Wesfarmers Health Telehealth Code of Practice

Critical criteria, key measures and evidence requirements

Introduction

Wesfarmers Health has developed the Telehealth Code of Practice (Code) to:

- Set industry standards, so that telehealth services operate with excellence, integrity and patient-centred care at its core;
- Provide a reference tool for organisations involved in telehealth or considering establishing a telehealth service;
- Promote continuous improvement in the quality of care offered to people accessing telehealth services; and
- Provide a framework and set criteria for the auditing process that leads to the accreditation of organisations delivering telehealth services.

The Code has been developed in alignment with the Australian Commission on Safety and Quality in Health Care (ACSQHC) National Safety and Quality Primary and Community Healthcare Standards (NSQPCHS). It outlines expectations and commitments across three key domains: Clinical Governance, Partnering with Consumers, and Clinical Safety. 18 criteria must be met to deliver best practice standards in telehealth.

The document outlines the critical criteria, key measures and evidence requirements that underpin compliance with the Code.

	Critical criteria	Measure	Evidence to show compliance
1	**Clinical Governance**		
1.1	**Governance, Leadership & Culture**		
	The telehealth service must demonstrate a strong clinical governance system and structure that drives a culture of safety, accountability and continuous improvement in the delivery of its healthcare services.	**A Clinical Governance Committee has been established** with clear terms of reference and defined responsibility for oversight of clinical quality, safety and patient outcomes. **A Clinical Governance Framework is in operation and maintained, setting the organisation's quality and safety goals, risk management processes,** and patient safety systems. **Clear clinical leadership roles are assigned**, including appointment of a Medical Director (however titled) who is responsible for practitioner oversight and setting clinical best practice standards.	- Clinical Governance Committee terms of reference and meeting minutes - Clinical Governance Framework - Clinical leadership and committee structures and reporting lines denoted in contracts/documentation, organisational charts and position descriptions - Position descriptions for all personnel incorporating patient safety and quality as part of their roles - Business strategy inclusive of patient safety and clinical governance activities, with key clinical metrics identified and monitored to measure patient safety

Australian Pharmaceuticals Pty. Ltd.
ABN 57 000 004 320

		Clear expectations are set to ensure that safety and quality care form part of all team members' roles within the telehealth service (clinical and non-clinical). **The business strategy prioritises safe and high-quality clinical care** that is communicated internally and externally. **Clinical indicators have been established** to measure and monitor key safety and quality areas, supporting ongoing improvements in care.	☐ Evidence of internal and external communications supporting commitment to patient safety and quality of care (eg memos to personnel and quality and safety statement published on websites)
1.2	**Patient Safety & Quality Systems**		
	The telehealth service must implement robust safety and quality systems that ensure safe, effective and evidence-based care, with a strong emphasis on continuous quality improvement and compliance with regulatory standards.	**Standardised care pathways and evidence-based treatment guidelines** are captured within the organisation's Quality Management System (however titled) and are easily accessible to all team members. **Structured escalation protocols are implemented**, which may include system forcing functions to escalate high-risk and critical presentations and transfer when emergency care is required (including transfer to hospital and/or welfare checks). **Safe prescribing guidelines** are documented and communicated to the workforce that recognises the scope of telehealth and appropriateness of medicines prescribed. **Critical information alerts and medication management systems** are established through electronic systems and protocols that flag allergies, medication interactions, and serious issues or diagnoses prominently in patient records to prevent errors during consultation or prescribing. **Fraud detection systems** are implemented to detect, prevent and respond to inappropriate use of telehealth services. This includes processes to confirm the patient's individual healthcare identifier (IHI) prior to consultation. **A clinical audit program** is in place that assesses clinical performance, identifies patient outcomes, and supports ongoing service improvements. **Independent/external assurance auditing** is undertaken to provide third-line oversight. **Structured clinical handover protocols are in place** to ensure safe and complete handover between clinicians, especially when care is transferred between practitioners or shifts (eg ISBAR tool).	☐ Clinical protocols and standardised care pathway documents, including safe prescribing guidelines ☐ Escalation flowcharts and clinical decision trees, emergency care protocols and processes ☐ Fraud detection tools and security policies ☐ Communication and documentation protocols (eg handover templates, clinical documentation policies and internal messaging systems) ☐ Audit program and review outcomes ☐ Minutes of governance and policy committee where review of screening tools/digital questionnaires are reviewed an updated accordingly in line with evidence-based standards

		Screening and assessment tools (including digital health questionnaires) are evidence-based, regularly reviewed to ensure best practice, and used to support practitioners in determining telehealth suitability and clinical risk.	
1.3	**Risk & Incident Management**		
	The telehealth service must have a clear risk management system in place to identify and reduce potential risks. It has plans to manage business disruptions and ensure services continue safely. All incidents, including near misses, are recorded, reviewed, and used to improve care. Serious incidents are appropriately investigated, and patients are informed through open disclosure, following national guidelines.	**A risk management framework is maintained,** and comprehensive risk assessments are routinely carried out to identify and implement appropriate mitigation strategies. **Business continuity and disaster recovery procedures and plans** are in place, and the workforce is trained to know what to do in the event of business interruption. **An incident management and reporting system** is in place and maintained to track, investigate and learn from clinical incidents and near misses. Incident management and reporting processes must be documented in a policy and should include clear accountability for reporting, review, investigation, close out and learning from incidents. **A standardised incident classification system is in use** to support effective management, investigation, escalation and reporting of incidents. This must include a process for external and mandatory reporting requirements. **A process and protocol for investigating high-risk, serious incidents are documented, which may consist of Root Cause Analysis (RCA) or Critical Case Review (CCR), as well as** corrective action implementation. **The service recognises open disclosure as best practice for transparent and accountable healthcare delivery.** The service adheres to the Australian Open Disclosure Framework to guide communication with patients following any clinical incidents.	☐ Risk Management Policy and Procedure, Risk Register (with evidence of regular updates and reviews) and Documented Risk Assessments (clinical, operational, technological) ☐ Records of risk mitigation plans ☐ Evidence of risk reporting to governance structures ☐ Business Continuity and Disaster Recovery plans ☐ Training records and drills (eg data hacking emergency response exercises) ☐ Communication protocols in the event of a disruption ☐ Incident Management Policy and Procedure ☐ Incident Reporting Forms or Incident Register (digital or manual), including examples of completed incident investigations and corrective actions ☐ Standardised incident classification matrix or taxonomy, with evidence of use in practice (eg classification on incident logs) ☐ Internal escalation and response thresholds ☐ Compliance with external reporting obligations (eg AHPRA, state health departments) ☐ Copies of mandatory reports (where applicable) ☐ Policy outlining the use of Root Cause Analysis (RCA) or Critical Case Review (CCR) ☐ Records of serious incident investigations and outcomes ☐ Open Disclosure Policy aligned with the Australian Open Disclosure Framework, templates for Open Disclosure discussions/letters, evidence of Open Disclosure training for clinicians, records of Open Disclosure communications (anonymised if needed for review) ☐ Clinical Governance Committee minutes showing review of: risk reports, incident trends; root cause findings, Corrective

			actions, quality improvement initiatives stemming from risk/incident reviews
1.4	**Clinical Performance & Effectiveness**		
	The telehealth service must ensure that clinical care is delivered by qualified, registered, and appropriately credentialed practitioners who operate within defined scopes of practice and are supported through ongoing performance monitoring and professional development. The organisation must monitor clinical performance metrics to ensure delivery of high-quality care. The telehealth service must submit data for external benchmarking.	**A formal practitioner credentialing and recredentialing process is in place** and ensures that: • All practitioners hold valid registration with AHPRA, with no restrictions, conditions or reprimands that would compromise safe practice; and • Skills checks, clinical assessment and reference checks are carried out. **Each practitioner's scope of practice is clearly defined** based on their qualifications, training and experience. **Practitioners are supported to work within their areas of competence, and escalation pathways are in place to manage cases that exceed** their scope. **Clinical performance is monitored** through regular activities, including peer review, clinical audits, performance appraisals, competency assessments, and continuing professional development (CPD). **Training programs are in place** that set mandatory learning. **Formal communication pathways have been established to provide updates and significant policy changes to the workforce**. **The workforce has the necessary tools, equipment and staffing to deliver high-quality care**. This includes training on data security, the use of appropriately configured systems, and secure access to the telehealth platform. **Clinical indicators and clinical effectiveness performance metrics are defined and monitored** and support ongoing patient safety and quality improvements. Indicators, at a minimum, include clinical incidents and medication safety (including prescribing errors). Clinical effectiveness metrics to include, at a minimum, consultation length and quality.	□ Practitioner credentialing records, including AHPRA registration verification reports □ Defined scope of practice documentation per practitioner role □ CPD logs, mandatory training compliance and performance review documentation □ Clinical Governance Committee meeting minutes □ Practitioner's escalation protocols □ Examples of communication to practitioners where major policy change has occurred/communication pathways used with the workforce □ Platform security training logs □ Clinical metrics dashboards, trend analyses and quality improvement reports □ Evidence of industry benchmarking participation or readiness

1.5	**Data Security, Management & Privacy**		
	The telehealth service must uphold the highest standards of data security and patient privacy by implementing robust systems, technology, and policies that ensure the confidentiality, integrity, and appropriate accessibility of patient health information.	**The organisation maintains ISO 27001 certification or equivalent** to demonstrate effective management of information security risks. **The service adheres to the Australian Privacy Act 1988 (Cth) & My Health Record Act and applicable state and territory legislation.** **The technology used for consultations, information storage, and communication is secure and suitable for clinical use.** Video conferencing and messaging platforms are encrypted and compliant with Australian Privacy and cybersecurity standards. **Practitioners understand their obligation to maintain privacy and confidentiality when conducting** consultations in a confidential, distraction-free environment that prevents unauthorised access to patient health information (audio or visual). **Mandatory cybersecurity training is in place** for all team members handling sensitive patient data. **Role-based access controls are in place** ensuring only authorised personnel can access sensitive data. **Incident response plans are in place for potential data breaches** aligned to the National Data Breach scheme. **Systems are in place to ensure that consultations can be resumed or rescheduled if technological issues occur.** **The telehealth service maintains a publicly accessible privacy policy on its website** that outlines how patient information is collected, used, stored and protected. This policy includes clear instructions on how patients can raise concerns or lodge complaints about privacy breaches, including contact details for submitting queries or concerns.	☐ Current ISO 27001 certification ☐ Information Security Management System (ISMS) documentation ☐ Risk assessment reports and mitigation plans, including penetration testing reports ☐ Privacy policy aligned with the *Privacy Act 1988 (Cth)*, *My Health Record Act*, and relevant state/territory legislation ☐ Policies and procedures established around access and release of patient medical record ☐ Documented privacy impact assessments ☐ Legal compliance registers ☐ Access control policy ☐ System access logs with audit trails ☐ Role matrix mapping users to system permissions ☐ Onboarding and offboarding checklists and processes ☐ Practitioner agreement/policy setting consultation environment standards ☐ Spot check/audit tools verifying compliance ☐ Practitioner onboarding training materials reflective of confidentiality and privacy standards and training records ☐ Privacy policy accessible via website

1.6	**Use of Artificial Intelligence in a telehealth service**		
	Telehealth services that integrate AI tools into clinical documentation or patient care workflows must do so in a responsible, transparent, and clinically governed manner. The use of AI may support—but never replace—clinical judgement.	**Processes and training are in place** to ensure AI-assisted clinical documentation is reviewed and edited by practitioners before being finalised. **AI tools are used only as decision-support aids**; clinical judgment remains the primary consideration. **There is transparent governance on AI tool selection, validation and ongoing compliance monitoring** and AI ethics is considered within its governance structures. **The telehealth service voluntarily adopts the Australian Voluntary AI Safety Standards to guide the responsible selection, implementation, and oversight of AI technologies.** **Patient consent protocols are in place** to ensure informed participation in AI-supported services. **AI tools used by the telehealth service comply** with the Privacy Act 1988 (Cth), the Health Records and Information Privacy Act. **Data security measures are in place** to ensure patient data processed by AI tools is encrypted in transit and at rest, with access restricted to authorised users.	☐ Clinical governance policy outlining the role of AI and the inclusion of clinician verification of AI-generated documentation ☐ Sample of audited clinical records showing evidence of clinician final review and sign-off ☐ Training records confirming clinician education on the AI scope of use ☐ Consent process configuration in the platform observed ☐ Audit trail from electronic health record showing consent documentation ☐ Contracts with AI vendors confirming legislative compliance ☐ Minutes from technology/ governance reviews
2	**Partnering with consumers**		
2.1	**Consumer engagement**		
	The telehealth service must demonstrate meaningful consumer engagement at both the individual practitioner and health service level. Practitioners actively involve patients in shared decision-making and care planning, while the telehealth service supports consumer participation in the design, evaluation, and continuous improvement of care, safety and quality systems.	**Culturally appropriate policies and procedures are in place that respect and integrate cultural practices and beliefs into healthcare provision.** **Practitioner training supports cultural safety and shared decision-making.** **The service incorporates input from consumers (eg consumer advisory groups) and patient feedback** to inform service design and drive ongoing quality improvement. **Implementation of the Australian Charter of Healthcare Rights** into telehealth policies is evident.	☐ Evidence of cultural awareness training/programs (including Aboriginal and Torres Strait Islander peoples) ☐ Health guides/facts sheets/decision aids that support patients with understanding clinical information ☐ Evidence of clinical work-flow prompts/templates for practitioners supporting shared decision-making ☐ Records of consumer co-design activities or committees ☐ Evidence of consumer feedback collection and resulting service improvements ☐ Consumer-facing materials (eg website) referencing the Healthcare Rights Charter

2.2	**Consumer choice**		
	The telehealth service must prioritise and facilitate informed consumer choice in care delivery, modality and medicine access.	**The service supports choice in mode of communication with practitioners (video, phone, asynchronous care)** where clinically appropriate to cater to the diverse needs of patients. **Processes are in place to allow patients to choose their preferred practitioner,** including options to book with the same practitioner for continuity of care or select the next available practitioner for timely access. **Patients are provided with options for how their medicines can be accessed or dispensed,** ensuring they are not restricted to a single, predetermined pathway and can exercise choice in line with ethical and legal standards.	☐ Booking system/app review that offers choice regarding practitioner, times, medicines dispensing/access
2.3	**Informed consent including financial consent**		
	Patients receive clear, upfront information about services, costs and billing arrangements, including Medicare and diagnostic costs, with consent processes embedded in workflows.	**Patients are clearly informed about their treatment and medicine options, including risks, benefits and costs, and consent is obtained and documented before care is provided.** **Consent workflows are embedded in the platform**, including consent for referrer correspondence, access to My Health Record and use of AI for clinical documentation. **Processes are in place to ensure costs of services (including cancellation fees and additional fees) are disclosed to patients before service delivery.** **Practitioners routinely discuss costs relating to treatment plans that result from a consultation (medications, investigations, follow-up).** **Interpreter access is available to meet patient needs** and maximise their ability to understand and make informed decisions about their care. **Pathology costs and potential gap payments are disclosed to patients upfront.**	☐ Samples of de-identified patient health records evidencing patient consent has been given and documented ☐ Evidence of consent disclosures in platform ☐ Examples of fee disclosure documents or online displays ☐ Interpreter access protocols ☐ Practitioner guidelines for informed financial consent ☐ Sample of patient records showing consent logged prior to service

2.4	**Consumer communication**		
	The telehealth service must ensure communication with patients is clear, culturally appropriate and tailored to their needs and preferences. Consumers must be provided with the necessary information in a format they can understand, enabling them to make informed decisions about their care. The service must also provide accessible information about how to access care, what services are available, associated costs, after-hours options and how to provide feedback or complaints.	**Communication with patients is based on needs, preferences and health literacy,** so the information being conveyed is easily understood. **Pre-consultation tech readiness information is provided to the patient** to ensure a seamless consultation. **Patients are informed that they may need in-person care if the practitioner considers the telehealth consult alone to be inappropriate.** **Communication addresses next steps in care**, including prescriptions, test requests or follow-up appointments. **Patients can access details about service scope, hours, costs, eligibility, access points and after-hours alternatives via the website/app.**	☐ Practitioner training materials on health literacy and person-centred communication ☐ Evidence of pre-consultation email/ SMS/ in-app communication sent to patients outlining tech setup and access instructions ☐ Appointment confirmation processes containing an in-person care disclaimer ☐ Webpage or app screen showing service information (scope, hours, costs, access) ☐ Patient survey results evidencing user experience and simplicity of information
2.5	**Feedback & complaints**		
	The telehealth service must have accessible, transparent and responsive feedback and complaints mechanisms that support continuous improvement and uphold consumer rights.	**Feedback is regularly sought from patients/consumers and the workforce** regarding their experience and outcomes to support continuous quality improvement. **A complaints handling policy is in place** that outlines clear procedures for managing complaints, including timeframes for resolution, escalation pathways and team member responsibilities. **Complaints management is incorporated into workforce training** and processes to ensure consistent and appropriate responses and resolution. **The complaints process is publicly accessible via the website**, so patients and carers are informed on how to lodge a complaint and what to expect. **Feedback is regularly sought from the workforce on its safety and quality systems** to ensure they are effective, embedded in day-to-day practice and understood.	☐ Evidence of patient satisfaction surveys, focus groups or patient research results ☐ Summary reports tabled at governance meetings ☐ A documented and approved complaints management policy, with defined resolution timeframes, escalation pathways, and role responsibilities ☐ Complaints log/register showing dates, categories, actions taken, and resolution status ☐ Evidence of periodic review of complaints trends and lessons learned incorporated into service improvements ☐ Live link to the complaints policy or complaints lodgement page on the organisation's website ☐ Evidence of complaints resolution training modules and training logs (eg workshop attendance logs, e-learning completions) ☐ Use of Feedback Loops evidenced: Demonstrating "you said, we did" changes — where feedback from workforce evaluations leads to real updates in protocols or systems

Wesfarmers Health Telehealth Code of Practice

Critical criteria, key measures and evidence requirements

3	**Clinical Safety**		
3.1	**Clinical appropriateness of treatments and services**		
	The telehealth service must ensure that all treatments and services are clinically appropriate, evidence-based, and aligned with patients' broader health needs. This includes comprehensive clinical assessments prior to initiating treatment, clear documentation of clinical rationale, condition-specific protocols for high-risk or narrow-scope services, and systems for regular review, escalation and referral. Services must safeguard against over-servicing and ensure care is delivered in accordance with the Medical Board of Australia's Code of Conduct.	**Health practitioners assess the clinical appropriateness of each consultation**, ensuring services align with the patient's condition, medical history, and best-practice guidelines. **Clinical justification for all diagnoses, investigations, treatments, and prescribed medicines is clearly documented** in the patient's electronic health record. **Patients are informed of treatment options, limitations of telehealth, and the reasons for any referrals or changes in care pathways.** **Standardised protocols and regular auditing are in place to prevent over-servicing or prescribing** where clinical benefit is not demonstrated. **Referral and escalation procedures are in place and followed** when a patient's condition is outside the scope of safe telehealth management. **For condition-specific models of care (e.g. weight management, medicinal cannabis, skin conditions or mental health), real-time consultations, red flag screening, defined exclusion criteria, and scheduled clinical reviews are embedded into care protocols.**	☐ Sample patient records showing clinical justification for diagnoses, prescriptions, investigations, and treatment options discussed. ☐ Audit logs or reports monitoring over-servicing, prescribing patterns, and protocol adherence. ☐ Referral and escalation policies and documented examples of their use in clinical records. ☐ Condition-specific protocols outlining red flag screening, clinical exclusion criteria, synchronous review schedules, and follow-up processes. ☐ Practitioner training materials covering condition-specific care pathways and appropriateness criteria. ☐ System prompts or workflows demonstrating required real-time consultation intervals in targeted service models.
3.2	**Diagnostics and results**		
	The telehealth service must maintain a robust, timely and clinically accountable diagnostics and results management system that ensures all results and clinical correspondence are reviewed, actioned and followed up in accordance with clinical best practice standards and aligns with the RACGP	**Standardised protocols are in place for timely review and follow-up of all investigation results,** and the workforce is trained in the follow up process, communication with patients about results and appropriate recording of patient discussions and results. **Integration with pathology and imaging services is in place** to ensure correspondence, and results are effectively incorporated into the patient's electronic health record.	☐ Diagnostics and Results Management Policy (incl. review timelines, responsibilities, and documentation requirements) ☐ Clinical protocols outlining delegation of results in clinician absence; notifying public health units of notifiable results; escalating urgent findings after hours and expected timeframes for follow-up ☐ Recall system documentation including recall register/logs and contact process for urgent and non-urgent results

	Good Practice Standards for follow-up care.	**A designated role (eg pathology nurse) has been appointed to monitor and have oversight of the recall process** and ensure appropriate action on results as an extra safety net. **A process is in place to delegate result review when the ordering clinician is unavailable**. **A process is in place to notify state public health units of notifiable results in a timely manner.** **A structured recall system is in place to identify and recall patients with significant results,** including documentation of recalls and defined responsibilities for clinical vs non-clinical roles is clear. **Emergency escalation protocols are in place for high-risk or life-threatening results received outside of hours,** including contact procedures; on-call practitioner details shared with diagnostic providers; and agreements with after-hours care services. **Clinically significant or complex results are delivered via synchronous telehealth consults**, with in-person follow-up arranged as needed.	☐ Evidence of documentation of patient contact attempts in patients record ☐ Role definitions for clinical vs no clinical team members ☐ Technology system overview showing diagnostic integration capability ☐ Audit logs or system screenshots demonstrating timely result review ☐ Sample patient records (de-identified) showing documented result review, patient communication and follow-up actions
3.3	**Medication Safety**		
	The telehealth service must have clear protocols and medication safety systems for prescribing in both synchronous and asynchronous models. It defines medication exclusions based on telehealth limitations, and ensures practitioners work within their scope, use current medication histories and support safe, person-centred care with appropriate follow-up and oversight.	**Prescribing protocols and approved medication lists are in place**, identifying medications and limits that are suitable for telehealth and those excluded. **Medication exclusions are defined for asynchronous care**, including restrictions on high-risk medicines, Schedule 8 and Schedule 4 Restricted drugs in asynchronous models. **Prescribing practices align with jurisdiction-specific legislation and practitioners have access to state-based prescription monitoring programs**. **The electronic health record is designed so a practitioner can easily identify previously prescribed medications, patient histories and critical alerts, and ensures that practitioners can collect a full medication history** including allergies, over-the-counter medications and supplements. **Clinical decision support tools are integrated with the electronic health record**, to flag interactions, contraindications and allergy risks. **System processes are designed (including forcing functions) to ensure real-time consultations occur before prescribing new medications.**	☐ Documented prescribing protocols and approved medication list specific to telehealth ☐ Copy of asynchronous prescribing catalogue ☐ User guides showing practitioner access to state prescription monitoring programs ☐ Review of electronic health record showing mandatory medication history fields and patient medication summaries ☐ Evidence of integration with drug database/drug interaction checker ☐ System logic or workflow diagram showing forced requirement for synchronous consult before issuing new script ☐ Medication safety audit report or dashboard ☐ Documented protocols for reporting ADRs to the TGA and internal documentation ☐ Practitioner training records or completion certificates for prescribing protocols ☐ Paediatric prescribing protocol or electronic health record support tool with weight-based dosage calculators

		Medication prescribing and safety risk areas are audited to identify problems and support quality improvements. **Adverse drug reaction reporting processes are in place**, enabling practitioners to report to the TGA and document incidents. **Escalation pathways are established** to manage and follow up serious drug reactions or medication-related safety concerns. **Prescribers are supported to work within their scope of practice**, and training on prescribing protocols is in place. **Where paediatric prescribing is carried out, systems and processes are in place to support accurate and safe prescribing.**	
3.4	**Antimicrobial stewardship**		
	Where a telehealth service prescribes antimicrobials, it must uphold responsible, evidence-based antimicrobial stewardship practices to support appropriate use and minimise the risk of antimicrobial resistance.	**A documented antimicrobial stewardship policy and training is in place** and aligned with the Antimicrobial Stewardship Clinical Care Standard and current Therapeutic Guidelines: Antibiotic (eTG). **Regular audits of antimicrobial prescribing practices are conducted**, with documented actions taken to address non-compliance, overuse or inappropriate prescribing.	☐ Antimicrobial Stewardship Policy aligned with current Therapeutic Guidelines and Clinical Care Standards ☐ Training materials/record of education of new practitioners on responsible antimicrobial use ☐ Audit reports and corrective actions documenting antimicrobial prescribing reviews and outcomes
3.5	**Medical Certificates**		
	The telehealth service must have policies, procedures, training programs and controls in place for issuing medical certificates via synchronous and asynchronous pathways. The telehealth service leverages technology to enhance patient safety, support clinical decision-making and uphold best practice.	**Synchronous and asynchronous issuing protocols** are clearly defined, with certificates only issued when clinically appropriate and within scope. **System safeguards** ensure medical certificates meet ethical and professional standards, including restrictions on duration, prevention of backdating, and features that enable medical certificate verification. **Screening and escalation mechanisms are in place** (such as integrated mental health screening) to ensure at-risk patients are directed to real-time consultations.	☐ Documented medical certificate protocols for synchronous and asynchronous medical certificate issuance ☐ Evidence of system safeguards that ensure certificates meet ethical standards, with restrictions on duration, prevention of backdating, and verification features (eg QR codes). ☐ Evidence of integrated screening processes (eg mental health screening) and escalation mechanisms to real-time consultations for at-risk patients ☐ Practitioner training resources on medical certificate issuing and training logs/records

		Mandatory training and clinical policies guide practitioners on certificate limitations, including strict prohibitions (inc. workers' compensation certificates) and guidance on recovery periods. **Practitioners have appropriate access to patient records to** support informed clinical decision making and appropriate documentation when issuing certificates. **Compliance oversight** is maintained through audit logs and regular audits of issued certificates to monitor adherence to legal and clinical standards.	☐ Evidence that practitioners have access to the necessary patient information, including medical and My Health records (if consented), to support decision-making ☐ Audit logs of issued certificates and evidence of regular audits to ensure compliance with legal and clinical standards
3.6	**Communicating for safety**		
	The telehealth service must have robust communication processes in place to ensure patient safety and continuity of care, encompassing accurate patient identification, effective referral and multidisciplinary collaboration.	**Systems are in place to accurately match patients to their healthcare and practitioners, and team members follow mandatory patient ID checking protocols** (including use of three patient identifiers) to verify a patient before providing care. **Structured handover processes are in place when transferring care** within the service, referring patients for in-person care, and transferring patients to emergency care. **Secure systems are enabled to support appropriate follow-up arrangements and information sharing of correspondence, referrals, results, prescriptions and advice with other providers if clinically indicated.** **Integration with My Health Record** is enabled to give practitioners access to critical health information, supporting safer care—where patient consent is provided. **Assessment of telehealth suitability** occurs prior to and throughout consultations and escalation to in-person care or clinical handover occurs when required. The system and workflows are designed to support assessment of telehealth suitability.	☐ Policy or protocol outlining use of three patient identifiers and audit record showing compliance with patient ID checks ☐ Documented handover procedure or handover template used for referrals, in-person transfers, and emergency escalation ☐ Review of secure messaging or clinical correspondence systems used for referrals, results, and follow-up ☐ System integration documentation or usage log demonstrating access to My Health Record (with patient consent workflows) ☐ Workflow diagram or clinical protocol showing telehealth suitability assessment checkpoints
3.7	**Emergency response and escalation**		
	The telehealth service must have clearly defined, system-enabled emergency response and escalation protocols to promptly identify and act on clinical deterioration so that patients at risk receive timely, appropriate care.	**Documented escalation protocols are in place** that define emergency indicators, risk thresholds (eg self-harm, worsening symptoms), and required actions for practitioners. **System-enabled escalation features have been developed** (such as automated alerts, forcing functions, and real-time monitoring) to trigger escalation/ rapid review for deteriorating or high-risk patients. **Integrated systems are in place to support rapid access to emergency services for urgent interventions**, including ambulance, police, Lifeline.	☐ Documented emergency escalation protocol outlining risk thresholds and required actions ☐ System documentation showing escalation alerts or forcing functions for high-risk patient scenarios ☐ Review of workflows or integration pathways with external emergency services (eg 000, Lifeline) ☐ Sample incident report or incident log from an emergency escalation reviewed by clinical leadership

		Incident reporting mechanisms are in place for all emergency escalations, to ensure oversight and review by senior clinical staff. **Practitioner training and onboarding occurs** that includes escalation protocols, use of system alerts, responsibility for initiating referrals to emergency services and appropriate documentation for transfer. **Audit and review systems are in place** to evaluate emergency responses and support continuous improvement in safety and escalation practices.	☐ Training log or onboarding materials covering emergency protocols, escalation responsibilities, and documentation requirements ☐ Most recent audit or review summary of emergency escalations and improvement actions taken
4	**Compliance obligations**		
4.1	**Licensing & approvals**		
	The telehealth service must comply with statutory and regulatory requirements, including approvals for licences dependent on the nature of the services provided.	Health service-specific licences and approvals are current, documented, and compliant with all relevant federal, state and territory legislative and regulatory requirements for delivering telehealth services.	☐ Records of relevant licenses/permits
4.2	**Advertising compliance**		
	The telehealth service must ensure that all advertising and promotional materials comply with relevant national and state laws and guidelines.	Processes are in place (including legal review where appropriate) to ensure advertising on the service's website and other promotional materials comply with the Health Practitioner Regulation National Law (as in force in each state and territory), the Australian Health Practitioner Regulation Agency (AHPRA) Guidelines for Advertising a Regulated Health Service, the Therapeutic Goods Advertising Code, and other applicable consumer protection laws.	☐ Evidence of review process of material and website content