



HPCSA BOOKLET 10:

THE HIDDEN LIABILITIES OF TELEHEALTH

KEY TAKE-AWAYS



WHY TELEHEALTH MATTERS

Many doctors **unknowingly practise telehealth** in their daily professional lives.

Under HPCSA Ethical Guidelines, telehealth covers the range of clinical interactions conducted via information and communication technology, including phone calls, WhatsApp, email, SMS and digital platforms. It encompasses consultations between healthcare practitioners and patients as well as between healthcare professionals where they seek advice, guidance or second opinions from colleagues in the care of their patients.

Recognised as a legitimate mode of practice by the Health Professions Council of South Africa (HPCSA), telehealth has become an integral component of modern healthcare delivery in South Africa. Other than providing an opportunity to improve access to care, particularly for remote and vulnerable patients, it can enhance continuity of treatment, system efficiency and collaboration between practitioners.

To be compliant as a healthcare practitioner when offering telehealth, the same ethical, professional and legal standards as for face-to-face consultations must be applied. Telehealth replicates—not dilutes—the standard of in-person care.

EthiQal, trading under Titan Risk Services (Pty) Ltd, an authorised financial services provider FSP 51361.

Disclaimer: This resource provides a simplified overview of HPCSA Booklet 10, related ethical guidelines, and South African laws. It aims to help healthcare practitioners understand key principles of telehealth but is not a substitute for the official HPCSA publications or legal advice. Practitioners should refer to the full guidelines and seek professional guidance when needed. EthiQal is not responsible for any loss arising from the use of this resource. Information is current as of November 2025. © 2025 EthiQal.

ETHIQAL
Your professional indemnity partner

WHAT YOU NEED TO KNOW

HPCSA Booklet 10 provides the primary ethical framework for telehealth in South Africa. Where it is silent or ambiguous, guidance must be drawn from existing health, medicines, consumer protection, electronic communications and data protection laws.

Important points to know:

- **Established Patient Relationship:** Other than in an emergency or other situation where telehealth may be in a patient's best interest, a practitioner should have an established relationship with the patient before providing telehealth.
- **Prohibition on Exclusive Practice:** No practitioner may exclusively render professional services through telehealth; physical consultations must remain part of the practice.
- **No lesser Ethical Principles:** The same core ethical principles as for in-person consultations apply.

Clinical appropriateness

- Telehealth **may not replace physical examination** when one is clinically necessary. When in doubt during a telehealth consultation, clinicians should escalate to face-to-face care. For example, where there is diagnostic uncertainty, red flags are present, records are unavailable, symptoms are evolving or severe, and/or no reasonable assessment is possible without a physical examination, doctors must insist on a face-to-face consultation.
- Images, questionnaires, or brief messages alone are **rarely sufficient** for diagnosis or prescribing. Adequate clinical information for a sound assessment must always be available.
- Quick, 'on the run' consults must be avoided to prevent unnecessary oversights in diagnosis and treatment.
- Clinical judgment must always override convenience, cost pressures, or technological optimism.

Informed consent

- This can be obtained in **writing or recorded orally**.
- It must include **identities** of the patient and all practitioners; **agreement** to the use of telehealth by the patient and that the practitioner determines whether telehealth is appropriate; identification of **material risks** to confidentiality arising from technology; and consent to **sharing of personal information**, which includes awareness of other persons present or able to access the information.
- **Hospital at Home Nuance:** For emerging "hospital at home" programs - programs that use telehealth and remote monitoring in the provision of home-based acute care as part of a complex contractual matrix that involves hospitals, home care companies, funders and device suppliers - participating practitioners must be satisfied that **all layers of consent** are covered, including the **mode of delivery of care, clinical risks, and data privacy**.



Confidentiality and privacy

- **Social Media Warnings:** Interacting via social media (e.g., WhatsApp, Facebook) is not advised as it is prone to accidental information disclosure to the wrong recipient and breaches of the **Protection of Personal Information Act (POPIA)**. It carries the additional risks of blurring doctor-patient relationship boundaries and creating unrealistic patient expectations in terms of availability.
- **Cybersecurity** should be a key focus for any practice offering telehealth. Data security is central to ethical telehealth practice.

Record-keeping

- Every clinical interaction forms part of the patient record, regardless of the method of engagement (eg. phone, WhatsApp) and should be recorded as such.
- Standard clinical record-keeping advice applies ([Click here](#)).
- **Not limited to Doctor-Patient consultations:** Phone and digital consultations between practitioners are also telehealth. The **consulting practitioner** (who offers remote advice and carries accountability for advice given) is held **to the same professional standards** as the **practitioner in charge** (who is with the patient and is responsible for final patient management and treatment decisions). Prior to identifiable information being shared, patients must consent to this; information exchange must be limited to clinically necessary information that is accurate; transmission of data must be secure, and **both parties** must keep **detailed records** of the advice provided, even for late-night calls.
- **Cross-Border Consultation Risks:** Cross-border consultations may require **registration** in both the **practitioner's and the patient's countries**. Practitioners should be aware that cross-border telehealth may expose them to parallel regulatory scrutiny - in South Africa, as well as in other jurisdictions.



TELEHEALTH CHECKLIST

- Know when conducting telehealth (phone calls, WhatsApp, email, SMS, digital platforms, including doctor-to-doctor advice).
- Confirm clinical appropriateness.
- Escalate to face-to-face care when necessary.
- Obtain explicit informed consent to remote care.
- Protect confidentiality.
- Secure devices and digital platforms.
- Ensure data is encrypted during transmission and stored securely.
- Maintain detailed patient records. This includes transcribing or storing all electronic communications like WhatsApp, emails, recordings, including source records.
- Use caution with social platforms (e.g. personal WhatsApp).
- Document doctor-to-doctor advice, no matter if consulting practitioner or practitioner in charge.
- Consider cross-border legal exposure, as regulatory obligations may apply in both the practitioner's and patient's jurisdictions.

SOME TIPS ON CYBERSECURITY

Devices used by clinicians are the **weakest link** - especially personal phones and laptops.

Using a VPN is good practice, but it does not eliminate endpoint vulnerabilities.

Practical safeguards include:

- Device encryption.
- Use of Password Managers and unique long passwords / passphrases.
- Use of multifactor authentication (e.g. separate pin sent to your cellphone when logging in).
- Automatic locking and remote wipe capability.
- Limited and controlled access, with no shared login details.
- Regular software updates.
- Antivirus protection (anti-malware and firewall).
- Secure backups.
- Vigilance against phishing. Trust in professional intuition - just as in clinical care, a sense that "something isn't right" often signals a real risk.
- Incident response. Know what to do if a device is lost or data compromised. Cyber insurance cover often includes incident response teams.
- Consulting a cybersecurity expert.

