is a lot more to it than just end to end encryption. HIPPA was enacted to protect patients' privacy and ensure they have access to their medical records. PII (Personal Identifiable Information), is protected in terms of how that information is stored, transmitted and who has access to it. The same can be said of WhatsApp. It may be used for general information but really wasn't made for the transfer of sensitive clinical information.</p>	<input type="checkbox"/>	<input type="checkbox"/>
3	<p>Easy is not always safe - While checking for compliance is the first step, your choice of telehealth platform should also be about genuinely concerning yourself around the data confidentiality of patient data. Sometimes the easiest route is not the safest. Don't always look at which is the easiest to use, rather look at which will give both you and your patient the security and peace of mind to continue using telehealth.</p>	<input type="checkbox"/>	<input type="checkbox"/>
4	<p>Back-up support - How does your solution provider assist in introducing your patients to telehealth? There is nothing more frustrating than embracing a secure, robust and effective telehealth solution, but no one uses it. Explore what support you will get to assist your patients to start using your solution.</p>	<input type="checkbox"/>	<input type="checkbox"/>
5	<p>Realtime, no time, anytime? - Does the solution provide both synchronous as well as asynchrony telehealth? In other words, do both parties need to be available at the same time, or is it possible to provide care on an asynchronous basis?</p>	<input type="checkbox"/>	<input type="checkbox"/>
6	<p>Tracking and billing functionality - Is there a facility to appropriately be remunerated and how easy is this process? Not all healthcare services will necessitate remuneration, but where appropriate, you deserve to be remunerated for your time and expertise. If you're having to go back to a</p>		

	manual process to be reimbursed, you may not be taking advantage of all that technology has to offer – from timesaving to automatic calculation of the consultation duration.	<input type="checkbox"/>	<input type="checkbox"/>
7	Voice, Video and Text - Does the solution only provide for video, or is there an ability for secure texting and calling as well? Not every patient wants to video call, in fact, globally, more texts occur than video calls. If you only offer a video calling solution, you may find a reticence to embrace telehealth. Try to provide at least text and video...we can't assume that all patients will embrace video calls.	<input type="checkbox"/>	<input type="checkbox"/>

As lockdown eases, so some normalcy may appear, although it will be a long time for things to revert to 'normal', if indeed, that ever happens. Telehealth is here to stay. Make sure you choose wisely and take your time in assessing a solution that will fit into your practice and that will last well into the future.