TELEHEALTH

MEDICO-LEGAL ASPECTS OF TELEHEALTH SERVICES FOR VICTORIAN PUBLIC HEALTH SERVICES

MARCH 2015

Michael Regos
Partner
DLA Piper Australia
140 William Street
(PO Box 4301)
Melbourne VIC 3000
Australia
Tel: +61 3 9274 5000
Fax: +61 3 9274 5111

TABLE OF CONTENTS

INTRODUCTION

Telehealth is one key future innovative model for the provision of medical services. Telehealth has the potential to bring significant benefits for both patients and medical practitioners.

Telehealth will provide patients in rural and remote communities with greater access to, and greater choice of, medical service providers. Delivery of health services via telehealth will reduce the expense and disruption of travel for patients, while also supporting the rural health workforce to provide high-quality care. Telehealth will facilitate the sharing of knowledge between health service providers in different geographical locations, as well as across areas of speciality. Health professionals will undoubtedly benefit from increased peer support, training and education options.

No Australian State or Territory yet has a fully implemented telehealth system. A significant barrier to a widespread uptake of telehealth is the medico-legal uncertainty that surrounds the implementation of such a system. Indeed, there are a number of important medico-legal risks that must be addressed. However, provided the risks are identified, acknowledged and dealt with appropriately, this should not be a barrier to a successful Victorian telehealth system.

The Victorian Department of Health and Human Services (**the Department**) has contracted DLA Piper to prepare this document to outline the medico-legal aspects of using telehealth technologies (i.e. including but not limited to videoconferencing and medical image exchange) to deliver or receive medical advice and services from other hospitals and specialist medical services within Victoria. It is limited to the discussion of the Victorian laws and relevant national legislation that also applies to Victorian health services. It is beyond the scope of this document to more fully consider the legal frameworks of other jurisdictions, and suggests that health services that have entered into arrangements with hospital and health service providers in other states and territories or internationally to provide or receive medical services using telehealth should receive legal advice on the laws that apply to the specific circumstances.

This document recognises that medico-legal risk is a reality for all health care professionals, but that if it is understood and managed it can be controlled. Clinicians and nurses who provide services using telehealth are already skilled and capable of providing care of an appropriate standard. The provision of training, clinical guidelines and support for GPs, nurses, hospitals and health services to collaborate and agree on their roles and how they will manage the delivery of health services using telehealth are all expected to assist significantly with the management of medico-legal risk. In particular, improved documentation and communication are key risk management tools.

This document outlines some of the legal issues that clinicians already engaged in telehealth services have raised and identified as areas of concern among colleagues. It focuses on the duty of care and the management and protection of individuals privacy and health records, both of which raise concerns among those that are practicing telehealth.

This document is provided as a resource only. Nothing in this document should be taken to be legal advice from the Department of Health and Human Services, or a direction or recommendation from

the Department. The Department does not endorse and has not approved the information in the document. The Department and the State of Victoria disclaim all liability for the accuracy or suitability of the information in the document. Health service providers and clinicians should seek independent legal advice about any medico-legal matters relating to telehealth.

The Australian legal system

The legal system in Australia is based on legislation and common law.

Legislation forms the framework of the law and exists in two forms:

- statutes, or Acts; these are made by Parliament, both at Commonwealth and State levels; and
- delegated or subordinate legislation, made under the Acts (i.e. regulations, rules); these are made by individuals or bodies authorised to do so by Parliament.

Legislation has supremacy over common law. There is a plethora of legislation which is relevant to health care professionals, some of which will be discussed in this document.

Common law is essentially judge-made law (case law) and is used to interpret common legal principles as well as legislation. Case law creates a precedent in the law so findings of the court will be influenced by similar cases previously decided. The precedent effect of case law can cross different jurisdictions, so for example the finding in an English case may have bearing on an similar Australian case.

The law is fluid, and ever changing. Particularly in the field of medical law, where the law must keep pace with scientific and socio-political developments, new cases will always be presenting before the courts. Although it can be difficult to predict with any certainty what decision a court will make when faced with a novel situation, there are some common principles that apply to the law of negligence which, when understood, provide a sound basis for managing medico-legal risk.

SCENARIOS

The law applicable to telehealth can best be illustrated by applying to likely scenarios. In the course of this guide, illustrations will be given of circumstances of how the law is applied to four factual scenarios. Although the facts are specific to treatment for an orthopaedic injury, they are equally applicable to any condition. The scenarios are:

- A rural health service seeks advice directly from a tertiary (or regional or subregional) health service.
- A tertiary (or regional or subregional) health service provides advice directly to the patient of a rural health service.
- A private specialist provides advice directly to a rural health service about the rural health service's patient.
- A private specialist provides services directly to a patient referred to it by a rural health service.

There is no question that telehealth services may be beneficially utilised in a myriad of factual circumstances and to deal with varying health issues. However, for the purposes of this guide, it will be helpful to identify four examples of scenarios in which telehealth might commonly be used. It matters not in any of the scenarios whether the patient is an admitted or non-admitted patient of the host health service. These scenarios are referred to throughout this guide and are used to better explain the legal framework and differing responsibilities and obligations of each of the health services and individuals involved in the delivery of a health service via telehealth. The scope of this guide will be kept within the scope of these four factual scenarios.

Scenario 1: A rural health service seeks advice directly from a tertiary (or regional or subregional) health service

A public patient attends a rural health service with a spinal fracture. An x-ray is taken. The rural health service considers it would benefit from the advice of a specialist orthopaedic surgeon in order to treat the patient. In the patient's absence, the treating doctor at the rural health service contacts a tertiary (or regional or subregional) health service and sends the patient's x-ray to the tertiary health service via telehealth facilities and a specialist from the tertiary health service advises the doctor at the rural health service as to the best course of treatment.

In this scenario, the rural health service is seeking advice directly from the tertiary health service. The patient is not present in any consultation with the telehealth provider (the tertiary health service) and therefore is not the recipient (albeit the beneficiary) of the telehealth service.

Scenario 2: A tertiary (or regional or subregional) health service provides advice directly to the patient of a rural health service

A public patient attends a rural health service with a spinal fracture. The rural health service considers it has insufficient expertise to treat the patient and so informs the patient. With the patient

in the room, the rural health service contacts a public tertiary (or regional or subregional) health service seeking a specialist orthopaedic surgeon at the tertiary health service to consult directly with the patient via telehealth facilities.

In this scenario, the tertiary health service is providing the telehealth service directly to the public patient. The rural health service is effectively referring the patient to the tertiary health service although it may assist by performing specific tasks at the direction of the tertiary health service.

Scenario 3: A private specialist provides advice directly to a rural health service about the rural health service's patient

A public patient attends a rural health service with a spinal fracture. An x-ray is taken. The rural health service considers that it would benefit from the advice of a specialist orthopaedic surgeon in order to treat the patient. The rural health service has a preference for one particular private specialist orthopaedic surgeon. The particular specialist operates as a visiting medical officer at a public tertiary health service but not the rural health service. The rural health service seeks advice directly from the specialist (rather than from the tertiary health service). The x-rays are sent to the specialist via telehealth facilities and the specialist provides advice to the rural health service via telehealth facilities. Staff at the rural health service may assist the tertiary specialist conducting the assessment by reporting vital signs and undertaking specific actions at the direction of the tertiary specialist.

In this scenario, the specialist orthopaedic surgeon is providing telehealth services directly to the rural health service. The patient is not the recipient (albeit the beneficiary) of the telehealth service.

Scenario 4: A private specialist provides services directly to a patient referred to it by a rural health service

A public patient attends a rural health service with a spinal fracture. The rural health service considers it has insufficient expertise to treat the patient and so tells the patient. The rural health service has a preference for one particular private specialist orthopaedic surgeon and gives the patient the option of becoming a private patient of the surgeon (and thus be billed by the surgeon) or being referred to another public health service. The patient elects to engage the surgeon. The rural health service telephones the surgeon who agrees to consult with the patient via telehealth. With the patient in the room, the rural health service contacts the surgeon via telehealth facilities in order for the surgeon to consult directly with the patient. Staff at the rural health service may assist the remote specialist conducting the assessment by reporting vital signs and undertaking specific actions at the direction of the orthopaedic surgeon.

In this scenario the surgeon is providing the telehealth services directly to the patient. The rural health service may assist in performing specific tasks at the direction of the tertiary health service.

REGULATORY BODIES

Key Points

- All health practitioners in Australia must have a current registration with the Australian Health Practitioner Regulation Agency (**AHPRA**).
- AHPRA is supported by 14 national boards that are responsible for regulating 14 health professions. The boards manage the registration of practitioners and investigations into professional conduct.
- There is no "Telehealth Board of Australia". Telehealth providers are subject to regulation by AHPRA and their relevant board.
- The Health Services Commissioner is a Victorian statutory authority responsible for dealing with complaints about health service providers (including health services provided by telehealth), disclosure of health information and access to health information.

The laws, regulations and regulatory bodies governing medical practitioners who practice via telehealth are the same as those who do not practice via telehealth.

A health practitioners' legal right to practice is subject to a number of forms of regulation. In Victoria, the *Health Practitioner Regulation National Law (Victoria) Act 2009* (**the National Law**) provides the legislative framework for the national scheme in Victoria.

As a minimum, all health practitioners in Australia must have a current registration with the Australian Health Practitioner Regulation Agency (**AHPRA**). Medical practitioners are also required to be registered by the Medical Board of Australia and a provider and prescriber number from Medicare Australia. The latter provides the practitioner with patient access to the Medicare and Pharmaceutical Benefits Schemes.[1] Medical practitioners may also have a specialist registration with AHPRA. Any practitioner who holds themself out as being a specialist in any given field (whether by virtue of their title or otherwise) is required to have specialist registration.[2] An individual who knowingly or recklessly uses a specialist title may face a penalty of up to $30,000. In the case of a body corporate, the penalty may be up to $60,000.[3]

AHPRA

AHPRA's operations are governed by the National Law. AHPRA supports the 14 national boards that are responsible for regulating the 14 health professions within the scope of the National Law, being the:

---

[1] http://docs.health.vic.gov.au/docs/doc/F75634AE22D42207CA25790D001A379F/$FILE/credentialling-and-defining-scope-of-clinical-practice-2011-update.pdf.

[2] *Health Practitioner Regulation National Law (Victoria) Act 2009*, section 115(1).

[3] Ibid.

- Aboriginal and Torres Strait Islander Health Practice Board of Australia;
- Chinese Medicine Board of Australia;
- Chiropractic Board of Australia;
- Dental Board of Australia;
- Medical Board of Australia;
- Medical Radiation Practice Board of Australia;
- Nursing and Midwifery Board of Australia;
- Occupational Therapy Board of Australia;
- Optometry Board of Australia;
- Osteopathy Board of Australia;
- Pharmacy Board of Australia;
- Physiotherapy Board of Australia;
- Podiatry Board of Australia; and
- Psychology Board of Australia.

AHPRA supports the national boards, manages the registration and renewal processes for health practitioners and students around Australia and works with the Health Services Commissioner in Victoria (and the various Health Complaints Commissions in the other States and Territories) to ensure the appropriate organisation deals with community concerns about health practitioners. AHPRA also manages investigations into the professional conduct, performance or health of registered health practitioners in all Australian jurisdictions except New South Wales (where this is undertaken by the Health Professional Councils Authority and the Health Care Complaints Commission) and Queensland (where this is undertaken by the Queensland Health Ombudsman, as of 1 July 2014).

There is no "Telehealth Board of Australia" or an equivalent. Telehealth providers will remain subject to regulation by AHPRA and their relevant Board. For example, a psychologist consulting a patient via telehealth will remain subject to regulation by the Psychology Board of Australia. The complaints procedure in relation to complaints about the provision of telehealth services will be the same as that for complaints about the provision of any other health service.

AHPRA does not impose registration or renewal requirements upon telehealth providers that are any different or more rigorous than those requirements for practitioners not wishing to practice via telehealth. However, if more onerous requirements were to be developed, presumably AHPRA would likely still be the body responsible for regulating these requirements.

Health Services Commissioner

The Health Services Commissioner (**HSC**) is an independent Victorian statutory authority that is responsible for dealing with complaints made about health service providers, disclosure of health information and access to health information.

The HSC has jurisdiction to deal with complaints about doctors, hospitals, dentists, pharmacists, physiotherapists and other providers of health services, or any person or organisation that collects, holds or discloses health information. As such, complaints made against a telehealth provider will be dealt with by the HSC in the same manner as if the practitioner or health service provider was providing the health service in a traditional, face-to-face consultation.

The Victorian HSC has jurisdiction to hear complaints about any treatment that was received by a patient in Victoria. In other words, the HSC will be able to hear any complaint about treatment provided via telehealth so long as those services were received in Victoria. This will be the case whether or not the telehealth provider was providing the services from Victoria or interstate.

AHPRA and HSC both play crucial roles in regulating the medical profession and the practice of medicine. They operate hand-in-hand while having distinct roles.

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (**OAIC**) is responsible for reporting to the Attorney-General on how public sector information is collected, used, disclosed, administered, stored and accessed. It is responsible for exercising the powers conferred by the *Privacy Act 1988* (Cth).

The nominated Commonwealth agency (currently the OAIC) has various enforcement and investigative powers in respect to the personally controlled electronic health record (**PCEHR**) system. The OAIC receives referrals directly from the HSC in relation to such matters.

RISKS ASSOCIATED WITH TELEHEALTH SERVICES

Key Points

- Limitations of telehealth. The greatest risk for telehealth providers and host providers is misdiagnosis.
- Additional risks particular to telehealth are also potential liabilities arising from inferior equipment and technology and the storage of images.

Risk management and other legal requirements

Risks can be minimised by health services:

- adopting a policy of open disclosure.
- implementing appropriate and adequate incident reporting guidelines, such as the Victorian Health Incident Management Policy. If a notifiable event occurs, the telehealth provider and host provider should communicate as to who will report the event.
- When required to perform a root cause analysis (**RCA**), the telehealth provider and the host provider should work collaboratively to complete the RCA.

The implementation of telehealth systems brings potential notable risks for host providers, telehealth providers and patients alike. Once identified, these risks can be effectively managed and the benefits of telehealth can be realised.

RISKS FOR MEDICAL PRACTITIONERS

The risks for medical practitioners engaging in telehealth are most likely to fall into the categories of litigation risk or reputational risk. Litigation risks may arise from misdiagnosis, inappropriate reassurance about symptoms of a condition or a failure to properly refer a patient to another health care provider. The risks of misdiagnosis, for example, are likely to be heightened in the context of providing a health service via telehealth because of the inherent limits of the clinical assessment.

Reputational risks may be secondary to litigation, whether that is a civil claim or in a coronial inquiry. Provided that appropriate procedures are followed and the telehealth provider engages in best practice as would be required in a face-to-face consultation, there is unlikely to be significant reputational fallout attributed to the fact that the service was delivered by telehealth.

Both litigation and reputational risks are further minimised by requirements that telehealth providers be credentialed appropriately and their scope of practice limited to that which is appropriate.

RISKS FOR PATIENTS

Risks for patients are likely to arise with respect to the quality of the care they receive via telehealth. This may or may not be a reflection of the competence or capabilities of the medical practitioner or other health professional providing telehealth services. It is more likely that risks for patients arise

out of the limitations in technology, especially in the early stages of the implementation of telehealth and the inability to do a hands-on assessment, for example, to palpate for swollen lymph nodes or to auscultate the lungs.

LIABILITY RISKS

Whenever a health service is provided there is a liability risk. That risk is that the service provided might be delivered negligently and cause harm as a consequence. In telehealth, whether at law the service is deemed to have been provided negligently and thus compensable depends upon whether the health service delivered in accordance with reasonable standards. This applies equally to telehealth and non-telehealth services.

As discussed in the "*Duty of Care*" section of this guide, a health service and health practitioners each owe a duty of care to the patient to exercise reasonable skill and care when advising and treating patients.

Both the host provider (the organisation or person the patient attended for treatment) and the telehealth provider (the organisation or person providing health services remotely via technology) owe a duty of care.

Misdiagnosis

When providing health services by telehealth, the greatest liability risk relates to misdiagnosis. The inability to perform a hands on examination can, in some instances, make diagnosis more difficult (for example, the inability to palpate lymph nodes). A health practitioner will have discharged their duty to take reasonable care if they take into account the limits of the technology when making the diagnosis or recommending treatment.

The limitations of telehealth might more often result in the making of alternative and provisional diagnoses, with the alternatives to be excluded by hands on examination at the host site. In that situation, there are liability risks for both the telehealth provider (the provider of the initial advice and differential diagnoses) and the host provider (who performs the examination to exclude the alternative diagnoses to arrive at a final diagnosis).

Liability arising out of inferior equipment and technology

There are potential liability risks associated with the state and quality of the equipment by which the telehealth services are provided.

There are no prescriptive laws in Victoria as to the type and standard of equipment that must be used when providing services via telehealth. Nevertheless, it is established law that where services are provided they must be provided to a standard that the person receiving them is reasonably entitled to expect. Accordingly, if telehealth services are to be provided, and if the quality of the service is dependent on the quality of the equipment, the equipment used must be fit for the purpose it is being used. For example, if a neurosurgeon is asked to interpret a CT scan taken at another site, the image

must be transmitted from the host provider and reproduced at the telehealth provider's end with acceptable clarity to enable the neurosurgeon to provide an informed opinion. If it is not, the neurosurgeon might (and perhaps should) decline to give an opinion. If an opinion is given and is wrong and the technology is deemed unfit for purpose, then liability will arise. There will however be exceptions where the urgency of the situation and limited available resources make the use of suboptimal technology reasonable in some circumstances. In those instances, a health practitioner will not be liable for an error made with the (suboptimal) equipment available if there were no other practical means and if the service provided was reasonable within the limits of the equipment and resources.

Storage of Images

There are potential liability risks arising out of the keeping, management and storage of images by telehealth by way of breaches of confidentiality (see the "*Health Record Management and Data Transmission and Storage*" section of this guide).

Minimising Risks

Liability risks for organisations and health professionals can be reduced by appropriate risk management strategies (see the "*Risk Management*" section of this guide) and the financial consequences by insurance (see the "*Insurance*" section of this guide).

RISK MANAGEMENT AND OTHER LEGAL REQUIREMENTS

There are a number of ways in which health practitioners providing and requesting telehealth services can reduce the risks to patients, and reduce the risk of consequent litigation and reputational fallout.

Obtaining valid consent to treatment

Obtaining valid consent to provide medical treatment is a standard risk management tool (and legal requirement) in all forms of medical practice. See the "*Informed Consent*" section of this guide for more detail.

Keeping accurate and contemporaneous records

Health practitioners and health organisations should keep accurate and contemporaneous records as a matter of risk management and best practice. Every observation, decision and communication should be recorded accurately and contemporaneously to minimise the risk of miscommunication or error, and therefore to minimise the risk of adverse events occurring. Accurate records also provide documentary evidence in the event that a complaint, claim or investigation is made.

Notes should be clear, legible and dated accurately. The start and end times of consultations and procedures should be recorded, as should all elements of the decision making process.

As discussed in the "*Medical Record Management and Data Transmission and Storage*" section of this guide, the responsibility for management of a patient's health records differs according to the particular telehealth arrangement. Although it is desirable for all practitioners involved to keep accurate and contemporaneous records, the responsibility for doing so will also ultimately differ according to the telehealth arrangement.

In Scenarios 1 and 3[4], both the host provider and the telehealth provider should keep records of their discussion. The host provider will need to rely upon these notes in order to treat the patient and the telehealth provider may need to rely upon these in the event that it is later alleged that the advice given was inappropriate.

Similarly in Scenarios 2 and 4[5], both the host provider and the telehealth provider should take accurate and contemporaneous notes and keep these records. If there is no suitable practitioner available at the host organisation to do so, the host provider and the telehealth provider should enter into an arrangement by which the telehealth provider agrees to send the host provider a copy of their records of the consultation. The telehealth provider's notes should be added to the host provider's file for completeness.

Open disclosure

The National Safety and Quality Health Service Standards recommend that health service organisations should implement open disclosure policies. The essential elements of open disclosure are outlined in the Australian Open Disclosure Framework (**the Framework**), created by the Australian Commission on Safety and Quality in Health Care. The Framework and Standards are not legally binding but if implemented can help minimise and manage risk.

According to the Framework, open disclosure is the open discussion with the patient, their family and carers of adverse events that result in harm to a patient while receiving health care. An adverse event is any unplanned event resulting in, or having the potential to result in, injury to a patient or an otherwise unintended outcome. For an event to be classified as an "adverse event", it is not necessary that any harm actually occurred or that there was any mistake or error.

The elements of open disclosure are:

- an apology or expression of regret, which should include the words "I am sorry" or "we are sorry". "We are sorry this happened to you" is often an appropriate expression;;
- a factual explanation of what happened;
- an opportunity for the patient, their family and carers to relate their experience;

---

[4] Refer to "*Scenarios*" section of this guide.

[5] Refer to "*Scenarios*" section of this guide.

- a discussion of the potential consequences of the adverse event; and
- an explanation of the steps being taken to manage the adverse event and prevent recurrence.

Open disclosure should occur as a process of discussion, not a one-way provision of information from the medical practitioner to the patient, their family and carers.

Where the adverse event triggering the need to engage in open disclosure followed or involved the provision of a telehealth service, the telehealth provider should be involved in the process of open disclosure. The level of involvement of the telehealth provider in the open disclosure discussions may be proportionate to the role they played in the patient's treatment prior to the adverse event in question, or the role their treatment had in triggering the adverse event. For example, in Scenarios 1 and 3[6], it may be normal for the telehealth provider to have little input in the process of open disclosure if their involvement in the patient's treatment did not directly relate to the occurrence of the adverse event.

Why do health service organisations need open disclosure policies?

As stated herein, the Framework and the Standards are not legally binding but if implemented can help health organisations manage future risk.

A health service organisation that does not have an adequate open disclosure policy might:

- risk losing government funding; and/or
- compromise its ISO certification and any other forms of certification and accreditation.

Pursuant to the *Health Services Act 1988* (Vic), the Secretary of the Department, in determining whether or not any grant, subsidy or other financial assistance should be given to an agency, will consider the extent to which arrangements are in place within that agency for:

- ensuring that it makes efficient use of its resources; and
- monitoring and improving the quality of health services provided by the agency; and
- making its services accessible to minority groups and disadvantaged people; and
- enabling users of its services to make informed decisions about health care; and
- enabling its employees to participate in decisions about their work environment.[7]

---

[6] Refer to "*Scenarios*" section of this guide.

[7] *Health Services Act 1988* (Vic), section 18(a)(i)-(v).

As such, if by virtue of the lack (or inadequacy) of an open disclosure policy the Secretary of the Department of Health and Human Services considers that the health service organisation is not taking steps to monitor and improve the quality of health services it provides[8], it may determine that any particular grant, subsidy or other financial assistance should not be granted.

A health service organisation that does not have an adequate open disclosure policy also risks compromising its certification, or eligibility for certification, from the International Organisation for Standardisation (**ISO**). Accreditation from other organisations, such as the Australian Commission on Quality and Safety in Health Care, might also be placed at risk.

Incident reporting guidelines

All Victorian publicly funded health organisations are required to comply with the Department of Health and Human Services incident reporting processes as part of their service agreement. Reporting of incidents as defined in the Department of Health and Human Services incident reporting instruction is compulsory, to ensure the Department complies with the requirements and expectations associated with public accountability, its legal obligations, and insurance requirements. While there is no legal requirement to follow these guidelines and policies, there is a strong belief that health service organisations stand to benefit in the long-term from open disclosure, particularly in relation to the introduction of a telehealth system (or any new system that utilises new technologies and charters new ground in the early stages of implementation).

Complying with incident reporting guidelines will also avoid the potential risk of compromising ISO certification and/or losing accreditation from the Australian Commission on Safety and Quality in Health Care.

Victorian Health Incident Management Policy

All Victorian publicly funded health services and agencies that provide health services on behalf of the Victorian Department of Health and Human Services are within the scope of the Victorian Health Incident Management Policy (**the VHIM Policy**) - a comprehensive guideline for health services and agencies that incorporates a State-wide framework for the collection and management of clinical incident reports.

The following health services and agencies are within the scope of the VHIM Policy and are therefore instructed by the Department of Health and Human Services to comply with it:

- public health services and all services under their governance structure;
- registered community health services;
- Ambulance Victoria;

---

[8] *Health Services Act 1988* (Vic), section 18(a)(ii).

- Royal District Nursing Service;
- Ballarat District Nursing and Healthcare;
- bush nursing centres (public funded);
- Forensicare (Thomas Embling Hospital); and
- incorporated residential aged care services (public funded).

The Department of Health and Human Services requires all publicly funded health services to follow the VHIM Policy as part of their service agreement.[9]

The VHIM Policy sets out the manner in which health services and agencies are to provide data to the Department of Health and Human Services. For example, de-identified data extracts of all clinical incidents are to be provided monthly via an electronic secure data exchange process that allows for data encryption. The VHIM Policy indicates that incident notifications are to be sent as a single incident transmission via the electronic gateway. If a notifiable event occurs during a telehealth consultation and both the telehealth provider and the host provider are aware of the event occurring, the two practitioners should communicate clearly and make a decision as to who will report the event.

The VHIM Policy also outlines specific timeframes within which certain categories of incidents must be reported. For example, the Department of Health and Human Services must be notified within three days of the occurrence of a reportable sentinel event.

Reportable sentinel events

A sentinel event is a relatively infrequent, clear-cut event that occurs independently of a patient's condition. Sentinel events often reflect hospital or agency system and process deficiencies, and result in unnecessary outcomes for patients. The VHIM Policy contains guidance on reporting sentinel events. As the Department of Health and Human Services requires all publicly funded health services to follow the VHIM Policy as part of their service agreement, failure to report a nationally-defined sentinel event within the specified time-frame may be seen as a failure to meet the requirements of the service agreement.

There are eight nationally-defined, reportable sentinel events. Of these, the most likely to occur as a result of telehealth service provision is "medication error leading to the death of patient reasonably believed to be due to incorrect administration of drugs". More specifically, this sentinel event might be caused by an inappropriate e-prescription being provided by a telehealth provider who has consulted a patient. This event might be more likely to occur in the context of telehealth as a prescribing telehealth provider cannot conduct a clinical assessment of the patient.

---

[9] http://docs.health.vic.gov.au/docs/doc/9735690875F2A312CA2578A90080F597/$FILE/110401_DoHVHIMS%20policy%20WEB%20v2.pdf

All host providers and telehealth providers (whether public or private) that identify a national sentinel event must report the incident to the Sentinel event program. The VHIM Policy requires notification to be made to the Department of Health and Human Services within three days of the event occurring.

Root cause analysis

Root cause analysis (**RCA**) is a process analysis method which is used to identify factors that cause adverse events. A root cause analysis process is a critical feature of safety management in health service providers and health care organisations. The approach focuses on the organisation of health care and aims to reduce errors at the health service level. The outcomes of root cause analysis can be used to detect failures in the current system and to find solutions to address these failures and prevent similar adverse events re-occurring.

All publicly funded health services and agencies that identify an incident that reflects a national sentinel event definition are required to report the incident to the Department's Sentinel Event Program. The policy excludes private health services and non-government organisations. The level of investigation will vary depending on the incident severity rating. Sentinel event and equivalent ISR 1 incidents require an RCA to be conducted and a summary report provided to the Department within 60 days. Publicly funded health services that do not comply with the obligation to report sentinel events will fail to meet the requirements of their service agreement.

Where the requirement to conduct a RCA arises out of a telehealth consultation/s, the telehealth provider and the host provider should work collaboratively to complete the RCA.

It is uncertain on the current state of the law as to whether in litigation a root cause analysis document is discoverable, meaning that it has to be disclosed in the litigation, or whether it is protected by public interest immunity, meaning that it is in the public interest that the RCA not be disclosed. It is arguably in the public interest not to disclose a RCA because to do so would impede the ability of health services in future to conduct open and frank discussion about reportable incidents given that what they said could later be accessible in litigation and used against them.

BEFORE YOU START

Key Points

- Although not law, the national standard for credentialing must be met for a health service to meet its accreditation requirements.
- Where patients of host providers receive advice by telehealth from health professionals who are not employees of the host provider, the host provider should ensure the telehealth service provider is appropriately credentialed.
- It is not necessary that a health service undertake the task of credentialing all telehealth providers it might use, but must be satisfied that the telehealth service provider has been appropriately credentialed by either a credentialing committee or a similar health service in Victoria.

CREDENTIALING AND DEFINING THE SCOPE OF CLINICAL PRACTICE

There are national requirements for all health service organisations to ensure their medical and other practitioners are appropriately credentialed. Health service organisations are also required to ensure that their medical and other practitioners do not practice outside an appropriate scope of their clinical practice. These requirements apply equally to host providers providing telehealth services as they do to a health service that only provides face-to-face consultations.

Framework of credentialing requirements: The National Standard

The Australian Commission on Safety and Quality in Healthcare (formerly known as the Australian Council for Safety and Quality in Health Care) has published the *Standard for credentialing and defining the scope of clinical practice* (2004) (**the National Standard**). The National Standard establishes a framework for credentialing of medical practitioners and defining the scope of a practitioner's clinical practice. It provides guidance regarding how the structure and processes of credentialing and defining the scope of clinical practice should be implemented. This includes guidance on establishing criteria for a position, verification of credentials, establishing processes for initial credentialing, re-credentialing, temporary credentialing, emergency credentialing and more.

Why follow the National Standard?

The National Standard is not a law and there is no legal obligation on a health organisation to credential health practitioners working at their facilities. However, the National Standard supports the National Safety and Quality Health Service (**NSQHS**) Standards, which must be met for a health service to meet its accreditation requirements. Further, it is a condition of the insurance arrangements of Victorian public health services that the health service credential practitioners who are appointed to their health service and who have individual responsibility for patient care. Further, compliance with the National Standard is recommended as a matter of risk prevention.

While the National Standard draws a distinction between credentialing and defining the scope of clinical practice, these two concepts operate hand-in-hand. An effective system of credentialing is valuable in minimising the risk of adverse events occurring by ensuring that hospitals or health services only grant health care professionals approval to perform procedures that are within their experience and competence.

The National Standard may be viewed as encouraging the implementation of systems such as telehealth as it:

- extends the concept of credentialing and defining the scope of clinical practice to encompass shared responsibility for safe service provision in supportive environments;
- acknowledges the importance of the input of medical practitioners in the process of improving safety and quality in healthcare organisations;
- reinforces the responsibility of healthcare organisations to provide resources to support the services they wish to offer;
- recognises that peer assessment and the willingness of individuals to comment on their own skills and the skills of others are fundamental to successful processes of credentialing and defining the scope of clinical practice.

Distinguishing between credentialing and defining the scope of clinical practice

According to the National Standard:

> *Credentialing refers to the formal process used to verify the qualifications, experience, professional standing and other relevant professional attributes of medical practitioners for the purpose of forming a view about their competence, performance and professional suitability to provide safe, high-quality healthcare services with specific organisational environments.*
>
> *Defining the scope of clinical practice follows on from credentialing and involves delineating based on the individual's credentials, competence, performance and professional suitability, and the needs and capability of the organisation to support the medical practitioner's scope of clinical practice.*[10]

In order to comply with the National Standard, a health organisation must firstly have a formal process for credentialing of the medical practitioners it employs and grants visiting rights to. It must then define the scope of each practitioner's clinical practice and limit their practising rights to that

[10] Department of Health and Human Services, *Credentialing and defining the scope of clinical practice for medical practitioners in Victorian health services - a policy handbook*, page 8.

scope. When credentialing a practitioner it is recommended that it be mentioned whether the scope of practice extends to delivering services via telehealth.

Responsibility for credentialing

In the traditional arrangement of health service provision, a health organisation will typically take responsibility for credentialing the health practitioners it employs or grants visiting rights to. However, it is again noted that this is not a legal obligation, it is a policy obligation under the Victorian Health Policy and Funding Guidelines. Accreditation status will be monitored by the Department in accordance with the *Accreditation – performance monitoring and regulatory approach business rules 2013*. These business rules detail the Department's regulatory approach to accreditation outcomes and provide health services with a clear understanding of the requirements of the new scheme and reporting obligations.

When providing health services via telehealth, the question of which organisation (that is, the host provider or the telehealth provider) should be responsible for credentialing the practitioner providing the telehealth service is less clear.

In Scenario 1[11], for example, where the host provider seeks advice directly from a tertiary institution, the host provider may reasonably rely on the tertiary institution to have appropriately credentialed and limited the scope of the individual practitioner. Such reliance would be reasonable simply by virtue of the fact that the telehealth provider is a tertiary institution.

On the other hand, in Scenarios 3 and 4[12], where a private specialist who is not associated with a tertiary health service provides health services via telehealth, the host provider is likely to be responsible for credentialing the private specialist prior to permitting him/her to consult the patient. There is no requirement that the rural health service undertake the task of credentialing for all the telehealth providers it might use. Provided the host provider is satisfied that the practitioner has been appropriately credentialed, either by a credentialing committee or by a similar rural health service in Victoria, it will be acceptable to rely on that credentialing.

Medical management and credentialing committees

The Department of Health and Human Services Policy Handbook on Credentialing and Defining the Scope for Clinical Practice for Medical Practitioners in Victorian Health Services (**the Handbook**) suggests that the "governing body of a health service should allocate a defined organisational committee to ensure effective processes of credentialing and defining the scope of clinical practice."

---

[11] Refer to "*Scenarios*" section of this guide.

[12] Refer to "*Scenarios*" section of this guide.

It also explains that:

> *the effectiveness of processes of credentialing and defining the scope of clinical practice depends on the contribution of professional peers who must verify credentials, evaluate competence and performance and recommend the appropriate scope of clinical practice in the context of the organisation's needs and capability.*

The process of credentialing could be undertaken at a local, sub-regional, regional or state level by way of a regional or sub-regional committee. Defining the scope of clinical practice, however, may only be undertaken by the individual health service. Therefore:

- a single health service in rural Victoria could establish a committee comprised by a group of the health service's staff to undertake both credentialing and defining the scope of clinical practice for both the health practitioners working at the health service and the telehealth practitioners the health service engages; or

- that health service in rural Victoria could join other health services in the same geographical region to establish a regional or sub-regional committee to undertake credentialing for all member health services. However, if the rural health service wished to limit a practitioner's scope of clinical practice at its particular health service further than the limits of the scope of practice imposed by the committee, it will be required to do so itself. Each health service needs to bear in mind that credentialing a practitioner and determining their scope of practice is not dictated solely by the practitioner's experience and expertise, but also by the facilities and resources of the particular health service to support the scope of practice being considered.

Regional and sub-regional committees might consider creating a "Directory of Credentialed Telehealth Providers" to list the telehealth providers (organisations and individuals) that the committee has credentialed to provide telehealth services to patients at health organisations represented by the committee. These directories could usefully identify the credentialed organisation or practitioner, provide their contact details, their speciality and details of standard arrangements for telehealth provision. Host providers could use this directory to define the scope of practice of each telehealth provider on the directory. Ideally, each rural health service intending to utilise telehealth should create a directory of this kind and ensure that it is made readily available for all staff.

The committees should meet regularly and meetings should be convened by the DMS/medical leader. It is clear that members of the committees must have relevant expertise for their role and must not have a conflict of interest. It is therefore advisable that committees are formed by representatives from a number of health organisations that will be represented by the committee and who have different fields of expertise. Further, to advance consumer partnerships (which is a component of the NSQHS scheme) the committee could include a member who brings expertise in consumer or community issues.

Guidance from the Victorian Department of Health and Human Services requires that appropriate credentialing is to be undertaken:

- prior to appointment to the health service;
- at least once in each five-year period; and
- at times where a review of credentials is requested by either the individual medical practitioner or by an authorised person within the health service.

PROVISION OF TELEHEALTH SERVICES TO PATIENTS

Key Points

Duty of care

- It is not essential that the health practitioner have a direct relationship with the patient to owe the patient a duty of care.
- When providing treatment to or advice to or about a patient, the health practitioner has a duty of care to the patient and will be liable for their negligent acts.
- In some circumstances the health provider is liable not only for their own acts or omissions but those of the telehealth provider also.

Informed consent

- In a telehealth arrangement, a host provider must obtain the patient's informed consent before performing any physical test or procedure and before providing the patient's health information to the telehealth provider.

  Adults who are incapable of consenting (instructions other than emergencies)

  - If an adult is temporarily unable to consent and treatment is required, permission (consent) to treat the patient ought to be obtained from the person highest on the list of the order of persons from consent can be obtained as set out in sections 37 and 39 of the *Guardianship and Administration Act 1986*.

  Emergencies

  - In the case of an emergency where the patient is not competent to consent, treatment can be lawfully administered without consent, although treatment cannot be administered if the patient had prior to becoming incompetent expressed a wish not to receive the treatment contemplated.

  Minors

  - Even if a patient is a minor, if the minor is mature enough to understand the nature and effect of the treatment proposed, consent should be obtained from the minor. Generally speaking, most adolescents aged 16 and over are capable of providing informed consent. Those aged 13 and under are generally not.

Referrals

- Some, but not all, telehealth arrangements constitute a referral. For those that do, the legislative requirements can be met by the host provider completing a referral form and electronically transmitting it via the telehealth system.

Confidentiality

- The *Privacy Act 1988* (Cth) and *Health Service Act 1998* (Vic) protect a patient's right to privacy and require that all health service providers observe the patient's privacy and confidentiality.
- The *Privacy Act* and *Health Records Act* contain health privacy principles regulating the collection, use, disclosure and storage of health information. All health service providers and health practitioners, whether providing services via face-to-face consultation or via telehealth, must comply with these principles.
- Health practitioners not only owe statutory duties of confidentiality but common law duties also.
- Unless a patient has expressly asked that information be held in confidence and not be conveyed to anybody else, a host provider providing information about a patient to a telehealth provider for the purposes of providing care to the patient does not constitute a breach of confidentiality obligations.

E-Prescribing

- Subject to specific criteria, prescriptions can be sent electronically to pharmacies across Victoria.
- There are limitations, most notably in the context of telehealth a medical practitioner is not permitted to prescribe medications other than for the treatment of a patient under that practitioner's care. In some telehealth scenarios the patient is not considered to be under the care of the telehealth provider. These circumstances may require the telehealth consultation to be modified such that the patient is in attendance.

DUTY OF CARE

Health services and their employees and independent health practitioners owe to the patient a duty to exercise reasonable skill and care when providing health services to those patients. It is no different when providing services via telehealth.

It is not essential that the health practitioner have a direct relationship with the patient to owe the patient a duty of care. A pathologist to whom blood samples are sent for testing owes a duty to the patient to exercise reasonable skill and care when doing so. When a health practitioner seeks a second opinion from another health practitioner, there is no direct relationship between the patient and the practitioner from whom the second opinion is sought. The direct relationship is between the two health practitioners. Notwithstanding the absence of a direct relationship, if the health practitioner providing the second opinion knows or ought reasonably to know that care of the patient will be to some degree dependent on the opinion given, then a duty is owed by that health practitioner to the patient.

Standard of care owed

At common law a health professional must act in a manner that can be reasonably expected of a person professing that skill. For example, a midwife owes a standard of care expected of a "*reasonable midwife*". Just like it is no defence for a "*P-plate*" driver to assert "*inexperience*" if involved in a motor vehicle collision, similarly for a health professional inexperience is not a defence.

The law treats two components of health care differently. Those components are:

- advising a patient about the benefits and risks of treatment; and
- the carrying out of the treatment.

The common law standard of care applies in respect of both aspects, however there is a statutory defence available in respect of carrying out the treatment but not in respect of the advising of the risks of treatment.

The *Wrongs Act 1958* (Vic) states that a professional (which includes a health professional) is not negligent if the professional acted in a manner that at the time the service was provided "*was widely accepted in Australia by a significant number of respected practitioners in the field (peer professional opinion) as competent professional practice in the circumstances*".[13]

The fact that there might be different peer professional opinions widely accepted does not prevent a successful defence.

The quoted section of the *Wrongs Act* does not apply in respect of advising a patient about the risks of treatment. Therefore, in respect of advising of the risks of treatment, a health professional will be judged by the standard of what the court determines was reasonable, irrespective of whether there are a significant number of peer professionals who would have given similar advice as the defendant.

Non-delegable duty of care

The law has imposed on some organisations a special category of "*non-delegable duty of care*". It means that the organisation is not only responsible for its own negligent acts and omissions but also the negligent acts and omissions of others not employed by the organisation and even if they are independent contractors.

Hospitals are one such category of organisations that the law recognises owe a non-delegable duty of care[14]. The scope of non-delegable duty to health organisations other than hospitals has not yet been tested, although it is conceivable that, if tested, it might also extend to health services generally, even if not strictly hospitals.

---

[13] Section 58(1) of the *Wrongs Act 1958*.

[14] *Ellis v Wallsend District Hospital* (1989) NSWLR 553 at 603-605; *Kondis v STA* (1984) 124 CLR 672 at 685-686.

The extent of the non-delegable duty of care owed depends upon the services that the hospital has undertaken to provide[15]. It has a non-delegable duty in respect of those services. A public hospital who admits a patient as a public patient undertakes to provide all aspects of care to the patient whilst under its care. As a consequence, it owes a non-delegable duty of care in respect of all aspects of the patient's treatment. For example, the public hospital, rather than perform pathology testing itself, might engage an independent contractor to do so. The hospital is liable to the patient for the acts and omissions of the independent contractor. [For completeness, the contractor also owes a duty to the patient and would be liable to the patient.] By contrast, a public (or private) hospital which admits a patient who elects to be treated as a private patient and engage their own surgeon is not liable for the negligent acts and omissions of the surgeon. In that situation, the hospital has undertaken to provide hospital services (such as nursing, operating theatres and the like) but not the medical services of the surgeon. As such, the hospital has a non-delegable duty of care in respect of the hospital services it has agreed to provide, but not the medical services of the surgeon. If that same hospital sends blood samples out for testing to an external independent laboratory, unless the patient was made aware that the hospital does not itself do pathology testing but can, on behalf of the patient, arrange testing by an independent laboratory to which the patient agrees and agrees to pay for, the hospital will likely be liable to the patient for the acts and omissions of the contractor under the principles of non-delegable duty of care.

Telehealth Scenarios[16]

In respect of the four telehealth scenarios, the relevant duties of care owed are as follows. In conducting this analysis it is assumed that the non-delegable duty of care the law imposes on hospitals equally applies to the health services referred to in the scenarios.

Scenario 1

The rural health service will likely owe a non-delegable duty of care to the patient. It owes the patient a duty of care in respect of its own acts and omissions. Under the principles of non-delegable duty, that duty extends to the acts and omissions of the provider of the telehealth service, namely the tertiary health service. The tertiary health service also owes the patient a duty of care because it is apparent to the tertiary health service that the tertiary health service's opinion will influence the management of the patient.

Therefore, the rural health service is liable to the patient for not only its own acts and omissions but for the acts and omissions of the tertiary health service also. The tertiary health service is liable to the patient for (only) its acts and omissions.

---

[15] *Elliott v Bickerstaff* (1999) 48 NSWLR 124.

[16] Refer to "*Scenarios*" section of this guide.

Scenario 2

The rural health service has recognised that the patient's treatment is outside its expertise and is referring the patient to the tertiary health service. In those circumstances, the rural health service's duty of care does not extend to the acts and omissions of the tertiary health service. It is liable only for its own acts and omissions. This includes tasks it performs at the request of the tertiary health service to assist with the assessment or treatment of the patient.

The tertiary health service, who is providing a service directly to the patient, owes the patient a duty of care. It is liable for its own negligent acts and omissions and will be liable for the acts of the rural health service done at its request. The law is not so clear as to be able to definitively say whether a tertiary health service will be liable to the patient for tasks it requests the rural health service to perform but which tasks are performed negligently.

If the rural health service competently performs a task at the request of the tertiary health service but the request is deemed negligent, the tertiary health service will be liable for any resultant injury to the patient. The rural health service will not be liable, unless the rural health service ought to have known that the task requested was contraindicated. For example, if the tertiary health service requests the rural health service to administer an injection of a common medication at a dose far in excess of the safe limit, the tertiary health service (for negligently directing an excessive dose be given) and the rural health service (for administering the excessive dose when it ought to have known it was excessive) will both be liable to the patient.

Therefore, the rural health service is liable to the patient for its own acts and omissions and, likewise, the tertiary health service is liable to the patient for its own negligent acts and omissions. The tertiary health service might be liable to the patient for tasks it request the rural health service perform and which are performed negligently.

Scenario 3

The patient is a patient of the rural health service and has engaged the specialist to provide it (rather than the patient) with advice on how best to treat the patient. In those circumstances, the rural health service has undertaken the care of the patient and owes the patient a duty of care and, it is likely that under the principles of non-delegable duty, that duty to the patient will extend to the acts and omissions of the specialist. The specialist too owes the patient a duty of care because the specialist knew or ought to have known that the specialist's opinion would influence the treatment provided by the rural health service to the patient.

Therefore, the rural health service is liable to the patient not only for its own acts and omissions but likely those of the specialist also. The specialist is liable to the patient for (only) the specialist's acts and omissions.

Scenario 4

The situation is similar to scenario 2. The rural health service has decided it does not have sufficient expertise and is effectively referring the patient to the private specialist. The rural health service owes the patient a duty of care but that duty of care does not extend to the acts and omissions of the specialist. It is only liable for its own acts or omissions. This includes tasks it performs at the request of the private specialist to assist with the assessment or treatment of the patient.

If the rural health service competently performs a task at the request of the private specialist but the request is deemed negligent, the private specialist will be liable for any resultant injury to the patient. The rural health service will not be liable unless the rural health service ought to have known that the task requested was contraindicated. For example, if the specialist requests the rural health service to administer a common medication at a dose far in excess of the safe limit, the private specialist (for negligently directing an excessive dose be given) and the rural health service (for administering the excessive dose when it ought to have known it was excessive) will both be liable to the patient.

The private specialist who is providing a service directly to the patient owes the patient a duty of care. The private specialist is liable for the specialist's own negligent acts and omissions and will be liable for the acts of the rural health service done at the specialist's request if those requests were carried out competently. The private specialist will not be liable for the negligent performance of those tasks requested.

Therefore, the rural health service is liable to the patient for its own negligent acts and omissions and, likewise, the private specialist is liable for the specialist's own negligent acts and omissions.

INFORMED CONSENT

Before a health practitioner commences treatment or intervention they must first have the patient's informed consent. This means that sufficient information has been given to the patient to enable the patient to decide whether to undergo the procedure or treatment and following this the patient has consented to it.

In order to be valid, consent must be informed, relevant, free and voluntarily given.

In a telehealth arrangement, a host provider is required to obtain the patient's informed consent before:

- performing any physical test or procedure on the patient; and
- providing the patient's health information to a telehealth provider.

The telehealth provider in the arrangement will not be providing hands on treatment but will instead provide advice to the patient or to the host provider or both. As such, there is no legal requirement on the telehealth provider to first obtain a person's consent in order to receive that person's health information nor to verbally provide that person with advice. Generally, the patient's participation in the telehealth consultation is sufficient.

Informed consent will be required if treatment is to be administered by the host provider (or anybody else) following the telehealth consultation and before treatment is commenced. For example, the telehealth provider might recommend that a lumbar puncture be performed. Before performing the lumbar puncture the host provider will need to inform the patient of what is involved, including the risks, so as to enable the patient to make an informed decision as to whether to consent to the procedure. Only if the patient thereafter consents can the lumbar puncture be lawfully performed.

Consent may be oral or written. Signed consent forms are not of themselves conclusive proof that a patient has given informed consent to a procedure or for their information being provided to another person. They do, however, constitute useful evidence of consent having been given.

It would be appropriate and reasonable for a host provider to require a patient to sign a form confirming that they consent to their health information being provided to the telehealth provider for the purposes of their further treatment. This would go a long way to avoiding a subsequent dispute as to whether consent was obtained.

Adults who are incapable of consenting (other than emergencies)

If an adult patient is temporarily unable to consent to treatment and the treatment proposed is not urgent, the health professional should wait until the patient has regained capacity. If the patient has a permanent incapacity or is unlikely to regain capacity within an appropriate time frame, permission to treat the patient ought to be obtained in accordance with Sections 37 and 39 of the *Guardianship and Administration Act 1986*. Under that Act, consent ought to be obtained from persons listed in the Act in order of priority. That list is lengthy, however it commences with persons specifically authorised to consent to treatment by way of appointments under the *Medical Treatment Act 1988*, or appointed by the Guardianship and Administration Tribunal. If there are no such persons who have been granted specific authority to provide consent, consent can be obtained from, in order of priority, the patient's spouse or domestic partner, the eldest person over the age of 18 years who is the patient's son or daughter, father or mother, brother or sister, grandfather or grandmother, grandson or granddaughter, uncle or aunt, nephew or niece.[17]

Emergencies

In the case of an emergency, where a patient is not competent to consent (whether it be by age, consciousness, affected by drugs or some other incapacity, temporary or permanent) and there is no person available to consent on that patient's behalf, treatment can be lawfully administered without consent.

To be deemed as an emergency, there must be a serious and imminent threat to the life or physical or mental health of the patient requiring immediate treatment.

---

[17] Section 37 *Guardianship and Administration Act 1986*.

If the patient had, prior to becoming incompetent, expressed a wish not to receive the treatment contemplated, the emergency treatment exception might not apply. For example, if a Jehovah's Witness who has when competent previously expressed their wish not to have a blood transfusion, and if that refusal covers the circumstances at hand, notwithstanding the blood transfusion might be necessary and be the only means to save the patient's life, it would be unlawful to proceed with a blood transfusion.

What if the patient is a minor?

A minor is a person under the age of 18 years.

If the minor is mature enough to understand the nature and effect of the procedure proposed, consent should be obtained from the minor. There is no fixed age by which the law considers a minor capable of providing informed consent, however, as a general rule of thumb, most adolescents aged 16 and over, if given an adequate explanation, are capable of providing informed consent. Those aged 13 and under generally are not. A common grey area are the ages of 14 and 15.

These ages are a guide only. As stated, the test is whether the individual has the capacity to understand the general nature and effect of the proposed procedure.

In the case of children who are too young to provide informed consent, consent to treatment should be obtained from a parent or guardian.

REFERRALS

Not all telehealth arrangements amount to a referral. However, in some situations, a host provider seeking a telehealth provider to consult a patient may be considered a referral.

Scenarios 1 and 3[18] are examples of telehealth arrangements that do not constitute a referral for the obvious reason that the patient has not actually been referred. On the other hand, Scenarios 2 and 4[19] are likely to constitute referrals and as such, there are a small number of legislative requirements that host providers need to be aware of in order for the patient to claim a Medicare benefit in respect of any referred service (that is, the service provided by the telehealth provider).

Requirements for referral to a medical specialist

The requirements for referral to a medical specialist are uniform across Australia and are contained in the *Health Insurance Regulations 1975* (Cth). Any referral to a medical specialist must be given in writing[20], signed by the referring practitioner[21] and dated[22].

---

[18] Refer to "*Scenarios*" section of this guide.

[19] Refer to "*Scenarios*" section of this guide.

[20] Regulation 29(4)(a) *Health Insurance Regulations 1975* (Cth).

The host provider must ensure these requirements are met to attract a Medicare benefit for the telehealth consultation with the specialist. These requirements can easily be fulfilled by the host provider completing a referral form and electronically submitting it via telehealth..

CONFIDENTIALITY

A patient's right to privacy is protected by the following statutes:

1. *Privacy Act 1988* (Cth) (***Privacy Act***) at the national level;

2. *Health Services Act 1988* (Vic) *(**Health Services Act***) at the State level; and

3. *Health Records Act 2001* (Vic) (***Health Records Act***) at the State level.

The confidentiality requirements contained within these Acts apply to all public and private health service providers. They require health service providers to deal with patients' personal (including health) information in a manner that will preserve the patient's privacy and confidentiality.

The Australian Privacy Principles and the Health Privacy Principles

The APPs and the HPPs are contained in the Commonwealth *Privacy Act* and the Victorian *Health Records Act* respectively. The APPs and the HPPs, which are largely consistent, cover topics including the collection, use, disclosure and storage of personal information by government agencies and some private sector organisations. They apply to health service providers public and private.

The APPs and HPPs are substantially similar. In respect of confidentiality they stipulate that a person's information cannot be disclosed for any purpose other than the primary purpose that it was collected, except in certain circumstances, such as:

- for related purposes;
- with the person's consent;
- where the person is not competent to consent and it is not reasonably practicable to obtain proxy consent;
- the person from whom the information is dead and is not known to have previously objected;
- for funding, monitoring, improving or evaluating health services, training staff, research or statistical purposes;

---

[21] Regulation 29(4)(b) *Health Insurance Regulations 1975* (Cth).

[22] Regulation 29(4)(c) *Health Insurance Regulations 1975* (Cth).

- to lessen or prevent a serious risk to the individual or the public; and
- to defend legal proceedings and in law enforcement.

All health service providers and health practitioners, whether providing services via face-to-face consultation or via telehealth (including where there is no direct relationship with the patient such as in Scenarios 1 and 3[23]), must comply with the APPs and HPPs.

Confidentiality under the *Health Services Act*

Further and more specifically, under section 141 of the *Health Services Act*, a health service organisation (public or private) and its employees[24] must not, except to the extent necessary, give any information to another person, whether directly or indirectly, that identifies the first person if that information was acquired by reason of it being a health service provider or health organisation.

In other words, section 141 of the *Health Services Act* prohibits a health service and its employees providing a person with information that could identify a patient of the health service. However, a health service *may* provide information that would identify a patient if:

1. The patient has given prior consent to that information being given; or
2. The giving of that information is required in connection with the further treatment of the patient.

In most cases involving telehealth, at least one of these two exceptions is likely to apply so that it will be lawful for a host provider to give information to the telehealth provider for the purposes of the telehealth consultation. In Scenarios 2 and 4[25], a host provider is unlikely to arrange for a consultation between a telehealth provider and the patient unless the patient has consented to the host provider doing so. In Scenarios 1 and 3[26], the host provider contacts the telehealth provider in order for it to receive advice regarding the further treatment of the patient.

Common law and ethical duty of confidentiality

The duty of confidentiality also arises in common law (case law, as distinct from legislation) and principles of professional ethics.

According to long-standing common law, health care professionals (including nurses, pharmacists, psychologists and so on) have a duty to maintain the confidentiality of their patients' information - a wrongful breach that causes significant injury to the patient could form the basis for a claim in

---

[23] Refer to "*Scenarios*" section of this guide.

[24] *Health Services Act 1988* (Vic), section 141(1).

[25] Refer to "*Scenarios*" section of this guide.

[26] Refer to "*Scenarios*" section of this guide.

negligence or breach of contract. The majority of such claims are now dealt with under the legislation and as a result, common law claims for failure to maintain confidentiality are now rare.

Disclosing information to another health service provider

A patient's information may, however, be disclosed to another health service provider if the information is to be used in the provision of further health services to the individual. For example, a nurse may provide information about a patient to a doctor, or vice versa, provided the recipient of the information is involved in the current care of the patient and the patient has not requested that the information be held in confidence. The provision of telehealth services is unlikely to cause issues in relation to disclosure of health information because this disclosure is for the purposes of the telehealth provider providing health care to the patient. Therefore, unless the patient does not consent to the telehealth provider being contacted (a scenario which is not likely to occur often), host providers engaging in the provision of telehealth services are unlikely to breach their confidentiality obligations by virtue of providing a patient's health information to a telehealth provider.

E-PRESCRIBING

Electronic prescribing (**e-prescribing**) is a mechanism that enables all stages of the prescribing and supply of medicine, and the claiming process to be completed electronically. The use of e-prescribing will likely increase as the use of telehealth systems increases as it will allow for greater efficiency in, and completeness of, telehealth service provision.

The current laws relating to e-prescribing differ in each State and Territory. There are three different approaches taken by the various jurisdictions:

1. **Dispensing rules:** where the laws regulate the pharmacist dispensing the prescription medication;

2. **Prescribing rules:** where the laws regulate the practitioner issuing the prescription; and

3. A combination of both dispensing rules and prescribing rules.

Victoria regulates e-prescribing practices according to dispensing rules.[27]

Following a successful e-prescribing trial by Peninsula Health and Austin Health, criteria for e-prescriptions were approved in September 2013.[28] This generic approval for e-prescriptions will allow electronic transmission of prescriptions to pharmacies across Victoria and will allow all patients based in Victoria to readily access the e-prescribing system.

---

[27] *Drugs, Poisons and Controlled Substances Act 1981* (Vic) and the *Drugs, Poisons and Controlled Substances Regulations 2006* (Vic).

[28] http://www.health.vic.gov.au/dpcs/approve.htm#e-Prescriptions.

E-prescribing will be a fundamental tool for the implementation of telehealth. It will allow for telehealth consultations to result in action and treatment, rather than merely un-actionable advice. In turn, e-prescribing will help to align the capabilities of telehealth closer to that of a face-to-face consultation.

Limitations of e-prescribing in telehealth

There are limitations to a practitioner's authority to e-prescribe. Most significantly in the context of telehealth is the fact that a medical practitioner is not permitted to prescribe medications other than for the medical treatment of a patient under that practitioner's care. This means that the telehealth provider in Scenarios 1 and 3[29] cannot prepare an "e-script" for the host provider's patient because in these scenarios, the telehealth provider has not actually consulted the patient and therefore the patient is not considered to be in the care of the telehealth provider.

If the purpose of the telehealth consultation is to obtain a prescription, the patient should be present in the consultation as in Scenarios 2 and 4[30]. In these scenarios, the telehealth provider may lawfully complete a script and send it via telehealth systems to the host provider, who may then print the script and provide it to the patient.

Other legislative limitations include:

- the requirement that a practitioner or organisation must have a permit from the Drugs and Poisons Regulation Group to prescribe Schedule 8 poisons in certain circumstances;
- the prohibition on prescribing anabolic steroids to enhance sporting performance; and
- the restriction on certain Schedule 4 poisons being prescribed by anybody other than a medical practitioner with the appropriate qualifications and expertise and who holds a warrant to prescribe the drug or a medical practitioner acting in accordance with the direction of a warrant holder.

These limitations apply to all medical practitioners in Victoria regardless of whether or not they provide telehealth services or wish to e-prescribe.

---

[29] Refer to "*Scenarios*" section of this guide.

[30] Refer to "*Scenarios*" section of this guide.

HEALTH RECORD MANAGEMENT AND DATA TRANSMISSION AND STORAGE

Key Points

- There are a range of Acts (State and Commonwealth) which regulate health record management and data transmission and storage.
- Steps must be taken to protect health information from misuse, interference, loss, unauthorised access, modification or disclosure.
- A Victorian public health service intending to transmit information about a patient to someone outside Victoria must comply with Health Privacy Principle 9 of the *Health Records Act 1988* (Vic).
- Who has responsibility for managing an individual's records in telehealth is less clear than in the traditional provision of health services.
- Victorian public health services are required to retain records for varying periods prescribed by the *Public Records Act 1973* (Vic).

In Victoria, there are four primary statutes that govern the management of health records:

1. *Public Records Act 1973* (Vic)

The *Public Records Act 1973* (Vic) (***Public Records Act***) applies to all Victorian health service organisations and individual practitioners in the public (but not private) sector.[31] The *Public Records Act* regulates for how long health services must keep original records, when copies can be made and the originals destroyed, and for how long the records (original or copies) must be kept before disposing of them altogether.

2. *Privacy Act 1988* (Cth)

All telehealth providers and host providers in telehealth arrangements across Australia will be subject to laws affecting the collection, recording and distribution of patient information contained in the *Privacy Act 1988* (Cth) (***Privacy Act***). The *Privacy Act* contains a set of Australian Privacy Principles (**APPs**).

The *Privacy Act* applies to:

- public and private health service organisations; and
- individual health practitioners, whether they work in the public or private sector.

[31] *Public Records Act 1973* (Vic), s 2.

The requirements imposed by the *Privacy Act* in relation to the collection, holding, use or disclosure of a patient's health information do not affect any State or Territory law.[32] That is, to the extent of any inconsistency between a State or Territory law and the *Privacy* Act, the State or Territory law will prevail. It follows that telehealth providers will be primarily governed by the law of the State or Territory in which they practice.

3. *Health Records Act 2001* (Vic)

The *Health Records Act 2001* (Vic) (***Health Records Act***) applies to all health service organisations and individual practitioners in both the public and private sectors to the extent that they provide a health service in Victoria or are located in Victoria and collect, use or hold health information. All telehealth providers in Victoria (individuals and organisations), whether public or private, will also be subject to the laws contained in the *Health Records Act*.

The *Health Records Act* contains a State-specific set of Health Privacy Principles (**HPPs**) that are largely consistent with the national APPs. The HPPs apply to both the public and private sectors in Victoria, however the equivalent privacy principles in the Australian Capital Territory and South Australia only apply to public sector health organisations.

4. *Privacy and Data Protection Act 2014* (Vic)

The *Privacy and Data Protection Act 2014* (Vic) (***Privacy and Data Protection Act***) applies to all public health services. All public health organisations providing telehealth services will be subject to the requirements contained in the *Privacy and Data Protection Act*.

The *Privacy and Data Protection Act* contains a set of Information Privacy Principles (**IPPs**). These are largely consistent with the State-wide HPPs and nation-wide APPs.

All health service organisations and individual practitioners in Victoria are subject to both the *Privacy Act* and the *Health Records Act*.

Public health service organisations in Victoria are also subject to the *Public Records Act* and the *Privacy and Data Protection Act.*

Australian Privacy Principles and Health Privacy Principles

In relation to the provision of telehealth services, significant features of the Acts listed above are the APPs, the HPPs and the IPPs. Although the scope of these Acts differ, the APPs, the HPPs and the IPPs are substantially similar. As a result, all health service organisations and independent practitioners involved in providing telehealth services are subject to very similar requirements in

[32] *Privacy Act 1988* (Cth), s 3.

relation to the management of patients' health records. Set out below is a summary of the obligations of Victorian health services.

Protection of health information - transmission and storage

All health services (public and private) that provide services in Victoria must take all reasonable steps to protect the health information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.[33] This is the only current legal requirement in relation to the protection of health information. In order to comply with this requirement, it is vital that health organisations and health practitioners understand the inherent risks in electronic transmission of information - including potential issues of interference, loss, distortion or inadvertent disclosure. Having identified these risks, telehealth providers must then identify mechanisms to minimise and manage those risks.

Given the number of ways that health information might be transferred, disseminated and stored in telehealth arrangements, the requirement to take all reasonable steps to protect that health information might be slightly more onerous in the context of telehealth than in the context of traditional, face-to-face health service provision. As such, health practitioners and organisations must make individual decisions about how they will provide telehealth services in practice. These decisions must be made following careful consideration of the risks, and after ensuring that the organisation or individual practitioner has the technological resources necessary to guard against those risks.

For example, in the case of transmission of information via a live video consultation between the patient and the telehealth provider, both health organisations might have to do the following in order to be considered to have taken all reasonable steps to protect the health information:

- ensure the rooms in which the patient and the telehealth provider are exchanging this information has restricted access for the duration of the consultation; and
- ensure that the transmission systems are secure and reviewed on a regular basis.

In the case where diagnostic images are transmitted from a computer in a rural health service to a specialist's smartphone for emergency medical advice, the legal obligation to take reasonable steps might require different steps to be taken by each of the health providers.

The host provider will be required to have systems in place to ensure that the health information is in fact sent to the correct telephone number. This might be done by:

- using a trusted source such as the National Health Service Directory (**NHSD**) (which includes the End Point Locator Service (**ELS**)) and/or the National Telehealth Connection Service (**NTCS**) to identify and confirm the correct contact details;

---

[33] APP 11.1 (a) and (b), Schedule 1 *Privacy Act 1988* (Cth); HPP 4.1, Schedule 1 *Medical Records Act 2001* (Vic).

- creating a directory of registered telehealth providers who agree to be on call to provide "mobile telehealth services" and setting up direct links to the telehealth provider's telephone number; and/or

- contacting the telehealth provider prior to sending any information to confirm that they are available to provide the emergency "mobile telehealth service" required, and confirming their telephone number/email.

Telehealth and host providers wishing to provide telehealth services using a smartphone or any other portable device might be required, if available, to use a commercially supported application that has a reasonable set of inbuilt and automated security and privacy controls in order to discharge the obligation to take reasonable steps to protect the health information. Because this is as yet an untested area of law, these are neither clear nor definitive legal requirements. Rather, they should be taken as suggestions for health organisations to consider when developing policies for the implementation of telehealth.

Trans-border data flow

Pursuant to the *Health Records Act 2001* (Vic)[34] a health service or a person employed by it may transfer information about a patient to someone outside Victoria only if:

(a) the heath service or person reasonably believes the recipient is subject to obligations similar to the HPPs of the *Health Services Act*; or

(b) the patient consents to the transfer; or

(c) all of the following apply:

  (i) the transfer is for the benefit of the patient;

  (ii) it is impracticable to obtain the patient's consent;

  (iii) if it were practicable the patient would likely consent; or

(d) the health service or employee has taken steps to ensure the information will not be held, used or disclosed by the recipient inconsistently with the HPPs; or

(e) the transfer is authorised by any other law.

Accordingly, when a Victorian health service and its employees are providing telehealth services involving the transfer of information to a recipient outside Victoria, the health service and its employees must ensure that these prescribed conditions are met.

---

[34] HPP 9.

Form of health records

There are presently no legal requirements pertaining to the form in which health records are to be retained. That is, provided that the records are adequate and suitably protected, it is irrelevant whether they are kept in paper form, electronic form, or both.

There is a widespread movement towards electronic record-keeping, which should prove beneficial in relation to records pertaining to and shared via telehealth. Similarly to the way in which records are made and kept in a traditional face-to-face consultation, written or typed notes are also likely to be sufficient in the telehealth context. It is unlikely that host providers of telehealth and telehealth providers will be required to keep video or audio recordings of telehealth consultations, although it is not unlawful to do so.

Who is responsible for keeping and managing an individual's health records?

In Victoria, the HPPs provide that health service organisations and individual practitioners must keep medical records for their patients for at least 7 years after the last occasion on which it provided a health service to the patient.[35] In other words, a health service organisation or individual practitioner that provides medical services to a patient must keep records of the services provided and will be responsible for the appropriate management of those records.

The question of who is responsible for the management of an individual's medical records in the provision of telehealth is less clear than in the traditional provision of health services. In the traditional arrangement, one health service provider provides a single service to an individual. A patient may be referred from one provider to another for different services, for example, from a general practitioner to a radiologist. The general practitioner and the radiologist in that scenario are providing different medical services to the patient. In that case, each provider is obliged to keep accurate records of their respective consultations.

In the context of telehealth, who is responsible for the management of a patient's health records depends upon the nature of the telehealth arrangement. For example, where responsibility lies will differ between Scenarios 1 and 3, and Scenarios 2 and 4.[36]

In Scenarios 1 and 3[37], the telehealth provider might not be required to create a record of the advice it gave the rural health service, because if the patient was not directly consulted, the telehealth provider is not required to create a file for the patient (and would not be subject to the same requirements regarding retention of records and so on). Although there is no requirement for the telehealth provider to keep a record, it might nevertheless be in their interests to do so.

---

[35] HPP 4.2.

[36] Refer to "*Scenarios*" section of this guide.

[37] Refer to "*Scenarios*" section of this guide.

In Scenarios 2 and 4[38], the tertiary health institution or the private specialist provides advice directly to the patient. In these situations, the telehealth provider will be responsible for creating and maintaining records of the service provided by them. This is because the patient effectively becomes the patient of the telehealth provider; the telehealth provider is the primary provider of health services for the relevant consultation. If the telehealth provider is providing services from a different State or Territory to the patient, the telehealth provider will be subject to the laws of the jurisdiction in which they practice. This applies to the manner in which records are kept and disposed of as well as the period for which they are to be retained.

There is no legal requirement for the telehealth provider to send the records it creates to the host provider. However, an arrangement can be made between the host provider and the telehealth provider to share records following the telehealth consultation. Alternatively, the telehealth provider may choose to post a record to a common repository, such as a personally controlled electronic health record (discussed below) or a shared care plan.

Requirements for the retention of health records apply equally to telehealth providers as to other health practitioners such as a general practitioner who regularly consults the patient. For this reason, it is advisable that a practitioner who provides telehealth services via a smartphone or other portable device should transfer any health information it receives onto a more secure computer system.

Period of retention for health records

Under the *Public Records Act*, the Public Records Office of Victoria (**PROV**) is responsible for issuing guidance and direction in relation to the retention and destruction of records held by State Government agencies. It does this by issuing Retention and Disposal Authorities (**RDAs**). The RDAs specify various retention periods for various classes of documents.

Public health services are required to comply with the *Public Record Office Standard PROS 11/06 Retention and Disposal Authority for Patient Information Records*. This document can be found at http://prov.vic.gov.au/wp-content/uploads/2011/09/PatientInformationRDAWebVersion20110916.pdf.
PROS 11/06 specifies functional classes of records and categorises the disposal action for each class as either permanent or temporary. It then specifies a minimum retention period for records with a temporary status (after which time these records may be destroyed) and custody arrangements for permanent records:

- *Permanent disposal action category*

  These are generally to be transferred to the PROV after their administrative use by the organisation is concluded. Examples include incident registers, patient registration forms and residential care registers.

[38] Refer to "*Scenarios*" section of this guide.

- *Temporary records*

  PROS 11/06 specifies a range of timeframes the documents must be retained depending on the type of document. Examples of documents falling within this category include patient histories, treatment plans and imaging media (such as x-rays, MRIs). The timeframes range from 2 to 25 years. Most of the records that are required to be retained for 25 years relate to newborns. Most records relating to adults are required to be retained for 12 years after the last date of attendance.

  A health service could comply with the *Public Records Act* and the relevant RDA if it kept all temporary records for the longest period specified for any record - that is, up to 25 years after the last entry. However, this would be unnecessarily long for most records. It is only obliged to retain each record according to the time period specified in the RDA for that category of record.

Destruction and disposal of health records

A health service provider may destroy a patient's health information after the required period of retention if:

- the health service provider no longer needs the information for any legitimate purpose; and
- the information is not contained in a Commonwealth record; and
- there is no law, court order or tribunal order requiring the health service to retain the information.

In these circumstances, a health service may (but is not required to) also keep a patient's health information in a de-identified form.

Telehealth providers who retain patient records are subject to the requirements relating to destruction and disposal of those records. These destruction and disposal requirements apply whether or not the telehealth provider was legally required to retain the records.

Breach of the Health Records Act

Complaints regarding breaches of the *Health Records Act* can be made to the Health Services Commissioner, who may refer complaints to the Victorian Privacy Commissioner or the Ombudsman or to the Victorian Civil and Administrative Tribunal. If the Commissioner is satisfied that there has been an interference with a patient's privacy, the Commissioner may require action to be taken to remedy the complaint. It is an offence to fail to comply with a compliance notice. A penalty of 3000 penalty units may be imposed on a body corporate for such failure to comply; 600 penalty units may

be imposed on an individual for failure to comply.[39] In the financial year from 1 July 2014 - 30 June 2015, one penalty unit in Victoria is the amount of $147.61. The value of a penalty unit for each financial year is fixed by the Treasurer[40] and can be found online on the Victorian Legislation and Parliamentary Documents website, http://www.legislation.vic.gov.au/.

Personally controlled electronic health record

Since 2012, patients have had the opportunity to register for a personally controlled electronic health record (**PCEHR**). This is a separate record from the patient's electronic medical record. The fact that a patient has a PCEHR does not affect a medical practitioner's obligation to keep accurate records for the patient. The PCEHR should be used as a secondary record of information only.

Access to a patient's records through the patient's PCEHR may be useful in the provision of telehealth services, particularly if the host provider has not already converted their record-keeping system to an electronic system.

Any issues with the PCEHR system or Patient Identifiers are referred to the Office of the Australian Information Commissioner (**OAIC**).

---

[39] Section 71 *Health Records Act 2001* (Vic).

[40] *Monetary Units Act 2004* (Vic).

INSURANCE AND INDEMNIFICATION

Key Points

- Under an insurance policy issued by Victorian Managed Insurance Authority (**VMIA**), Victorian public health services are indemnified for claims arising directly out of health care services, which includes telehealth.
- Subject to one exception, employees of Victorian public health services are indemnified by VMIA when:
  - providing advice, care or treatment to patients of their employer health service or patients of another Victorian public health service; and
  - providing advice to another healthcare facility, whether or not a Victorian public health services.

  The exception is employee medical practitioners who provide treatment (as distinct from advice) to a non-Victorian public healthcare facility. In those circumstances, the medical practitioner will need to turn to their own insurance.
- For those medical practitioners requiring cover for their private patients, most of the policies of the major medical indemnity providers in Australia are broad enough such that telehealth services would fall within the ambit of cover. Nevertheless, there are variances and medical practitioners (in telehealth) ought to check their indemnity arrangements

PUBLIC HEALTH SERVICES

This section covers the arrangements that are in place to indemnify Victorian public health service organisations and their employees in the event of claims for injury arising out of telehealth services.

Victorian public health service organisations

Under a medical indemnity master insurance policy issued by Victorian Managed Insurance Authority (**VMIA**)[41], Victorian public health services are, subject to the terms of the policy, indemnified in respect of claims against them seeking compensation for injury arising directly out of health care services provided by them. This includes telehealth.

The health service is covered whether it treats the patient publically or privately, however there is a slight difference in the cover.

[41] The insurance policy can be accessed via https://www.vmia.vic.gov.au/insure/policies/medical-indemnity.

Treating public patients

When treating public patients of its own, or of another Victorian public health service, the health service is entitled to indemnity in respect of claims made against it. This includes whilst delivering health services by telehealth and is irrespective of whether the health service is the host provider or the telehealth service provider.

Treating private patients

When treating its own private patients, the health service is entitled to indemnity in respect of claims made against it. However, it is a condition of the insurance policy that the private practitioner treating the patient at the health service must be appropriately credentialed and have their scope of clinical practice defined by the health service otherwise the health service risks not being indemnified.

The private practitioner treating the patient is not entitled to indemnity from VMIA and must look to their own insurance cover.

The health service is also entitled to indemnity in respect of advice (but not treatment or care) given to a patient of another healthcare facility that is not a Victorian public health service or organisation. It is only entitled to indemnity in respect of care and treatment provided by that other healthcare facility if it has first secured the agreement of VMIA to cover it for such treatment and care.

What does this mean in respect of telehealth services?

In all four scenarios[42] each of the health services referred to therein (whether they be the host provider or the telehealth service provider) are entitled to be indemnified by VMIA for claims made against them by patients for injury arising out of telehealth services.

Employees of Victorian public health service organisations

Employees of those Victorian public health services holding a policy of insurance with VMIA are entitled to indemnity by VMIA under their employer's VMIA insurance policy whilst providing health care services (including telehealth services) to patients of the health service.

In respect of providing advice to another health service (public or private) or care, treatment or advice to a patient of another health service (public or private) or to a medical practitioner, the following applies:

- Employee registered medical practitioners of a Victorian public health service are indemnified by VMIA whilst providing treatment, care or advice to a public patient of another Victorian public health service.

[42] Refer to "*Scenarios*" section of this guide.

- Employee registered medical practitioners of a Victorian public health service are indemnified by VMIA whilst providing advice to another health service[43], not being a Victorian public health service, or to another Australian registered medical practitioner in respect of care of the patient of that other health service or other registered medical practitioner.

- Employees of a Victorian public health service who are not registered medical practitioners are indemnified by VMIA when providing advice to another Victorian public health service about the treatment of a patient of that other Victorian public health service.

- Employees of a Victorian public health service who are not registered medical practitioners and who provide treatment, care and advice to a public patient of another Victorian public health service are entitled to indemnity under the VMIA policy but, strangely, not the policy of the employer health service but of the health service to whose patient the employee is providing treatment, care or advice.[44]

- Employees of a Victorian public health service who are not registered medical practitioners are indemnified in respect of the advice they give another health service[45], not being a Victorian public health service, or a patient of that other health service, but are not indemnified in respect of any treatment or care (as distinct from advice) they give to the patient of that other health service.

This all seems quite complex, but, subject to one exception, the net effect is that employees of Victorian public health services are indemnified when:

- providing advice, care or treatment to patients of their employer health service or public patients of another Victorian public health service; and

- providing advice to another healthcare facility whether or not a Victorian public health service.

The exception is employee medical practitioners who provide treatment or care (as distinct from advice) to private patients of another Victorian public health service or to patients of a healthcare facility which is not a Victorian public health service. Those medical practitioners are indemnified by VMIA for advice so given, but not any treatment or care. Those medical practitioners will need to have their own insurance cover if they are to provide care or treatment in such circumstances. (See following section "*Health practitioners individually*".)

---

[43] "Another health service" includes interstate and international (excluding USA and Canada) health services but not in respect of claims issued in a court outside the Commonwealth of Australia, Papua New Guinea or New Zealand.

[44] If the claim is in respect of advice given by the employee, the employee is entitled to indemnity under the VMIA policy held both by the employee's employer and the policy held by the Victorian public health organisation whose patient the employee is providing services to.

[45] "Another health service" includes interstate and international (excluding USA and Canada) health services but not in respect of claims issued in a court outside the Commonwealth of Australia, Papua New Guinea or New Zealand.

INDIVIDUAL HEALTH PRACTITIONERS

Any health practitioner involved in providing health services not covered by a VMIA policy will be required to have their own medical indemnity cover. Most health practitioners involved in such activities have such cover. It is a requirement by AHPRA for registration that a health practitioner have such insurance cover.

Medical practitioners

At the time of writing, a review of the medical indemnity policies of some of the major medical indemnity providers in Australia[46] reveals that each either specifically includes cover for provision of telehealth services or the wording is broad enough such that telehealth services would fall within the ambit of cover. There are, however, geographical limitations. More specifically:

- Avant - specifically includes telehealth services but excludes services provided to patients outside Australia.
- MDA National, MIGA and MIPS - make no specific reference to telehealth services but the policy wording is wide enough such that the medical practitioner would be entitled to indemnity in respect of scenario 3, but perhaps not in scenario 4, although in respect of scenario 4 the medical practitioner would be entitled to indemnity from VMIA, the public health services insurer.

Medical practitioners practising telehealth and who are doing so not as an employee of a Victorian public health service ought to check their indemnity arrangements.

HOW THESE INSURANCE ARRANGEMENTS APPLY TO THE FOUR TELEHEALTH SCENARIOS

In summary, all Victorian public health services and their employees are, under indemnity arrangements with VMIA, entitled to indemnity for claims for injury arising out of the provision of telehealth services in each of the scenarios set out in the "*Scenarios*" section of this guide. Health practitioners providing services not covered under those arrangements will be indemnified under their own insurance arrangements assuming they have taken out such insurance as they are required to do as a condition of their registration with AHPRA.

More specifically, looking at the four scenarios the insurance cover arrangements are as follows:

Scenarios 1 and 2

- The host provider (rural health service) is entitled to indemnity from VMIA under the rural health service's insurance policy with VMIA.

[46] Avant, MDA National, Medical Indemnity Group Australia (MIGA) and Medical Indemnity Protection Society (MIPS)

- The treating doctor at the host provider site is entitled to indemnity from VMIA under the host provider's insurance policy with VMIA.
- The tertiary health service providing the telehealth service is entitled to indemnity from VMIA under the tertiary health service's insurance policy with VMIA.
- The doctor at the tertiary health service is entitled to indemnity from VMIA under the tertiary health service's insurance policy with VMIA.

Scenario 3

- The host provider (rural health service) is entitled to indemnity from VMIA under the rural health service's insurance policy with VMIA.
- The private specialist orthopaedic surgeon is entitled to indemnity from VMIA under the rural health service's insurance policy with VMIA. That private specialist orthopaedic surgeon might also be entitled to indemnity under their own medical indemnity policy in the event that they have one.

Scenario 4

- The host provider (rural health service) is entitled to indemnity from VMIA under the rural health service's insurance policy with VMIA.
- The private specialist is not indemnified by any VMIA policy and must look to the specialist's own medical indemnity cover (required for registration under AHPRA) for indemnity.