Practice Guidelines for South African Telemedicine

Table of contents

Acknowledgements

The Digital Healthcare Association of South Africa (DHCA) wishes to express sincere appreciation to the Core Practice Guidelines Committee for its valuable contributions in the research and development of the following telemedicine guidelines.

Core Practice Guidelines Committee

Members:

Ronald Whelan, *MBBCh, MBA, Chief Commercial Officer, Discovery Health*
Unben Pillay, *MBChB, Chief Executive Officer, Alliance of South African Independent Practitioners Associations*
Neil Kinsley, *BALaw C.F.P. PTA, Managing Director, Medici*
Dirk Wagener, *MEng, GM Healthcare, StoneThree Healthcare*
Naim Rassool, *MSc(Eng) MBA, BD Healthcare, StoneThree Ventures*
Saul Kornik, *BBusSc(Hons Finance), BComm(Hons Accounting), PGDA, MComm, CFA, CA(SA), CEO, Healthforce*

Project Team:

Henru Krüger, *BProc. B.Compt CIA C.Prac, Chief Operating Officer, Alliance of South African Independent Practitioners Associations*
JW Kleynhans, *MBChB, Chief Medical Officer, Healthfor.life*
Dulaine Stander, *BPharm, Business Analyst, Healthfor.life*

Copyright statement:

Contact details:

The Chairman: Digital Healthcare Association
Office 201, Second Floor, The Club Shopping Centre
Cnr of Pinaster Avenue and 18th Street,
Hazelwood,
PRETORIA
0081
Email address: info@dhca.org.za

Preamble

Background

The Digital Healthcare Association of South Africa brings together a diverse group of industry participants who are passionate about the potential for telemedicine to significantly increase access to high quality and affordable healthcare for all South Africans. The aim of these Core Practice Guidelines for Telemedicine (hereinafter referred to as “the Guidelines”) is to advance telemedicine practices in South Africa in a responsible, professional, equitable and ethical manner.

Definition of Telemedicine

Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve patients' health status.
Closely associated with telemedicine is the term "telehealth," which is often used to encompass a broader definition of remote healthcare that does not always involve clinical services.

Examples of solutions considered part of telemedicine and telehealth:

- Videoconferencing,
- Transmission of still images
- e-health including patient portals
- Remote monitoring of vital signs
- Continuing medical education
- Nursing call centres are all considered part of telemedicine and telehealth.

Telemedicine is not a separate medical specialty. Products and services related to telemedicine are often part of a larger investment by health care organisations in either information technology or the delivery of clinical care. Telemedicine encompasses different types of programs and services provided for the patient. Each component involves different providers and consumers.

How the guidelines are helpful

The Guidelines seek to provide the following:

- Guidance to telemedicine technology and service providers on acceptable standards of best practice, quality benchmarks and main regulatory requirements
- Guidance to healthcare professionals around acceptable standards of practice and main regulatory requirements
- Guidance to funders, patients and end-users of what constitutes acceptable standards of practice and their rights relating to standards of care, quality of service and access to information

Resources used to develop the guidelines

The Guidelines have been developed by various stakeholders and professionals working in the healthcare industry in South Africa and globally.

The team also used the following international and local guidelines as a reference:

- Guidelines for good practice in the healthcare professions, General ethical guidelines for good practice in telemedicine, Health Professions Council of South Africa, April 2014
- Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions, American Telemedicine Association, May 2014
- National Telemedicine Guidelines, National Telemedicine Advisory Committee, Singapore, January 2015
- European Code of Practice for Telehealth Services, Telescope Project, 2014

Disclaimers

The technical and administrative guidelines in this document do not purport to establish binding legal standards for carrying out telemedicine interactions. The Guidelines must therefore be read and implemented in conjunction with all relevant legal and regulatory requirements including, but no limited to, the following:

- the Promotion of Access to Information Act 2 of 2000
- the Electronic Communications and Transactions Act 25 of 2002 (as amended)
- the Protection of Personal Information Act 4 of 2013
- the Consumer Protection Act 68 of 2008
- the Medical Schemes Act 131 of 1998 (as amended)
- the National Health Act 61 of 2003
- the Children's Act 38 of 2005
- the Choice on Termination of Pregnancy Act 92 of 1996
- Ethical Rules of Conduct for Practitioners Registered under the Health Professions Act, 1974 published as GNR 717, dated 4 August 2006 in the Government Gazette ("the Ethical Rules")
- Occupational Health and Safety Act (Act No. 85 of 1993)
- Medicines and Related Substances Control Act (Act No. 101 of 1965)
- Health Professions (Act No. 56 of 1974)
- HPCSA Policy Document on Business Practices as of 26 October 2016
- All applicable guidelines published in General Ethical Guidelines for the Health Care Professions as published by the Health Professions Council of South Africa ("the HPCSA guidelines").

Furthermore, although the Guidelines seek to be as comprehensive and specific as possible, all telemedicine practices and services must ensure the best interests of the patient are preserved and protected at all times.

Scope

Recognising the potential for telemedicine to significantly increase the access to high quality and affordable healthcare, South African telemedicine role players want to ensure that all telemedicine services are delivered in alignment with international best practice and South African and African regulations, business and operational environments.

Telemedicine is the means by which technologies and related services concerned with health and well-being are accessed by people or provided for them irrespective of their location. Simply put, the person accessing the service is not physically in the location of service provision. (See the glossary for an expanded list of terms and their definitions)

The WHO Classification of Digital Health Interventions[1] defines the following four categories of telemedicine services:

- Consultations between remote client and healthcare provider (2.4.1)
- Remote monitoring of client health or diagnostic data by a healthcare provider (2.4.2)
- Transmission of medical data to a healthcare provider (2.4.3)
- Consultations for case management between healthcare provider(s) (2.4.4)

For practical purposes these Guidelines are focused only on the domain of Telemedicine consultations where a patient is present i.e. 2.4.1 and 2.4.4:

- Direct patient to healthcare provider video consults (i.e., patient consults a healthcare provider directly via a secure video link)
- Multidisciplinary healthcare provider video consults (i.e., patient consults a healthcare provider in person at a particular physical location and then, in-turn, connects to a healthcare provider in another physical location via secure video link)

This version of the Guidelines excludes the following domains defined by the WHO:

- Remote monitoring of client health or diagnostic data by a healthcare provider (2.4.2)
- Transmission of medical data to a healthcare provider (2.4.3)

Examples of the excluded domains include the following:

- Activity and lifestyle monitoring
- Safeguarding and monitoring in care settings
- Gait, seizure and falls prediction/management
- Vital signs monitoring
- Telecare and social alarms (PERS)
- Chatbots and chat-based platforms

[1] World Health Organization Classification of Digital Health Interventions, https://apps.who.int

- Teleradiology
- Doctor to Patient telephone calls

Companies with technologies used in the delivery of the service will still require registration and compliance with the relevant compliance bodies e.g. South African Health Products Regulatory Authority, ISO13485:2016 Medical Devices QMS.

Structure of The Guidelines

The Guidelines are structured in four main sections:

A. *Planning:* Activities that need to be performed before commencing telemedicine service provision
B. *Service delivery:* Activities that need to be performed during the delivery of the telemedicine services
C. *Learning:* Monitoring and reporting activities that need to be performed during the delivery of the telemedicine service
D. *Risk and Quality Management:* Activities that need to be performed based on the results of monitoring to improve the quality of the telemedicine service

Although the guidelines should be read and implemented in full, each of the sections is divided into subsections that are relevant to the following role players:

1. *Organisations. i.e.,* institutions, corporate and business entities, group and solo practices;
2. *Healthcare Providers* i.e., individuals registered as healthcare professionals e.g. doctors, nurses, pharmacists
3. *Technology Providers* i.e., software and hardware companies and devices that enable the delivery of telemedicine.

The subsections contain guidance and best practice distilled from international sources and Guidelines in the beginning and are followed by a checklist of items to help role players self-assess their progress towards successful implementation of the Guidelines.

To help readers assess the level of compliance required, the following adjectives are used in the Guidelines:

- “must” (mandatory),
- “should” (strongly encouraged),
- “may” (truly optional).

1. Planning

1.1. Organisations

1.1.1. Compliance with the Practice Guidelines

1.1.1.1. Organisations must be internally reviewed on their relevant sections.

1.1.1.1.1. Internal reviews must be performed every year.

1.1.1.2. A copy of the Guidelines must be easily available to staff, users and patients and section on their website noting adherence to the guidelines.

1.1.2. Governance

1.1.2.1. Organizations must have policies and procedures in place to govern telemedicine services with regards to, the sections that are covered individually through the guidelines.

1.1.2.2. Organisations must clearly document roles and responsibilities that, within the organisation, clearly addresses who has management responsibility for the telemedicine service, data protection and healthcare provider compliance.

1.1.3. Procurement from Technology Providers

1.1.3.1. Organisations must confirm to the compliance of their suppliers and vendors to regulatory requirements specific to their products.

1.1.4. Installation, Programming of Technologies

1.1.4.1. Organisations must ensure that equipment and technologies utilised are appropriate for the service delivered taking into consideration:

1.1.4.1.1. Medical devices, where included, must be marked with their classification which, in the context of Telemedicine, will testify to their satisfying regulatory and licensing requirements of the country.

1.1.4.2. Organisations must ensure that the installation, programming, calibration, initial testing and demonstrating of technologies/equipment, are undertaken in accordance with manufacturer's or supplier's guidance.

1.1.4.3. Installation and related work must be undertaken by people who have the required skills, knowledge and expertise.

1.1.5. Staff Training and Development

1.1.5.1. Organisations should confirm and record that Healthcare providers and staff have had appropriate training and development programs.

1.1.5.2. Clinical training to ensure alignment with latest treatment protocols.

1.1.5.3. Operational training to ensure users know how to use the systems and devices appropriately.

1.1.6. Data Protection

1.1.6.1. Policies:

1.1.6.1.1. Organisations must maintain current policies and procedures for the management and protection of personal information.

1.1.6.1.2. Policies and procedures must ensure that the manner of storage, management and sharing of personal information normally carries the consent of users and patients.

1.1.6.2. Responsible parties:

1.1.6.2.1. Organisations should have an effective, up-to-date privacy Compliance management program in place in the event of a complaint investigation.

1.1.6.2.2. Front-line and management staff must be trained on privacy and information security principles.

1.1.6.3. Information officer:

1.1.6.3.1. Organisations should have an information officer that must ensure that a compliance framework is developed, implemented and monitored.

1.1.6.4. Information processing:

1.1.6.4.1. Contracts should be in place for the transfer of personal information to third parties for processing (operators)

1.1.7. Checklist

Organisations must:

Compliance with the Practice Guidelines

Organisations must perform internal review of compliance to their sections ☐
A copy of the practice guidelines must be easily available to staff, users and patients. ☐

Governance

Organizations must have policies and procedures in place to govern telemedicine services ☐
Organisations must have a clearly documented governance structure with documented roles and responsibilities ☐

Procurement from Technology Providers

Organisations must confirm the compliance of their suppliers and vendors to regulatory requirements. ☐

Installation, Programming of Technologies

Organisations must check that equipment and technologies are properly installed ☐

Staff Training and Development

Organisations should confirm and record that Healthcare providers and staff have had telemedicine training and development programs. ☐

Data Protection

Organisations must maintain current policies and procedures for the management and protection of personal information. ☐
Organisations should have an effective, up-to-date privacy compliance management program in place in the event of a complaint investigation. ☐
Front-line and management staff must be trained on privacy and information security principles. ☐
Organisations should have an information officer that must ensure that a compliance framework is developed, implemented and monitored. ☐
Contracts should be in place for the transfer of personal information to third parties for processing ☐

1.2. Healthcare providers

1.2.1. Compliance with the Practice Guidelines

1.2.1.1. A copy of the practice guidelines must be easily available to staff, users and patients.

1.2.1.2. The healthcare provider must add a section to their website noting adherence to the guidelines.

1.2.2. Conflicts of Interest

1.2.2.1. Healthcare providers must always act in the best interests of patients.[2]

1.2.2.2. Healthcare providers must avoid conflicts of interest when providing a service. Specifically:

1.2.2.2.1. Always seek to give priority to the investigation and treatment of patients solely on the basis of clinical need.

1.2.2.2.2. Recommend or refer patients for necessary investigations and treatment only and prescribe only treatment, drugs or appliances that serve the needs of patients.

1.2.2.2.3. Declare to patients verbally and by a displayed notice any financial interest they may have in institutions and diagnostic equipment.

1.2.3. Corporate ownership

1.2.3.1. Anybody that is not a registered healthcare practitioner does not qualify to directly or indirectly share in the profits or income of a professional practice, and which may take the form of [2]:

1.2.3.1.1. Transferring the income stream generated in respect of patients from the practice to such a person

1.2.3.1.2. Giving (directly or indirectly) shares or an interest similar to a share in the professional practice to such a person; or

1.2.3.1.3. Transferring income or profits of the professional practice to a service provider through payment of a fee which is not a market-related fee for the services rendered by the service provider.

1.2.3.1.4. Paying or providing a service provider with some or other benefit which is intended or has the effect of allowing the service provider or persons holding an interest in such a service provider to share, directly or indirectly, in the profits or income of such a professional practice or to have an interest in such a professional practice.

1.2.3.1.5. Direct or indirect corporate ownership of a professional practice by a person other than a registered healthcare practitioner in terms of the Act is not permissible.

[2] Health professions council of South Africa, guidelines for good practice in the health care professions, general ethical guidelines for the health care professions, Booklet 1, Pretoria, May 2008

1.2.3.2. Healthcare providers should follow the Health Professions Council guidance on preventing conflicts of interests, but as a rule, there should be a clear separation between the Organisation, the Healthcare provider and the Technical provider in line with the preceding clause.

1.2.4. Scope of practice

1.2.4.1. Healthcare providers must ensure that the service that is delivered is in line with their scope of practice as registered in the relevant regulation and they have the appropriate level of qualification, competence and experience for the service they are delivering.

1.2.4.2. A practitioner shall help or support only a person registered under the Pharmacy Act, the Nursing Act, the Social Service Professions Act, Dental Technicians Act, or the Allied Health Professions Act,

1.2.4.3. Where the healthcare provider or organisation deliver a service to a specific subset of patients e.g. mental health, the appropriate level of skill and qualification for that subgroup needs to form part of the service delivery team.

1.2.4.4. Interns and students may only perform such activities as is part of their structured training program

1.2.4.5. A nurse must be employed as a specialist nurse, unless the nurse holds the necessary qualification and is registered.

1.2.4.5.1. The scope of practice of nurses does not include the performance of occupational medical examinations required by the Occupational Health and Safety Act.

1.2.4.5.2. The Nursing Act contains no provisions for extending the scope of practice of nurses to include clinical assessment and diagnosis other than under the control of a medical practitioner

1.2.4.6 PCDT Pharmacists must adhere to the Primary Care Drug Therapy List aligned to the Standard Treatment Guidelines and Essential Medicines List as set out by the Department of Health Affordable Medicines Licensing Unit

1.2.5. Guideline training

1.2.5.1. Healthcare providers should have specific telemedicine training programs and development programs beyond what is provided by telemedicine organisations

1.2.5.2. Organisations and Healthcare providers should have specific training programs to ensure staff understand and can implement the Guidelines. This can be achieved through implementing the following practices:

1.2.5.2.1. Record of guideline training must be maintained

1.2.5.2.2. Staff who have never completed Guideline training should not commence telemedicine service provision.

1.2.5.2.3. Guideline specific training should be completed at least every two (2) years.

1.2.6. Asset Register

1.2.6.1. Healthcare providers must maintain an up to date and accurate registry of technologies/equipment that is used for stored data or supplied to users and patients including laptops and computers.

1.2.6.2. The registry should contain serial numbers, date of purchase, service calibration dates and any certifications related to the technologies/equipment.

1.2.6.3. Healthcare Providers must ensure that the installation, programming, calibration, initial testing and demonstrating of technologies/equipment, are undertaken in accordance with manufacturer's or supplier's guidance.

1.2.7. Data Protection

1.2.7.1. Policies:

1.2.7.1.1. Healthcare providers must maintain current policies and procedures for the management and protection of personal information.

1.2.7.1.2. Healthcare providers and procedures must ensure that the manner of storage, management and sharing of personal information normally carries the consent of users and patients.

1.2.7.2. Responsible parties:

1.2.7.2.1. Healthcare providers should have an effective, up-to-date privacy Compliance management program in place in the event of a complaint investigation.

1.2.7.2.2. Front-line and management staff must be trained on privacy and information security principles.

1.2.7.3. Information officer:

1.2.7.3.1. Healthcare providers should have an information officer that must ensure that a compliance framework is developed, implemented and monitored.

1.2.7.4. Information processing:

1.2.7.4.1. Contracts should be in place for the transfer of personal information to third parties and for processing (operators)

1.2.8. Checklist

Healthcare providers must:

Compliance with the Practice Guidelines

- Have a copy of the practice guidelines available. ☐
- The healthcare provider must add a section to their website noting their adherence to the guidelines. ☐

Conflicts of Interest

- Healthcare providers must avoid conflicts of interest in line with HPCSA guidelines. ☐

Undesirable corporate ownership

- Anybody that is not a registered healthcare practitioner does not qualify to directly or indirectly share in the profits or income of a professional practice. ☐

Level of skills and knowledge

- Healthcare providers must ensure that the service that is delivered is in line with their scope of practice. ☐
- Healthcare providers must have the appropriate level of qualification, competence and experience for the service they are delivering. ☐

Guideline training

- Record of guideline training must be maintained ☐

Asset Register

- Maintain an up to date and accurate registry of technologies/equipment. ☐
- Ensure that the technologies/equipment are managed in accordance with manufacturer's or supplier's guidance. ☐

Data Protection

- Healthcare providers must maintain current policies and procedures for the management and protection of personal information. ☐
- Patients must consent to the manner of storage, management and sharing of personal information ☐
- Front-line and management staff must be trained on privacy and information security principles. ☐
- Healthcare providers should have an information officer that must ensure that a compliance framework is developed, implemented and monitored. ☐
- Contracts should be in place for the transfer of personal information to third parties and for processing ☐

Healthcare providers should:

Guideline training

- Healthcare providers should have specific telemedicine training programs and development programs. ☐
- Staff who have never completed Guideline training should not commence telemedicine service provision. ☐
- Guideline specific training should be completed at least every two (2) years. ☐

1.3. Technology providers

1.3.1. Services agreements

1.3.1.1. Technology providers must maintain agreements with relevant telecommunications providers, companies or their agents. These agreements must comply with relevant legislation regarding:

1.3.1.1.1. Location of data storage

1.3.1.1.2. Access to data by third parties

1.3.1.1.3. Backup and storage

1.3.2. Data Protection

1.3.2.1. Technology providers must ensure that a robust plan for information security is in place with regular review and clear processes for:

1.3.2.1.1. Responding to and reporting security breaches;

1.3.2.1.2. Testing of information security defences

1.3.2.1.3. Data access control

1.3.2.1.4. Appropriate encryption

1.3.2.2. Technology providers must have a demonstrable capacity to comply with the POPIA Act.

1.3.2.2.1. A compliance framework

1.3.2.2.2. An information officers

1.3.2.2.3. Measures must ensure the 'confidentiality, integrity and availability' of the records, systems and services and the personal information processed within them.

1.3.2.3. Technology providers should review current best practice and costs of implementation of data security measures, but they must be appropriate and reasonable both to the circumstances and the risk that the processing poses.

1.3.2.4. The data protection measures must also enable the restoration of access and availability to personal information in a timely manner in the event of a physical or technical incident.

1.3.3. Checklist

Technology providers must:

Services agreements

Technology providers must maintain agreements with relevant telecommunications providers, companies or their agents. ☐

Data Protection ☐

Technology providers must ensure that the responsibilities and authorities for roles relevant to data protection is assigned and communicated. ☐

Technology providers must ensure that a robust plan for information security is in place. ☐

Technology providers must have a demonstrable capacity to comply with the POPI Act. ☐

Technology providers must implement a data protection risk management system that defines: ☐

- Data protection security risk acceptance criteria
- A method to identify data protection risks
- Analysing data protection risks
- Evaluating data protection risks and
- The treatment of data protection risks

Technology providers should:

Data Protection

Technology providers should review current best practice and costs of implementation of data security measures, but they must be appropriate and reasonable both to the circumstances and the risk that the processing poses. ☐

The data protection measures should also enable the restoration of access and availability to personal information in a timely manner in the event of a physical or technical incident. ☐

2. Delivery

2.1. Organisations

2.1.1. Appropriate patients

2.1.1.1. Organisations must confirm that healthcare providers have a pre-existing relationship with a patient before a telemedicine consult is started:

2.1.1.1.1. Direct patient to healthcare provider video consults:

2.1.1.1.1.1. The patient must be known to the healthcare provider to enable sufficient knowledge of the patient's clinical condition to be able to render a proper and clinically justifiable diagnosis, treatment or recommendation

2.1.1.1.1.2. This implies that the patient must have previously been examined in person and is known to the healthcare provider.

2.1.1.1.2. Multidisciplinary healthcare provider video consults:

2.1.1.1.2.1. The presenting healthcare provider must first examine the patient to enable sufficient knowledge of the patient's clinical condition to be able to discuss the patient with another healthcare provider.

2.1.1.2. Organisations must have a structured method of confirm that it is clinically appropriate to deliver a healthcare service via telemedicine (e.g. Triage)

2.1.2. Promotion and Marketing

2.1.2.1. Organisations must promote their services in a balanced and appropriate way:

2.1.2.1.1. Do not exaggerate the extent of disease risk

2.1.2.1.2. Do not exaggerate the anticipated benefits of Telemedicine service.

2.1.2.1.3. Promote the product offering by employing guarantees or material benefits outside the categories of professional services.

2.1.2.2. Organisations must be compliant with the relevant regulations regarding promotion and marketing of professional services.[3]

2.1.3. Physical Security

2.1.3.1. Organisations must ensure the suitability and physical security of the location or locations from which their service operates specifically related to[4]:

2.1.3.1.1. Accessibility of locations for people with disability

2.1.3.1.2. Adequate space and privacy of locations. The location of the consulting or servicing healthcare practitioner must be physically secure to ensure that the duties to patients that include, but are not limited to, always acting in the best interest or well-being of the patient, respecting patients' privacy and dignity, giving patients the information they need about their conditions, and maintaining confidentiality at all times as required are adhered to.

[3] HPCSA , Guidelines for making professional services known

2.1.4. Sufficiency of Staff for Service Provision

2.1.4.1. Healthcare providers and organisations should have a sufficient variety and quantity of staff to ensure a safe, effective and sustained operation of the service.

2.1.4.2. Healthcare providers and organisations should be able to demonstrate how they determine and monitor the appropriate number of staff and how they plan for their staff resource in the context of service maintenance, growth or development.

2.1.5. Agreements with patients

2.1.5.1. Organisations must have an agreement with patients regarding the manner of service provision, selected payment option(s) where they apply, arrangements for gathering personal information, response protocols, and procedures for service discontinuation.

2.1.6. Data Protection

2.1.6.1. Usage of Personal Information

2.1.6.1.1. Organisations must ensure that users and patients are aware of whether, how and in what circumstances their personal information is shared with other bodies.

2.1.6.1.2. Organisations must be compliant with the relevant regulations regarding usage of personal information e.g., National Health Act, POPIA, PAIA etc.

[4] Occupational Health and Safety Act (Act No. 85 of 1993), the Constitution, SA National Patients' Rights Charter, the National Health Act No 61 of 2003, the Promotion of Access to Information Act No 2 of 2000, the Protection of Personal Information Act No 4 of 2013, the Common law and the HPCSA's ethical guidelines on patient confidentiality in Booklet 10

2.1.7. Checklist

Organisations must:

Promotion and Marketing

Organisations must promote their services in a balanced and appropriate way ☐

Physical Security

Organisations must ensure the suitability and physical security and safety of the location. ☐

Agreements with users and patients

Organisations must have an agreement with patients regarding the manner of service provision, selected payment option(s) where they apply, arrangements for gathering personal information, response protocols, and procedures for service discontinuation. ☐

Data Protection

Organisations must ensure that users and patients are aware of whether, how and in what circumstances their personal information is shared with third parties. ☐

Organisations must be compliant with the relevant regulations regarding usage of personal information e.g. POPIA ☐

Organisations providers should:

Sufficiency of Staff for Service Provision

Healthcare providers and organisations should have a sufficient variety and quantity of staff to ensure a safe, effective and sustained operation of the service. ☐

2.3. Healthcare providers

2.3.1. Promotion and Marketing

2.3.1.1. Healthcare providers must be compliant with the relevant regulations regarding promotion and marketing of professional services.[5]

2.3.1.1.1. Advertising

2.3.1.1.1.1. A healthcare practitioner shall only advertise his or her services or permit, sanction, or acquiesce to such advertisement if it is done in the manner determined by the HPCSA from time to time.

2.3.1.1.2. Canvassing and touting

2.3.1.1.2.1. A healthcare practitioner must not canvas for patients in whatever manner from door to door in any particular area to recruit patients either verbally or by handing out promotional material;

2.3.1.1.2.2. A healthcare practitioner must not tout for patients in whatever manner by improperly drawing attention, either verbally or by means of the printed or electronic media to the titles, professional attainments, personal qualities, superior knowledge or quality of service of a particular practitioner or by improperly drawing attention to his or her practice or best prices offered.

2.3.2. Patient Selection Duty of care

2.3.2.1. Organisations should not take over the care of a patient from another provider unless:

2.3.2.1.1. They have taken reasonable steps to inform the other provider that the patient has requested care to be taken over

2.3.2.1.2. Has established from the other provider the current treatment of the patient , which the other provider is obliged to share.

2.3.2.2. There must be agreement by the patient that the servicing practitioner will decide whether or not the condition being diagnosed or treated is appropriate for a telemedicine consultation

2.3.2.3. Healthcare providers must respect patients' requests for in-person care whenever feasible.

2.3.3. Clinical Guidelines

2.3.3.1. The healthcare providers providing care via Telemedicine must be aware of pertinent professional discipline guidelines and standards that must be upheld in the Telemedicine encounter, with consideration of the specific context, location, timing, and services delivered to the patient.

2.3.3.2. Healthcare professionals must be culturally competent to deliver services to the populations that they serve.

2.3.3.2.1. Examples of factors to consider include awareness of the client's language, ethnicity, race, age, gender, sexual orientation, geographical location, socioeconomic, and cultural backgrounds.

2.3.4. Identification

2.3.4.1. Healthcare provider and patient identity must be verified.

2.3.4.1.1. The Telemedicine provider must provide the patient (or legal representative) with his or her qualifications and professional registration information, where applicable.

2.3.4.1.2. Patients must provide their full name, date of birth, and contact information that allows healthcare professionals, organisations and technology platform providers to make contact them should the need arise.

2.3.4.2. Healthcare professionals may ask patients to verify their identity more formally by providing a government-issued photo ID.

2.3.4.3. In cases where there is an existing established relationship between patient and healthcare professional and this documentation already exists, this process may be omitted.

2.3.5. Consent

2.3.5.1. Healthcare providers must be familiar with the Health Professions Council guidance regarding consent. [6]

2.3.5.2. Explicit consent must be obtained from the patient for medical acts that would normally require explicit consent in the traditional health care setting (e.g. video or audio recording of the sessions, use of data for research or educational purposes).

2.3.5.3. The patient must be given the ability to make informed decisions. The following information should be included:

2.3.5.3.1. The objective of the Telemedicine interaction

2.3.5.3.2. The role and responsibility of the provider and the patient during the Telemedicine interaction

2.3.5.3.3. Other healthcare professionals participating in the interaction

2.3.5.3.4. Care documentation requirements

2.3.5.3.5. Risks and benefits

2.3.5.4. As far as possible, the consent process should be integrated with the existing routine care processes.

2.3.6. Consultations

2.3.6.1. Healthcare providers must be aware of the differences between Telemedicine consultations and face-to-face contact.

2.3.6.2. Healthcare providers should adhere to the following principles so that they can ensure that the standard of care is maintained in Telemedicine consultations:

2.3.6.2.1. The service must be provided as part of a structured and well-organized system and the overall standard of care delivered by the system must not be any less compared to a service not involving Telemedicine.

2.3.6.2.2. Where a face-to-face consult is not reasonably practicable, it is permitted to deliver care exclusively via Telemedicine as this is better than not having any access to care at all.

2.3.6.2.3. Where face-to-face consultations are reasonably practicable, the delivery of care via Telemedicine must not compromise the overall quality of care provided as compared with non-Telemedicine care delivery.

[5] HPCSA , Guidelines for making professional services known

[6] GUIDELINES FOR GOOD PRACTICE IN THE HEALTH CARE PROFESSIONS SEEKING PATIENTS' INFORMED CONSENT: THE ETHICAL CONSIDERATIONS BOOKLET 9

2.3.6.3. Prior to commencing Telemedicine services to a patient, the healthcare provider must be satisfied that the patient is suitable for a Telemedicine interaction (Appropriate patient) and that the standard of care delivered via Telemedicine is reasonable considering the specific context.

2.3.6.3.1. A face-to-face evaluation/consultation where reasonably practical should be done before or very soon after the commencement of Telemedicine services.

2.3.6.3.2. The reasonableness of delivering care via Telemedicine is determined by the clinical context, the clinical objectives and the compatibility of technology to meet those objectives.

2.3.6.3.3. Other considerations include the literacy level of the patient, the level of training of the healthcare professional, and the availability of satisfactory alternative

2.3.6.3.4. No opening of video or audio channels must take place until the 'call' has been accepted by the patient or the receiving service provider.

2.3.6.4. Provision must be made for patients and/or receiving healthcare providers to easily terminate such consultations. It must, in either case, be clear to them when video and/or audio links have been closed.

2.3.6.5. Where telemedicine consultations are delayed, notification must be made to all parties involved in the consultation.

2.3.7. Clinical Notes

2.3.7.1. The patient's records established during the use of telemedicine must be accessible and documented for both the healthcare practitioners involved and their patients.

2.3.7.2. Record keeping guidelines according to the HPCSA Health care practitioners should enter and maintain at least the following information for each patient consulted:

2.3.7.2.1. Personal (identifying) particulars of the patient.

2.3.7.2.2. The biopsychosocial history of the patient, including allergies and idiosyncrasies.

2.3.7.2.3. The time, date and place of every consultation.

2.3.7.2.4. The assessment of the patient's condition.

2.3.7.2.5. The proposed clinical management of the patient.

2.3.7.2.6. The medication and dosage prescribed.

2.3.7.2.7. Details of referrals to specialists, if any.

2.3.7.2.8. The patient's reaction to treatment or medication, including adverse effects.

2.3.7.2.9. Test results.

2.3.7.2.10. Imaging investigation results.

2.3.7.2.11. Information on the times that the patient was booked off from work and the relevant reasons.

2.3.7.2.12. Written proof of informed consent, where applicable.

2.3.8. E-Prescribing

2.3.8.1. Electronic scripts must have an encrypted signature on script in line with regulations.[7]

2.3.8.2. The following prescriber details should be on the script

- 2.3.8.2.1. Prescriber name
- 2.3.8.2.2. Their qualification
- 2.3.8.2.3. Their registration number with according to the HPCSA[8]
- 2.3.8.2.4. The practice address
- 2.3.8.2.5. Prescriber practice should be added to assist Pharmacies when claiming from Medical Schemes

2.3.8.3. The following patient details should be on the script

- 2.3.8.3.1. Patient National identification of Passport number
- 2.3.8.3.2. Patient Address

2.3.8.4. The following details should be on the script

- 2.3.8.4.1. Date of script issue
- 2.3.8.4.2. Product name
- 2.3.8.4.3. Product strength and dosage form
- 2.3.8.4.4. Product quantity (S6 in words and figures)
- 2.3.8.4.5. Dosing instructions
- 2.3.8.4.6. Patient age
- 2.3.8.4.7. Patient gender
- 2.3.8.4.8. Number of repeats

2.3.8.5. Transmission of electronic script

- 2.3.8.5.1. The script must be prepared with a secure electronic agent
- 2.3.8.5.2. The script must be sent to patient's choice of pharmacy via electronic agent
- 2.3.8.5.3. The script must be sent directly to pharmacy and not to the patient who forwards the script to the pharmacy.

2.3.9. Handover of patients

2.3.9.1. Telemedicine opens up numerous options for referral and coordinated care. Proper referral and other necessary protocols should be put in place to avoid fragmentation of care, and all parties involved should be aware as to who is responsible for each aspect of care.

2.3.9.2. Healthcare providers must have procedures and protocols when patients need routine or emergency handover to another healthcare provider or service.

[7] Advanced electronic signature in compliance with section 13 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002

[8] Medicines and Related Substances Act, 1965 (Act No. 101 of 1965),

2.3.10. Data Protection

2.3.10.1. Maintaining Records

2.3.10.1.1. Healthcare providers must maintain comprehensive and up to date records for the service.

2.3.10.1.2. Health records should be stored in a safe place and if they are in electronic format, safeguarded by passwords.

2.3.10.1.3. Health records should be stored for a period of not less than six (6) years as from the date they became dormant.

2.3.10.1.4. In the case of minors and those patients who are mentally incompetent, health care practitioners should keep the records for a longer period:

2.3.10.1.5. For minors under the age of 18 years health records should be kept until the minor's 21st birthday because legally minors have up to three years after they reach the age of 18 years to bring a claim. This would apply equally for obstetric records.

2.3.10.1.6. For mentally incompetent patients the records should be kept for the duration of the patient's lifetime.

2.3.10.1.7. In terms of the Occupational Health and Safety Act (Act No. 85 of 1993) health records must be kept for a period of 20 years after treatment.

2.3.10.1.8. Records should also document information on

2.3.10.1.8.1. staff engaged; and the

2.3.10.1.8.2. qualifications, training and competencies of staff.

2.3.10.2. Sharing Information with users and patients

2.3.10.2.1. Healthcare providers and organisations must make information about the service available to patients, so they can exercise informed choices and give consent regarding their acceptance (or not) of the service and service options.

2.3.10.2.2. Sharing may or may not be subject to anonymisation or pseudo-anonymisation. In the case of the latter, the procedure selected must ensure that reasonable steps are taken to remove the possibility that individuals can be identified from the information in question.

2.3.10.2.3. Informed choice means that users and patients must receive information (whether in speech, written or printed material, in video, DVD or in apps) that is timely, clear and comprehensive.

2.3.10.2.4. Through such information patients need to be made aware of:

2.3.10.2.4.1. Service options

2.3.10.2.4.2. The risks and benefits pertaining to service operation

2.3.10.2.4.3. Rights and responsibilities

2.3.10.2.4.4. Arrangements for termination of or withdrawal from the service

2.3.10.2.4.5. Applicable charges and costs

2.3.10.3. Device security:

2.3.10.3.1. Healthcare providers must ensure that access to any patient contact information stored on any device is adequately restricted.

2.3.10.3.1.1. Devices must require a passphrase or equivalent security feature before the device can be accessed.

2.3.10.3.1.2. If multi-factor authentication is available, it should be used.

2.3.10.3.1.3. Devices must be configured to utilize an inactivity timeout function that requires a passphrase or re-authentication to access the device after the timeout threshold has been exceeded. This timeout should not exceed 15 minutes.

2.3.10.3.1.4. Mobile devices should be kept in the possession of the provider when travelling or in an uncontrolled environment.

2.3.10.3.1.5. Unauthorized persons must not be allowed access to sensitive information stored on any device or use the device to access sensitive applications or network resources.

2.3.10.3.1.6. Healthcare providers should have the capability to remotely disable or wipe their mobile device in the event it is lost or stolen.

2.3.10.3.1.7. Healthcare providers and organizations may consider establishing guidelines for periodic purging or deletion of Telemedicine related files from mobile devices.

2.3.10.3.2. Access to records:[9]

2.3.10.3.2.1. A health care practitioner must provide any person of age 12 years and older with a copy or abstract or direct access to his or her own records regarding medical treatment on request (Children's Act (Act No. 38 of 2005)).

2.3.10.3.2.2. Where the patient is under the age of 16 years, the parent or legal guardian may make the application for access to the records, but such access should only be given on receipt of written authorization by the patient (Access to Information Act (Act No. 2 of 2000)).

2.3.10.3.2.3. Information about termination of a pregnancy may not be divulged to any party, except the patient herself, regardless of the age of the patient (Choice on Termination of Pregnancy Act (Act No. 92 of 1996)).

2.3.10.3.2.4. No health care practitioner must make information available to any third party without the written authorisation of the patient or court order or where nondisclosure of the information would represent a serious threat to public health (National Health Act (Act 61 of 2003)).

2.3.10.4. Staff Access to Personal Information

2.3.10.4.1. Organisations and Healthcare providers must ensure that only authorised staff can access personal information regarding users and patients.

2.3.10.4.2. Healthcare providers and staff must be individually identified when accessing information and access credentials should not be shared between users and patients for services and device

[9] From HPCSA GUIDELINES FOR GOOD PRACTICE, BOOKLET 14, PRETORIA, MAY 2008

2.3.11. Checklist

Healthcare providers must:

Compliance with the Practice Guidelines

Duty of care

Organizations and healthcare providers must record patients' preference for care via telemedicine. ☐

Clinical Guidelines

The healthcare providers providing care via Telemedicine must have copies of pertinent professional discipline guidelines ☐

Identification

Healthcare provider and patient identity must be verified. ☐

Consent

Healthcare providers must have a copy and be familiar with the Health Professions Council of South Africa rules and guidance regarding consent. ☐

All patients must provide consent to the telemedicine consult or service. ☐

Consultations

Prior to commencing Telemedicine services to a patient, the healthcare provider must be satisfied that the patient is suitable for a Telemedicine interaction (e.g. Triage). ☐

No opening of video or audio channels must take place until the 'call' has been accepted by the patient or the receiving service provider ☐

Provision must be made for patients and/or receiving healthcare providers to easily terminate such consultations. It must, in either case, be clear to them when video and/or audio links have been closed. ☐

Where telemedicine consultations are delayed, notification must be made to all parties involved. ☐

E-Prescribing

Electronic scripts must have an encrypted signature on script in line with regulations. ☐

The script must contain the prescriber details ☐

The script must contain the correct patient details ☐

The script should contain the appropriate medication details ☐

The script must be prepared with a secure electronic agent ☐

The script must be sent to patient's choice of pharmacy via electronic agent ☐

The script must be sent directly to pharmacy and not to the patient who forwards the script to the pharmacy. ☐

Data Protection: Maintaining Records

Healthcare providers must maintain comprehensive and up to date records for the service. ☐

Health records must be stored in a safe place and electronic format, safeguarded by passwords. ☐

Health records must be stored for a period of not less than six (6) years as from dormant date ☐

Health record of minors (under 18 years) must be kept until the minor's 21st birthday This would apply equally for obstetric records. ☐

Health record of mentally incompetent patients the records should be kept for patient's lifetime ☐

Occupational records must be kept for a period of 20 years after treatment. ☐

Data Protection: Sharing Information with users and patients

Health care providers should inform patients of: ☐

- Service options
- The risks and benefits pertaining to service operation
- Rights and responsibilities
- Arrangements for termination of or withdrawal from the service
- Applicable charges and costs

Device security:

Devices must require a passphrase or equivalent security feature before the device can be accessed. ☐
Devices must be configured to utilize an inactivity timeout function that requires a passphrase or re-authentication to access the device after the timeout threshold has been exceeded. This timeout should not exceed 15 minutes. ☐

Access to records:

No health care practitioner must make information available to any third party without the written authorisation of the patient or court order or where nondisclosure of the information would represent a serious threat to public health (National Health Act (Act 61 of 2003)). ☐

Staff Access to Personal Information

Organisations and Healthcare providers must ensure that only authorised staff can access personal information regarding users and patients and their service usage. ☐
Healthcare providers and staff must be individually identified when accessing information and access credentials should not be shared between users and patients for services and devices. ☐

Healthcare providers should:

Consent

Healthcare providers must have a copy and be familiar with the Health Professions Council guidance regarding consent. ☐
The consent should at least contain the following: ☐

- The objective of the Telemedicine interaction
- The role and responsibility of the provider and the patient during the Telemedicine interaction
- Other people participating in the interaction
- Care documentation requirements

Clinical Notes

Healthcare practitioner should enter and maintain at least the following information for each patient consulted: ☐

- Personal (identifying) particulars of the patient.
- The biopsychosocial history of the patient, including allergies and idiosyncrasies.
- The time, date and place of every consultation.
- The assessment of the patient's condition.
- The proposed clinical management of the patient.
- The medication and dosage prescribed.
- Details of referrals to specialists, if any.
- The patient's reaction to treatment or medication, including adverse effects.
- Known Test results.
- Known Imaging investigation results.
- Sick notes Informed consent copies

Handover of patients

Healthcare providers should have procedures and protocols when patients need routine or emergency handover to another healthcare provider or service. ☐

Data Protection: Sharing Information with users and patients

Health care providers should inform patients of: ☐

- Service options
- The risks and benefits pertaining to service operation
- Rights and responsibilities
- Arrangements for termination of or withdrawal from the service
- Applicable charges and costs

Device security:

Healthcare providers should have the capability to remotely disable or wipe their mobile device in the event it is lost or stolen. ☐

2.4. Technology providers

2.4.1. Training for patients

2.4.1.1. Technology providers must provide guidance and training to patients if they required to interact directly with the telemedicine technology.

2.4.2. Quality of the telemedicine consultation

2.4.2.1. Technology providers must make all efforts to ensures stability of the telemedicine consult so that it happens without interruption of degradation of the service.

2.4.2.2. Technology providers must ensure that the consultation is appropriately closed with an end of all video and sound streams.

2.4.2.3. Technology providers must store the data of the consultation in an appropriate and secure format, including:

2.4.2.3.1. Time and date of consultation

2.4.2.3.2. Length of consultation

2.4.2.3.3. Quality metrics

2.4.3. User and Patient Fault Reporting

2.4.3.1. Technology providers must provide service users and patients with an easy means of reporting faults or failures of the technologies.

2.4.3.2. There must be a support facility for users and patients to report faults via the service website and/or via telephone.

2.4.3.3. Faults reported must be assessed promptly and ranked according to impact of the service on patient safety and service delivery.

2.4.3.3.1. Based on the ranking a specific resolution time should be agreed between technology providers, organisations and healthcare providers.

2.4.3.3.2. Clear circumstances and reasoning must be defined for the immediate cessation of the service.

2.4.1. Compliance Checklist

Technology providers must:

Data Protection

The technology provider must perform data protection risk assessments at planned intervals or when significant changes are proposed or occur, taking account the criteria established under the Planning section.

Training for patients

Technology providers must provide guidance and training to patients if they required to interact directly with the telemedicine technology. ☐

Quality of the telemedicine consultation

Technology providers must make all efforts to ensures stability of the telemedicine consult so that it happens without interruption of degradation of the service. ☐

Technology providers must ensure that the consultation is appropriately closed with an end of all video and sound streams. ☐

Technology providers must store the data of the consultation in an appropriate and secure format, including: ☐

- Time and date of consultation
- Length of consultation
- Quality metrics

User and Patient Fault Reporting

Technology providers must provide service users and patients with an easy means of reporting faults or failures of the technologies ☐

There must be a support facility for users and patients to report faults via the service website and/or via telephone. ☐

Faults reported must be assessed promptly and ranked according to impact of the service on patient safety and service delivery. ☐

Clear circumstances and reasoning must be defined for the immediate cessation of the service ☐

3. Learning

3.1. Organisations

3.1.1. Outcomes Focused Appraisal

3.1.1.1. Organisations should undertake a regular telemedicine outcome focused appraisal to help management improve services. This should include a review of:

3.1.1.1.1. The impact on the health of the patients who used the service

3.1.1.1.1.1. Clinical outcomes and treatment efficacy

3.1.1.1.1.2. Disease progression (i.e., how is the health of patients progressing)

3.1.1.1.1.3. Clinical outcomes (i.e., did the treatment work)

3.1.1.1.1.4. Compliance with clinical protocols

3.1.1.1.1.5. Perception of healthcare professional

3.1.1.1.2. How the service has acted upon the complaints, compliments and suggestions received

3.1.1.1.3. Feedback from any surveys of healthcare providers and patients.

3.1.1.2. In new services, the outcomes-focused appraisal should put baselines in place and offer a framework against which future measurement of progress can be made.

3.1.2. Operational Performance

3.1.2.1. Organisations should record their performance in relation to a set of measures relevant to the telemedicine service they provide.

3.1.2.2. Operational measures may include the time taken, number or frequency with regard to:

3.1.2.2.1.1. Wait times

3.1.2.2.1.2. Audio-visual quality

3.1.2.2.1.3. State of equipment

3.1.2.3. Organisations should have a process of addressing and improving performance issues identified.

3.1.3. Compliance Checklist

Organisations providers should:

Outcomes Focused Appraisals

The impact on the health of the patients who used the service	☐
Clinical outcomes and treatment efficacy	☐
Disease progression (i.e., how is the health of patients progressing)	☐
Clinical outcomes (i.e., did the treatment work)	☐
Compliance with clinical protocols	☐
User experience outcomes	☐
Perception of healthcare professional	☐
How the service has acted upon the complaints, compliments and suggestions received	☐
Feedback from any surveys of healthcare providers and patients.	☐

Operational Performance

Organisations should record their performance in relation to a set of measures relevant to the telemedicine service they provide.	☐
Wait times	☐
Audio-visual quality	☐
State of equipment	☐

3.3. Health care providers

3.3.1. Clinical Performance

3.3.1.1. Healthcare providers must undertake an annual appraisal appropriate to the telemedicine service they deliver.

3.3.1.2. The clinical appraisal may include:

3.3.1.2.1. Compliance with clinical guidelines

3.3.1.2.2. The incidence of conditions treated

3.3.1.2.3. Incidence of emergency, acute and chronic visits

3.3.1.2.4. Adverse events

3.3.1.2.5. Mortality events

3.3.1.3. In new services, the outcomes-focused appraisal should put baselines in place and offer a framework against which future measurement of progress can be made.

3.3.2. Service Performance

3.3.2.1. Healthcare providers should record their performance in relation to a set of measures relevant to their registered profession.

3.3.2.2. Operational measures may include the time that is taken, number or frequency with regard to:

3.3.2.2.1. Patient quality feedback scores

3.3.2.2.2. Complaints, compliments and suggestions.

3.3.2.3. Organisations must have a process of addressing and improving performance issues identified.

3.4.1. Compliance Checklist

Healthcare providers should:

Clinical Performance

Healthcare providers should undertake an annual appraisal appropriate to the telemedicine service they deliver.	☐
Monitor compliance with clinical guidelines	☐
Monitor the incidence of conditions treated	☐
Monitor the incidence of emergency, acute and chronic visits	☐
Record Adverse events	☐
Record Mortality events	☐

Service Performance

Healthcare providers must record their performance in relation to a set of measures relevant to their registered profession	☐
Operational measures may include the time that is taken, number or frequency with regard to: Patient quality feedback scores	☐
Complaints, compliments and suggestions.	☐
Organisations must have a process of addressing and improving performance issues identified	☐

3.5. Technology providers

3.5.1. Uptime

3.5.1.1. Technology providers must have standard service level agreements with Organisations and Healthcare providers regarding:

3.5.1.1.1. Service and support availability (up time)

3.5.1.1.2. Turnaround time on fixes of issues and faults

3.5.2. Communications Networks

3.5.2.1. Technology providers must monitor the communications networks used to ensure that they are operational and that faults are speedily identified and remedied.

3.5.2.2. The outcomes of monitoring must be recorded to ensure that the integrity of communications networks is maintained in accordance with service levels given. This must include monitoring for cyber-attacks.

3.5.3. User and patient Fault Reporting

3.5.3.1. Organisations, Healthcare providers and technology providers must provide service users and patients with an easy means of reporting faults or failures of the technologies.

3.5.3.2. There must be a support facility for users and patients to report faults via the service website and/or via telephone.

3.5.3.3. Faults reported must be assessed promptly and ranked according to impact of the service on patient safety and service delivery.

3.5.3.3.1. Based on the ranking a specific resolution time should be agreed between technology providers, organisations and healthcare providers.

3.5.3.3.2. Clear circumstances and reasoning must be defined for the immediate cessation of the service.

3.5.4. Compliance Checklist

Technology providers must:

Data Protection

The technology provider must review data protection management at planned intervals to ensure its continuing suitability, adequacy and effectiveness of the data protection measures. This may include feedback from users, inputs from data protection risks assessments and results from fault reporting.

Uptime

Technology providers must have standard service level agreements. ☐

Monitor service availability (up time) ☐

Monitor turnaround time on fixes of issues and faults ☐

Communications Networks

Technology providers must monitor the communications networks used to ensure that they are operational and that faults are speedily identified and remedied. ☐

The outcomes of monitoring must be recorded to ensure that the integrity of communications networks is maintained in accordance with service levels given. This must include monitoring for cyber-attacks. ☐

User and patient Fault Reporting

Technology providers must provide service users and patients with an easy means of reporting faults or failures of the technologies. ☐

There must be a support facility for users to report faults via the service website and/or via telephone. ☐

Faults must be assessed promptly and ranked according to impact of the service on patient safety and service delivery. ☐

Based on the ranking a specific resolution time should be agreed between technology providers, organisations and healthcare providers. ☐

Clear circumstances and reasoning must be defined for the immediate cessation of the service ☐

4. Risk and Quality Management

4.1. Organisations

4.1.1. Risk Management

4.1.1.1. Organisations must have a current risk management system that takes account of the outcomes of risk assessments and seeks to reduce the likelihood and impact of any adverse incidents for all elements of service provision.

4.1.1.2. This system and related documents must identify and follow a clear risk assessment process by which these are assessed and prioritised. It/they must cover risks that relate to buildings, the communications infrastructure, information (cyber-) security, contamination of equipment/technologies and other matters relating to service provision.

4.1.2. Insurance

4.1.2.1. Organisations must have current insurance policies including, for example, buildings and equipment, public and product liability, professional indemnity, employer's liability, cyber security and, where appropriate any cover that reduces the risk of legal litigation.

4.1.2.2. Organisations may carry insurance policies for healthcare providers that help deliver the service.

4.1.3. Business Continuity Plan

4.1.3.1. Organisations must have a business continuity plan that supports service dependability and determine the way in which disruption to the service will be dealt with or closure of the service achieved - whilst, at the same time, providing safeguards for users and patients including those regarding their personal data.

4.1.3.2. Considerations around disruption may include:

- 4.1.3.2.1. Network failures
- 4.1.3.2.2. Information security breaches (including DDoS, distributed denial of service attacks)
- 4.1.3.2.3. Extreme weather
- 4.1.3.2.4. Employee illness
- 4.1.3.2.5. Loss of a key sub-contractor
- 4.1.3.2.6. Service insolvency.

4.1.3.3. The business continuity plan must be dated, and key elements tested at an appropriate level, at least annually.

4.1.4. Compliance Checklist

Organisations providers should:

Risk Management

Organisations must have a risk management system. ☐
This system and related documents must identify and follow a clear risk assessment process by which these are assessed and prioritised. ☐

Insurance ☐
Organisations must have current insurance policies ☐

Business Continuity Plan

Organisations must have a business continuity plan that supports service dependability and determine the way in which disruption to the service will be dealt with. ☐

4.3. Healthcare provider

4.3.1. Risk Management

4.3.1.1. Healthcare providers should have a current risk management system that takes account of the outcomes of risk assessments and seeks to reduce the likelihood and impact of any adverse incidents for all elements of service provision.

4.3.2. Insurance

4.3.2.1. Healthcare providers must have current insurance policies including, for example, buildings and equipment, public and product liability, professional indemnity, employer's liability, cyber security and, where appropriate any cover that reduces the risk of legal litigation.

4.3.3. Compliance Checklist

Healthcare providers must:

Healthcare providers must have current insurance policies ☐

Healthcare providers should:

Healthcare providers should have a current risk management system. ☐

4.5. Technology providers

4.5.1. Back Up IT Arrangements

4.5.1.1. Technology providers must maintain procedures for real-time or, at a minimum, daily transfer of information relating to service operation and the personal data of users and patients, to a secure environment.

4.5.1.2. The back-up procedures must relate to all core functions of the service. These must enable the minimisation of any disruption following an 'event' and the continued operation (or prompt recommencement of operation) at a satisfactory level (i.e. with ongoing monitoring of or for service users).

4.5.1.3. The procedures must take account of the potential for disruption that can arise due to IT failure or a cyber (information) security attacks, problems with the telecommunications network or staff shortages. In any event, the procedures must ensure that personal information regarding service users and patients (and access to it) is safeguarded.

4.5.2. Equipment Recall, Removal and Disconnection Procedures

4.5.2.1. Technology providers must have procedures for the recall, removal and/or disconnection of faulty or contaminated equipment from users and patients

4.5.2.1.1. These procedures should include, where appropriate, of the disconnection of technologies/equipment supplied by users and patients themselves.

4.5.2.1.2. They should ensure, wherever appropriate, timely replacement and/or provision of relevant advice or guidance to ensure that users and patients are safeguarded.

4.5.2.2. It is recognised that for some services such procedures may be given effect through intermediary organisations.

4.5.3. Protection and Safe-keeping of Technologies/Equipment

4.5.3.1. Technology providers must make provision for the protection, safe-keeping and storage of technologies/equipment.

4.5.3.2. The requirement for the protection and safekeeping of technologies/equipment must be satisfied either directly by services or via arrangements with subcontractors. It is recognised that such protection and safekeeping will, in some cases, be undertaken by intermediary organisations.

4.5.4. Maintenance, Servicing, Repair and Replacement of Technologies/Equipment

4.5.4.1. Organisations, Healthcare providers and Technology providers must have robust procedures in place to enable maintenance, servicing, calibration, repair or replacement of technologies/equipment where supplied by the service.

4.5.4.2. Maintenance, servicing, repair or replacement must be undertaken within contracted timescales, in accordance with manufacturer's or supplier's guidance only by people who have required skills, knowledge and expertise.

4.5.4.3. Determining the maximum timescales for repairs and maintenance (within e.g. any contracted arrangement) will have involved consideration, by services, of the risks to users and patients. Required action may, for some services, be given effect through intermediary organisations.

4.5.4.4. Maintenance must include, wherever appropriate, cleansing and decontamination, (re)calibration, battery replacement (or re-charging) and functional checks.

4.5.4.5. Separate quality assurance checks may be necessary for devices that measure vital signs or are used for testing at the point of care.

4.5.1. Compliance Checklist

Technology providers must:

Back Up IT Arrangements

Technology providers must maintain procedures for real-time or, at a minimum, daily transfer of information. ☐

The back-up procedures must relate to all core functions of the service. ☐

Equipment Recall, Removal and Disconnection Procedures

Technology providers must have procedures for the recall, removal and/or disconnection of faulty or contaminated equipment from users and patients ☐

Protection and Safe-keeping of Technologies/Equipment

Technology providers must make provision for the protection, safe-keeping and storage of technologies/equipment. ☐

Maintenance, Servicing, Repair and Replacement of Technologies/Equipment

Maintenance, servicing, repair or replacement must be undertaken within contracted timescales, in accordance with manufacturer's or supplier's guidance only by people who have required skills, knowledge and expertise. ☐

Maintenance must include, wherever appropriate, cleansing and decontamination, (re)calibration, battery replacement (or re-charging) and functional checks. ☐

Improvement

A root cause investigation must be performed if a reported fault is classified as an incident or if a fault trend has been identified during the Learning process.

5. List of common Telemedicine terms

A	Authentication:	A method of verifying the identity of a person sending or receiving information using passwords, keys and other automated identifiers
B		
C	Council for Medical Schemes	The Council for Medical Schemes is a statutory body established by the Medical Schemes Act (131 of 1998) to provide regulatory supervision of private health financing through medical schemes.
	Clinical Decision Support System (CCDS):	Systems (usually electronically based and interactive) that provide clinicians, staff, patients, and other individuals with knowledge and person-specific information, intelligently filtered and presented at appropriate times, to enhance health and health care
	Clinical Information System:	Hospital-based information system designed to collect and organize data relating exclusively to information regarding the care of a patient rather than administrative data. .
	Compliance management program	Compliance management is the process by which managers, plan, organize, control, and lead activities that ensure compliance with laws and standards. These activities can include: Internal audits, Third-party audits, Security procedures and control, Preparing reports and providing supporting documentation, Developing and implementing policies and procedures to ensure compliance
	Computer-based Patient Record (CPR	An electronic form of individual patient information designed to provide access to complete and accurate patient data.
D	Diagnostic Equipment	Scopes, Cameras and Other Peripheral Devices. A piece of hardware or device not part of the central computer (e.g., digitizers, stethoscope, or camera) that can provide medical data input to or accept output from the computer.
	Digital Imaging and Communication in Medicine (DICOM):	The international standard for medical images and related information (ISO 12052). DICOM consists of a set of protocols describing how images are identified, formatted, transmitted and displayed that is vendor-independent. It was developed by the American College of Radiology and the National Electronic Manufacturers Association
	Electronic Signature:	Mathematical scheme for authenticating digital messages or documents. Valid signatures give the recipient evidence that the message was created by a known sender and not altered in transit.
	Distance Learning:	The incorporation of video and audio technologies, allowing students to "attend" classes and training sessions that are being presented at a remote location. Distance learning systems are usually interactive and are a tool in the delivery of training and education to widely dispersed students, or in instances in which the instructor cannot travel to the student's site.
	Distant Site:	Site at which the physician or other licensed practitioner delivering the service is located at the time the service is provided via telecommunications system. Other common names for this term include hub site, specialty site, provider/physician site and referral site. The site may also be referred to as the consulting site

E	e-Pharmacy:	The use of electronic information and communication technology to provide and support comprehensive pharmacy services when distance separates the participants.
	eHealth:	Healthcare practice supported by electronic processes and communication.
	Electronic Data Interchange (EDI):	The sending and receiving of data directly between trading partners without paper or human intervention.
	Electronic Health Record (EHR):	A systematic collection of electronic health information about individual patients or populations that is recorded in digital format and capable of being shared across health care settings via network-connected enterprise-wide information systems and other information networks or exchanges. EHRs generally include patient demographics, medical history, medication, allergies, immunization status, laboratory test results, radiology and other medical images, vital signs, characteristics such as age and weight, and billing information.
	Electronic Medical Record (EMR):	A computerized medical record generated in an organization that delivers health care, such as a hospital or physician's office. EMRs are often part of a local stand-alone health information system that allow storage, retrieval and modification of records.
	Electronic Patient Record (EPR):	An electronic form of individual patient information that is designed to provide access to complete and accurate patient data, alerts, reminders, clinical decision support systems, links to medical knowledge, and other aids.
	Encryption:	A system of encoding electronic data where the information can only be retrieved and decoded by the person or computer system authorized to access it.
	e-Prescribing:	The electronic generation, transmission and filling of a medical prescription, as opposed to traditional paper and faxed prescriptions. E-prescribing allows for qualified healthcare personnel to transmit a new prescription or renewal authorization to a community or mail-order pharmacy.
F		
G	Guideline:	A statement of policy or procedures to determine a course of action or give guidance for setting standards (http://jtt.rsmjournals.com/content/8/2/63.abstract).
H	Health Information Exchange (HIE):	the mobilization of healthcare information electronically across organizations within a region, community or hospital system. (Wikipedia)
	Health Level-7 Data Communications Protocol (HL-7):	Communication standard that guides the transmission of health-related information. HL7 allows the integration of various applications, such as bedside terminals, radiological imaging stations, hospital census, order entries, and patient accounting, into one system.
	Home Health Care and Remote Monitoring Systems:	Care provided to individuals and families in their place of residence for promoting, maintaining, or restoring health or for minimizing the effects of disability and illness, including terminal illness. In the Medicare Current Beneficiary Survey and Medicare claims and enrolment data, home health care refers to home visits by professionals including nurses, physicians, social workers, therapists, and home health aides. Use of remote monitoring and interactive devices allows the patient to send in vital signs on a regular basis to a provider without the need for travel.

I	Informatics:	The use of computer science and information technologies for the management and processing of data, information and knowledge. The field encompasses human-computer interaction, information science, information technology, algorithms, areas of mathematics, and social sciences.
	Interoperability:	The ability of two or more systems (computers, communication devices, networks, software, and other information technology components) to interact with one another and exchange data according to a prescribed method in order to achieve predictable results (ISO ITC-215). There are three types of interoperability: human/operational, clinical, and technical.
J		
K	Kiosk:	Specifically, designed computer system for accessing specific programs or search sites that is typically part of a structure designed to prevent theft or tampering and withstand unattended public use and promote privacy and security during use.
L	Licensure:	a restricted practice requiring a license, which gives a "permission to practice." Such licenses are usually issued in order to regulate some activity that is deemed to be dangerous or a threat to the person or the public or which involves a high level of specialized skill. (Wikipedia)
M	m-Health:	Practice of medicine and public health supported by mobile communication devices, such as mobile phones, tablet computers and PDAs for health services and information.
	Medical Codes:	A process of describing medical diagnoses and procedures using specific universal medical code numbers. States may select from a variety of HCPCS codes (T1014 and Q3014), CPT codes and modifiers (GT, U1-UD) in order to identify, track and reimburse for telemedicine services. (http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Delivery-Systems/Telemedicine.html)
N	Network Integrators:	Organizations specializing in the development of software and related services that allow devices and systems to share data and communicate to one another.
	Noise Cancellation:	Method for reducing unwanted sound during videoconferencing or other electronic audio transmission.
O	Originating Site:	Location of the Medicaid patient at the time the service being furnished via a telecommunications system occurs. Telepresenters may be needed to facilitate the delivery of this service. (http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Delivery-Systems/Telemedicine.html). Other common names for this term include spoke site, patient site, remote site, and rural site.

P	Protection of Personal Information Act (POPIA):	PoPI Act is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise the personal information in any way.
	Peripheral Devices:	Any device attached externally to a computer (e.g., scanners, mouse pointers, printers, keyboards, and clinical monitors such as pulse oximeters, weight scales).
	Personal Health Record (PHR):	Health record maintained by the patient to provide a complete and accurate summary of an individual's medical history accessible online.
	POTS:	Acronym for Plain Old Telephone Service.
	Presenter (Patient Presenter):	An individual with a clinical background (e.g., LPN, RN, etc) trained in the use of telehealth equipment who must be available at the originating site to "present" the patient, manage the cameras and perform any "hands-on" activities to complete the tele-exam successfully. In certain cases, a licensed practitioner such as an RN or LPN might not be necessary, and a non-licensed provider such as support staff, could provide tele-presenting functions. Requirements (legal) for presenter qualifications differ by location and should be followed.
R	Remote Monitoring:	Type of ambulatory healthcare where patients use mobile medical devices to perform a routine test and send the test data to a healthcare professional in real-time. Remote monitoring includes devices such as glucose meters for patients with diabetes and heart or blood pressure monitors for patients receiving cardiac care.
	Risk management system	Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters
S	Spoke Site:	Remote site where the patient is presented during telemedicine encounter or where the professional requesting consultation with a specialist is located.
	Standard:	A statement established by consensus or authority that provides a benchmark for measuring quality and that is aimed at achieving optimal results.
	Systemized Nomenclature for Medicine:	Clinical Terms (SNOMED CT): Provides core general terminology for EHRs and contains more than 311,000 active concepts with unique meanings and formal logic-based definitions organized into hierarchies. When implemented in software it can be used to represent clinically relevant information consistently, reliably and comprehensively as an integral part of producing electronic health records. (http://www.ihtsdo.org/snomed-ct/)

T	Telecommunications Providers (Telco):	An entity (the Federal Communications Commission in the US licenses Telcos) that provides telecommunications services to individuals or institutions.
	Teleconferencing:	Interactive electronic communication between multiple users at two or more sites that facilitates voice, video, and/or data transmission systems: audio, graphics, computer and video systems.
	Teleconsultation:	Consultation between a provider and specialist at distance using either store and forward telemedicine or real time videoconferencing.
	Telehealth and Telemedicine:	Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve patients' health status. Closely associated with telemedicine is the term "telehealth," which is often used to encompass a broader definition of remote healthcare that does not always involve clinical services. Videoconferencing, transmission of still images, e-health including patient portals, remote monitoring of vital signs, continuing medical education and nursing call centers are all considered part of telemedicine and telehealth. Telemedicine is not a separate medical specialty. Products and services related to telemedicine are often part of a larger investment by health care institutions in either information technology or the delivery of clinical care. Even in the reimbursement fee structure, there is usually no distinction made between services provided on site and those provided through telemedicine and often no separate coding required for billing of remote services. Telemedicine encompasses different types of programs and services provided for the patient. Each component involves different providers and consumers.
	Telematics:	The use of information processing based on a computer in telecommunications and the use of telecommunications to permit computers to transfer programs and data to one another.
	Telementoring:	The use of audio, video, and other telecommunications and electronic information processing technologies to provide individual guidance or direction.
	Telemetry:	Remote acquisition, recording and transmission of patient data via a telecommunications system to a healthcare provider for analysis and decision making.
	Telemonitoring:	The process of using audio, video, and other telecommunications and electronic information processing technologies to monitor the health status of a patient from a distance.
	Teleradiology and Picture Archiving and Communications Systems (PACs):	The electronic transmission of radiological images, such as x-rays, CTs, and MRIs, for interpretation and/or consultation.
U	Videoconferencing:	Real-time transmission of digital video images between multiple locations
V		
W		