



Prepared for
**Department of Health and
Ageing**

Subject
**Telehealth Business Case,
Advice and Options
Final Report**

28 June 2011
UniQuest Project No: 16807

UniQuest Pty Limited



UniQuest Pty Limited
Consulting & Research
(A.B.N. 19 010 529 898)

Level 7, GP South Building
Staff House Road
University of Queensland
Queensland 4072

Postal Address:
PO Box 6069
St Lucia
Queensland 4067

Telephone: (61-7) 3365 4037
Facsimile: (61-7) 3365 7115

Title
Telehealth Business Case, Advice and Options - Final Report

Author's Declaration

This report/proposal has been prepared in accordance with UniQuest's Quality Management System, which is compliant with AS/NZS ISO 9000:2000.

The work and opinions expressed in this report are those of the Authors.

Authors:

Prof. Len C Gray
A/Prof. Anthony C Smith
Dr Nigel R Armfield
Dr Catherine Travers
Prof. Peter Croll
Dr Liam J Caffery

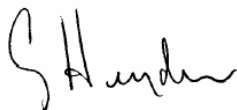
Internal review and quality assurance:

Prof. Anthony Maeder

We acknowledge contributions by:

Ms Natalie Bradford
Dr Sisira Edirippulige
Mr Adam Mothershaw
Dr Jasper Van der Westhuyzen

Signed for and on behalf of UniQuest Pty Limited



.....
Gary Heyden – General Manager
UniQuest Signatory
UniQuest Project No: **16807**

TABLE OF CONTENTS

Glossary..... 4

Section 1 Executive Summary 5

1.1 Introduction..... 5

1.2 Methods..... 5

1.3 Contemporary use of telehealth..... 5

1.4 The case for telehealth..... 6

1.5 The need for an iterative implementation 6

1.6 Security, privacy and authentication..... 7

1.7 Interoperability and integration..... 7

1.8 Hardware and software requirements 7

1.9 Clinician discretion in the use of telehealth 8

1.10 Change management..... 8

1.11 Strategic recommendations..... 8

Section 2 Business Case 11

2.1 Background..... 11

2.2 Benefits 12

2.3 Business requirements..... 14

2.4 Use cases 16

2.5 State of readiness..... 19

 2.5.1 *Infrastructure* 19

 2.5.2 *Stakeholders*..... 20

 2.5.3 *Vendor groups*..... 21

 2.5.4 *Governance arrangements* 21

 2.5.4.1 *Effective management of implementation* 22

 2.5.5 *Estimated timeline to achieve readiness* 25

2.6 Performance and monitoring 26

- 2.7 Risks28**
- 2.8 Gap analysis29**

- Section 3 Advice and Options 33**

- 3.1 Security, privacy and authentication.....33**
- 3.1.1 Background 33
- 3.1.2 Legislation 34
- 3.1.3 Privacy protection 35
- 3.1.4 Assessing risk..... 39
- 3.1.5 Security, privacy and authentication framework for telehealth..... 50
- 3.1.6 Recommendations..... 56
- 3.2 Interoperability and integration.....59**
- 3.2.1 Interoperability 59
- 3.2.2 Integration 61
- 3.2.3 Practice management systems 62
- 3.2.4 Desktop clinical systems..... 63
- 3.2.5 Scheduling and co-ordination systems..... 64
- 3.2.6 Summary 65
- 3.3 Hardware, software and support.....66**
- 3.3.1 Medium to long-term functional requirements 66
- 3.3.2 Medium to long-term non-functional requirements 66
- 3.3.3 Supporting systems 67
- 3.3.4 Supporting processes 68
- 3.3.5 Technical requirements 70
- 3.3.6 Technical options..... 74
- 3.3.7 Recommendations..... 94
- 3.4 Change management.....95**
- 3.5 Initial costing97**

- Section 4 Recommendations 99**

- 4.1 Strategic recommendations99**
- 4.2 Governance arrangements..... 103**
- 4.3 Performance and monitoring recommendations 104**

4.4 Security and privacy recommendations 105

4.5 Interoperability and integration recommendations 108

4.6 Hardware, software and support recommendations 109

4.7 Technical Recommendations 110

4.8 Technical Option Recommendations 111

Appendix 1 Bandwidth Requirements - Published Studies 113

GLOSSARY

ADSL	Asymmetric Digital Subscriber Line
AR	Assessment Recommendation
COH	Centre for Online Health
DoHA	Department of Health and Ageing
EHR	Electronic Health Record
FPS	Frames Per Second
FR	Functional Requirement
GAR	Governance Arrangement Recommendation
GP	General Practitioner
IIR	Interoperability and Integration Recommendation
ISDN	Integrated Services Digital Network
HD	High Definition
HSSR	Hardware Software and Support Recommendation
NFR	Non-functional Requirement
MBS	Medicare Benefits Schedule
MCU	Multipoint Control Unit
PC	Personal Computer
PCEHR	Personally Controlled Electronic Health Record
PMR	Performance and Monitoring Recommendation
QoS	Quality of Service
SD	Standard Definition
SIP	Session Initiation Protocol
SPR	Security and Privacy Recommendation
TOR	Technical Option Recommendation
TRR	Technical Requirement Recommendation
UQ	The University of Queensland
VC	Video Conferencing

SECTION 1 EXECUTIVE SUMMARY

1.1 Introduction

In August 2010, the Australian Government made an important and significant commitment to support Medicare benefits for online consultations, in general practice and across a range of health specialties, with a specific focus on video-consultation.

In November 2010, the Department of Health and Ageing commissioned UniQuest to provide expert advice and options to assist in establishing appropriate arrangements to facilitate the introduction of video-consultation. UniQuest represents researchers and technical experts based at, and affiliated with, the Centre for Online Health at The University of Queensland. The consultancy was funded by the Department of Health and Ageing.

1.2 Methods

The consultants undertook a variety of tasks in the preparation of this report: A review of the international and domestic peer-reviewed, web and grey literature; consultation with key stakeholders, including peak organisations representing clinicians and the eHealth / video-conferencing (VC) industry, and state and territory governments; a survey of general practitioners; and consultation with independent expert advisors.

The key findings of the investigations are as follows:

1.3 Contemporary use of telehealth

Telehealth around the world, and in Australia, is currently focussed on specialist consultation to patients in rural and remote locations. It concentrates on selected medical specialties, which are least compromised by the limitations associated with video-consultation. In most services, (relatively expensive) hardware video-conferencing equipment is utilised. This equipment typically complies with international telecommunication standards (referred to as “standards-based” in this report) and offers a high degree of interoperability between vendors. Considerable financial support and economies of scale are required to ensure effectiveness and viability in services that use hardware-based video conferencing. For similar reasons, many services are based in, or are associated with, hospitals. Very little

information was identified in relation to general practice or personal computer (PC) based video-conferencing, most likely suggesting very low use.

1.4 The case for telehealth

There are powerful arguments for the widespread use of telehealth, including video-consultation. The greatest advantage, in the short-term, rests with patients and practitioners located in rural and remote locations. Advantages include minimising the need for travel for patients (thus improving equity of access to health care). However, financial savings will occur primarily to individuals (except through less disruption to work attendance), rather than to health services. Health services will only secure gains where they currently bear the cost of patient transport, or when the patient is in hospital, through shorter hospital stays, if more timely specialist advice is available.

The advantages are amplified for people with chronic illness (need for repeat visits) or disability (need to have an escort – paid or family member – to attend a consultation). This applies to persons located at home, as well as in institutional settings (residential aged care facilities and hospitals). As the cost of video-consultation declines and its quality improves its use will become more ubiquitous and advantages will emerge for people living in metropolitan areas.

1.5 The need for an iterative implementation

Because the lead time to the availability of MBS benefits is short, in the immediate short-term, a pragmatic approach to implementation which makes use of readily available, off-the-shelf technical options is required, accepting that these options may not be the best fit to all of the requirements of telehealth. By implication, this will impact on the type of telehealth interactions that can be recommended as sufficiently safe, effective, secure and private in the short-term. In the medium-term, allowing for development time and experience with the short-term implementation, a solution for sustainable pervasive video consultation can be achieved.

The implementation of telehealth video consultations should be seen as an iterative process that will require a number of years of gestation before maturity will be reached.

1.6 Security, privacy and authentication

When clinical consultations occur at a distance, a special range of issues in relation to security, privacy and authentication emerge. Data in the form of video and audio, as well as clinical data are transmitted between locations, all of which are exposed to the risk of interception. A variety of solutions are available to minimise this risk.

1.7 Interoperability and integration

Clinicians operate in heterogeneous environments, where access to equipment, software and connectivity vary considerably. To achieve widespread use of VC, it is important that all endpoints are able to communicate. This implies the use of standards-based video conferencing endpoints, or gateway facilities to allow interoperability between proprietary systems and standards-based systems. In the short-term, tight integration with other software based systems (such as practice management systems) is unlikely to be necessary; however in the medium to long term, such integration would be beneficial.

1.8 Hardware and software requirements

Ideally, for clinical consultations, there is a minimum VC hardware, software and environment configuration required to ensure an acceptable patient experience, clinical accuracy and safety, security and privacy, interoperability, audit and billing.

Both hardware and software-based options are readily available. Hardware solutions typically implement international telecommunications standards to ensure interoperability between vendors. Some proprietary hardware-based video conferencing systems are commercially available however they account for a negligible market share and there are few such systems known to be in use to deliver telehealth services.

A variety of PC based software applications (including standards-based and proprietary solutions) are available. None of the currently available solutions meet all of the longer-term functional and non-functional requirements of video consultation identified by this report. A hardware-based system is ideal for clinical applications but may be considered expensive for a standard doctor's surgery, unless usage is very high. PC based solutions are relatively inexpensive, and some products are available at no cost, but there is currently insufficient evidence that such products meet state and federal privacy and security requirements, or that they are safe and effective for diagnostic use or for complex management.

Acknowledging this, clinicians will need to choose what particular telehealth system meets their clinical requirements.

However, with the appropriate incentives, and a growing market, it is likely that more suitable solutions may be achievable within the next few years.

1.9 Clinician discretion in the use of telehealth

This report makes recommendations on the minimum requirements for clinical telehealth interactions. However, the decision to use, or not to use, telehealth together with the choice of particular hardware or software methods for consultation should rest with the clinician. In making their choices, clinicians should consider any legal (privacy and security), safety and clinical effectiveness implications. The Divisions of General Practice, professional colleges, and peak representative bodies may have a role in supporting their members in making informed choices regarding the use of telehealth.

1.10 Change management

Experience has demonstrated that, in spite of the obvious appeal of video-consultation, and provision of suitable infrastructure, that take-up of VC has been generally low. Lack of funding for clinician time is often a barrier, but this will be overcome by the provision of a fee schedule on the Medicare Benefits Schedule (MBS). Successful VC requires education of health professionals, adjustment to administrative procedures, special scheduling and other changes to work flows and patterns.

1.11 Strategic recommendations

The implementation of video consultation will depend on the development of a range of processes and capabilities, some of which will be necessary and achievable in the immediate/short-term (0 to 3 years) and others in the medium to long term (3 to 6 years).

In the short-term, in some circumstances, contemporary PC and hardware based video conferencing systems may be used to provide video consultation.

In the longer term the development of fully featured health teleconsultation applications that may be used anywhere that there is a PC, webcam and good broadband network access would be beneficial. Applications could be designed to meet the full requirements of clinical video consultation.

Strategic recommendations arising from this report are as follows. Further information to support these recommendations is provided in Section 6:

- SR1** *Video-consultation should be phased in over several years, with a primary focus, in the first instance, on Patient-GP-Specialist interactions, reflecting well established telehealth practice.*
- SR2** *Home based VC could be considered in some scenarios as suitable systems become available, and after demonstrations have shown good levels of acceptability, reliability, security, safety and affordability.*
- SR3** *In the short-term, clinical consultations involving complex diagnostic and management decisions, where the patient is not accompanied by another health professional, may have to be limited until standards-based VC equipment is available for use at the patient endpoint. PC based equipment may be suitable at the health professional endpoint.*
- SR4** *PC based equipment may be appropriate at the patient endpoint when there is another health professional accompanying the patient, who can assist in diagnostic and management decisions.*
- SR5** *In hospitals and residential aged care facilities, where there is a high probability of diagnostic uncertainty and where complex medical decisions may be required, dedicated VC equipment should be utilised at the patient endpoint. PC based equipment may be suitable at the health professional endpoint.*
- SR6** *Until demonstrations indicate otherwise and for the purpose of claiming MBS items for online consultations, VC at the patient endpoint should primarily occur in a health setting where conventional clinical consultations occur, to ensure authentication of the patient, and to provide technical and clinical assistance when required. This includes GP surgeries, community health centres, hospital outpatient clinics, hospital wards and residential aged care facilities.*
- SR7** *Colleges and other professional bodies should consider developing guidelines for the safe and effective use of VC by their members.*

SR8 *Funding for VC could be on the same basis as equivalent face to face consultations listed in the Medical Benefits Schedule.*

SR9 *Payments to compensate for the higher cost of VC and to encourage the use of VC could be introduced. This could include a loading to each consultation referred to in Recommendation SR8.*

SR10 *Additional “incentive” payments might be offered to GPs operating in rural settings to encourage their participation. In metropolitan areas, similar incentive payments could be offered when the consultation involves a person living in a rural setting or a person with significant disability. The latter group should include persons living in Residential Aged Care Facilities.*

SR11 *Telehealth service providers should periodically review and update their privacy practices, policies and notices to ensure that they adequately address the management of information gathered during telehealth consultations.*

SR12 *A successful telehealth implementation will require an active change management strategy. This would entail consultation with clinicians, the development of guidelines and marketing of the initiative.*

SECTION 2 BUSINESS CASE

In this section, the rationale for the introduction of video conferencing as a medium for clinical consultation in Australia is presented. The section considers the benefits of, and the business requirements for, introduction of teleconsultation.

2.1 Background

Telehealth, in a variety of formats, is established in Australia.

Common telehealth methods include:

- Video consultation between patients and health professionals (usually a specialist medical practitioner), with and without another health professional accompanying the patient;
- Video consultation between specialists and other health professionals, in both individual and in case conference configurations;
- Store-and-forward interactions involving images, or clinical data, where a specialist reviews and reports remotely.

These interactions involve both hospital inpatients and outpatient or ambulatory services. The majority of consultations in the ambulatory setting involve specialists located in, and affiliated with, hospitals.

The majority of existing telehealth activity is supported by state governments, or hospital networks predominantly funded by state governments. Although activity is relatively high, there are many reports which suggest that take-up has been sub-optimal. Explanations for this include failure to fund clinician time, lack of clinician interest, poor coordination, and technical deficiencies.

The Medical Benefits Schedule contains several items that relate to telehealth, primarily in the areas of psychiatry and radiology services. For psychiatry, items numbers exist for direct patient contact by telehealth but large scale take-up is yet to occur, despite rebates being available for six years.

Outside of the public hospital and associated outpatient settings, there has been very little activity in Australia. Involvement of General Practice in telehealth has been minimal.

The relative lack of telehealth activity outside of the public system could be explained by several factors:

- Lack of telehealth infrastructure, including equipment, software and shared health records;
- Lack of funding for clinician participation;
- Lack of economies of scale in general practice or private specialist settings;
- Absence of training, support and coordination functions;
- Low need outside of the public sector.

The current, significant Australian government initiatives to develop the National Broadband Network, to support shared electronic health records (through the Personally Controlled Electronic Health Record), and to fund clinician involvement in teleconsultation may mitigate several of these factors.

The emergence of low cost systems based on personal computers to support video-consultation may also serve to mitigate some of the barriers related to economies of scale.

2.2 Benefits

The majority of Australia's population is concentrated in larger cities, with smaller communities distributed across a large area. The distribution of health professionals does not mirror that of the general population, probably for two reasons: There are insufficient economies of scale (including insufficient numbers of patients) in regional centres and smaller communities to justify the presence of many types of health professional, particularly specialists. The greater the level of specialisation, the larger community is required to support the health professional. Thus, medical specialists are often absent in regional cities and towns, and GPs may not be available in small rural towns. Similar considerations apply to nursing and allied health professionals.

Secondly, for professional and social reasons, many health professionals prefer to live in large cities.

This mismatch of population results in less adequate access to health professionals for regional and rural communities. This lack of access is traditionally addressed by the patient visiting cities to access advice and management. In major emergencies, this access is usually facilitated by state emergency transport services. In non-emergency situations, there may be access to state services to support transport costs. However, this varies across

jurisdictions. Very often, the patient will need to bear the cost of travel, and the associated travel time, which may in turn disrupt work and other responsibilities.

When the patient is unwell or is disabled, and must be accompanied, the problem is amplified. Patients in small rural hospitals have limited access to specialists, unless there is a clear cut major indication (usually a need for ICU or surgery). Access can be a major issue, even when the distance to the health service is quite short. For example, the residents of residential aged care facilities require expensive escorts to visit specialists, even in metropolitan areas. Older or disabled people at home may have access difficulties, which increases as doctors are less inclined or able to make home visits.

This inequity of access to the best medical advice directly impacts on health status and productivity.

One strategy that is commonly used to address access issues is doctors travelling to the patient. Such visits vary from flying periodically to a remote location, to making a home visit in the city. While this appropriate for some clinical scenarios – non-urgent issues of a chronic nature – it is inadequate for many others, particularly complex diagnostic and management problems for patients in hospital.

While many rural public hospitals are now introducing VC to secure remote consultation, this is not possible in private hospitals, as there is no mechanism to remunerate the specialist, who would otherwise consult on a fee-for-service basis through Medicare.

Travel of specialists represents two other problems: Time consumed travelling effectively reduces the time available for the doctor to see other patients. Secondly, it is only feasible when a *group* of patients require consultation. Travelling large distances to see a small number of patients is not cost effective. As a result, smaller communities are unable to access visiting specialists.

Telehealth represents a major opportunity to overcome these access issues.

For patients, telehealth should:

- Improve access to health professionals;
- Reduce travel time to visit health professionals;
- Reduce the burden on carers and subsidised transport schemes for patients who must be accompanied to visit health professionals and
- Potentially improve clinical outcomes.

The extent of benefit will depend on the travel time to the health professional and the need for special transport arrangements and / or an escort (family member or health professional). It will therefore be of most benefit for people in rural and remote communities, and people with illness and disability for whom travel is difficult.

For health professionals, telehealth should:

- Reduce the travel time required to visit patients;
- Increase the range of specialist advice available;
- Increase the timeliness of specialist advice;
- Increase the scope of practice to include patients in more diverse locations.

For the health "system", telehealth should:

- Overcome inequities of access to health services;
- Reduce the expenses related to patient transport;
- Increase the self-sufficiency of health professionals;
- Increase the self-sufficiency of smaller institutions such as rural hospitals and residential aged care facilities which, in turn, will...
- Reduce the demand on emergency departments and larger hospitals.

2.3 Business requirements

The business requirements for the successful implementation of a viable telehealth video conferencing consultation solution include:

(a) Technical infrastructure

The following infrastructure is usually required:

- VC equipment which is easily accessible to patients – could be in the GP surgery, a local private or public hospital ambulatory clinic, or a community health centre;
- The technical requirements of the VC connection will be determined by the nature of the consultation. Higher requirements apply to situations where diagnostic work or complex management decisions are required, and situations where the patient is not accompanied by a healthcare professional. Currently, video consultations in these circumstances are best provided by hardware VC systems, with full remote camera control, being operated over reliable, high-speed, low-latency networks. In other circumstances, PC-based systems may be adequate. Therefore, we have categorised

VC capability into two classes: (i) *diagnostic quality* and (ii) *general quality*. [For a more detailed discussion of this aspect, refer to Section 3.3.6];

- Shared medical records (and / or record sharing through transmission of information) including interoperability between EHR and PCEHR systems, privacy, security, and authentication. Where such systems are unavailable or not yet mature, existing methods of sharing information at a distance (e.g. fax and secure email) may be appropriate;
- Physical environment for video-consultation. Ideally, the patient should be consulted in an environment similar to that in which conventional consultations occur. Unless no physical examination is contemplated, there may be a need to move the patient, demonstrate range of movements, examine gait, take blood pressure and so forth. In addition, attention needs to be paid to providing good lighting and sound proofing, possibly at a standard somewhat higher than a standard clinical consulting room. Telehealth rooms might be located in:
 - The GP surgery with a GP present;
 - A separate studio within the GP premises, when the GP is not present;
 - A local community hospital;
 - A community health centre.

(b) Telehealth enabled specialists

For GP to specialist referrals, there will be a need to develop a network of specialists who are telehealth enabled. Without this, GPs will have nobody to refer to. Ideally, specialists who serve the community in which the GP operates will arrange to provide a telehealth capability. Alternatively, there may be adjustment of the specialist “market” whereupon specialists who are telehealth enabled become preferred providers in particular communities. This is a critical issue for successful implementation of a telehealth program.

(c) Training & coordination

Widespread video-consultation is unlikely to occur without attention to several aspects of the process in the setup phase

- Practitioners will need access to short training sessions or courses to understand the various forms of teleconsultation

- Coordination
 - Processes to synchronise GP – Specialist live interactions will be difficult to manage, as both practitioners will need to be available simultaneously.
 - Interactions between a patient referred by a GP to a specialist will present less logistic difficulties, but there will still be a need for a “studio” to be “booked” at a remote location.
 - There will need to be adjustments to usual record keeping and billing procedures.

(d) Funding

Funding is required to support clinician engagement:

- The GP or specialist who is providing advice might be compensated on the same (time related) basis as for conventional in person consultations;
- Where the GP accompanies the patient in a video-consultation the GP will require compensation on a similar (time related) basis;
- A telehealth subsidy payment (per occasion of service) might be considered. [If and when telehealth becomes commonplace, this payment could be gradually reduced.]

It could acknowledge any or all of the following ingredients:

- Infrastructure costs related to VC equipment
- The cost of a staff member to chaperone the consultation
- An incentive payment to encourage access to telehealth

2.4 Use cases

The following scenarios have been constructed to illustrate how video-consultation might be utilised. All case studies are fictitious. They are based on either current practice, or in some cases, on speculation. The comments associated with each case indicate into which category each example fits.

Patient – GP interactions

- Patient at home, GP in clinic

Scenario 1: Mrs A, 79 years, has hypertension, diabetes and severe osteoarthritis of both knees. She lives alone in a small town 35 km from a regional centre, where her GP is located. Travel to the town is difficult, as there is no public transport and she does not drive. Her blood pressure, and random blood glucose readings are recorded remotely and uploaded to the GP practice. Remote monitoring and video consultation enable the majority of her regular follow appointments to be conducted at home.

Comment: Possible now, more likely to be common in 3-5 years. Probably requires diagnostic quality VC.

- Patient in hospital, GP in clinic

Scenario 2: Mr Smith, 63 years has Parkinson's disease and is admitted to the local rural hospital with a chest infection. On day 3, he is recovering but falls and has pain in the left thigh. His walking is limited. His GP is flat out with a fully booked clinic. He is able to visit the patient at the bedside using VC and make a more accurate assessment than is possible by telephone. He concludes that the patient has no serious injury after a nurse assisted examination, arranges some investigations and delays his visit to the hospital for several hours until after his clinic is concluded.

Comment: Possible now, more likely to be common in 3-5 years. Requires diagnostic quality VC.

- Patient in residential aged care facility, GP in clinic

Scenario 3: Mrs C is 85 years old and lives a high care residential aged care facility. Nursing staff think that she is unwell and request a visit from the GP whose surgery is 25 minutes away. His clinic is fully booked for the day. He visits the patient by VC and makes an assessment of illness severity. He suspects that the patient has significant respiratory or cardiac failure. He is able to recommend some urgent measures and arranges further assessment at the emergency department of the local hospital.

Comment: Possible now, more likely in 3-5 years. Requires diagnostic quality VC.

GP – Specialist interactions

- Patient accompanied by GP, specialist in clinic

Scenario 4: Mr W aged 61 lives in outer Melbourne. His wife reports that he is snoring loudly and the GP is concerned that he has obstructive sleep apnoea. He is referred to a sleep specialist who sees him in person, and arranges sleep studies. However, the follow-up visit is conducted by VC in the GP's clinic with the patient, his wife and GP present. Results of the studies are demonstrated by VC, and further treatment plans negotiated.

Scenario 5: Mrs Y aged 57 has diabetes mellitus, which is proving difficult to control. Her GP refers her to a specialist 6 hours driving time away. She does not drive. A consultation with the endocrinologist is conducted by VC in the GP clinic. The GP is able to assist with provision of additional clinical information and aspects of the physical examination. Insulin is recommended, and the practice nurse is engaged to assist with the starting regime, and patient education. Two subsequent consultations are required with the endocrinologist, which involve the practice nurse and the patient, each conducted by VC.

Comment: Currently operating but unfunded. Requires general quality VC.

- Patient unaccompanied (but referred by GP), specialist in clinic

Scenario 6: Mr J, aged 69, lives with his wife in a remote town where there is a GP and community health centre. His wife is concerned that he is developing dementia. His GP refers him to a memory disorders specialist located 8 hours travelling time away. A consultation is conducted by VC in the studio located at the community health centre. Two follow up consultations are conducted in the same manner. He is diagnosed with early Alzheimer's disease and recommended medication is prescribed by his GP.

Comment: Currently operating in public sector, unfunded in private practice. Requires diagnostic quality VC.

- Patient in hospital, specialist in clinic

Scenario 7: A private hospital rehabilitation service in a regional city has been unable to recruit a suitable specialist. A city based specialist conducts regular ward rounds using mobile wireless VC, ad hoc consultations when required and participates in a weekly multi-disciplinary team meeting. He is accompanied on rounds by a ward nurse.

Scenario 8: The same hospital does not have access to a neurologist. Neurological consultations are required once or twice a month. A city based neurologist can be consulted

by VC. The attending GP is usually able to be present when the consultation occurs, and is able to assist in examination and implementation of recommendations.

Comment: Both of these services are feasible now. Requires diagnostic quality VC.

- Patient in residential aged care facility

Scenario 9: Mrs Z, aged 91 years, lives in a residential aged care facility. Over the past 4 weeks, she has developed an increasingly severe skin condition. Her attending GP is uncertain of the diagnosis, and refers her to a dermatologist. High quality images are submitted to the teledermatology service and a clinical diagnosis is established. The dermatologist communicates with the patient and staff about the complicated treatment regime, via VC.

Comment: Available now, but unfunded. Requires diagnostic quality VC.

2.5 State of readiness

2.5.1 Infrastructure

Considerable video and networking infrastructure exists within the state health departments and may be available for use, subject to access agreements. Little video infrastructure exists in the private health care sector and new hardware, software and suitable communications infrastructure will be required (both to, and within practices) to equip GPs and specialists to provide video consultations.

The public Internet is not yet pervasive and performance is variable. The NBN is predicted to address these issues.

Diagnostic quality VC is relatively expensive, and thus requires considerable volume of use to justify its availability. Present diagnostic quality VC is therefore likely to be restricted to locations where considerable use is expected: hospitals; large clinics; and possibly residential aged care facilities. As PC based VC develops, together with rollout of the NBN, diagnostic quality VC may become available in a much lower cost format, potentially extending its availability to general and specialist practice consulting rooms. However, at the present time, these settings are likely to be restricted to general quality VC.

Estimated timeline to achieve readiness

Using standards-based hardware or software options, installation is feasible in the short-term. Current video implementations do not support all of the functional and non-functional requirements for telehealth identified in this report. It is anticipated that it may take 3 to 5 years to develop a dedicated health application which satisfies all of the requirements described. Meanwhile, telehealth may still be practiced in the short-term, with contemporary hardware and software systems, subject to caution and limitations.

Where available, broadband may also be installed in the short-term. The NBN (and hence pervasive, high-speed broadband) will not be available in the short-term. While the NBN will be rolled out progressively, some recent reports have indicated that it may take ten years for the implementation to be completed.

2.5.2 Stakeholders

In general, current involvement of specialists in telehealth is modest. For GPs telehealth experience is very limited most current activity relates to select subspecialties where aspects of the work are well suited to VC: psychiatry, dermatology, wound care, etc. Most activity occurs within the public hospital system, and relates to both inpatient and ambulatory care. Those specialists currently involved in telehealth in these contexts are the most likely to expand their activity to a Medicare funded fee-for-service setting, in the short-term. They are familiar with the process, are likely to have access to technical infrastructure, and have established relationships with referring GPs and organisations.

On the other hand, take-up by clinicians who are not to date involved in VC is likely to be slow, for the following reasons:

- Diagnostic quality VC equipment, best suited to clinical work, is expensive and must be shared among groups of clinicians to be cost-effective.
 - Clinicians are already busy, and VC, in isolation, will not result in improved efficiency of their activities. If room changes and setup time are required, efficiency may be reduced.
 - Referral networks that currently exist between GPs and specialists may not be replicated by VC networks.
- If a rural GP has a relationship with a particular city based specialist, and that specialist is not able or interested in VC, then the GP will need to adjust his referral pattern.

- Similarly, if a city-based specialist decides to participate in VC, he must then establish a “market” of referral sources to justify the investment. Existing referring GPs may not be able or be interested in establishing a VC capability at the patient endpoint. He would then need to establish new sources of referral for VC purposes.

Even if significant financial incentives are provided to encourage the use of VC, usage rates will develop gradually, due to the large number of factors that need to be in place for successful implementation. These apparent “barriers” will be progressively mitigated over time, as the cost of diagnostic quality VC declines, as clinicians become aware of the potential of VC, as patients request alternatives to travel, and as referral practices and patterns adjust to this new approach to consultation.

Estimated timeline to achieve readiness

Some clinicians may be ready, with suitable technology and interest in video consultation, to practice in the short-term. However, take-up is usually slow in telehealth implementations and it is likely to take a number of years before there is a critical mass of specialists and referring GPs who are suitably equipped and interested in practicing by video. From the patient perspective, there are likely patients who would participate in Medicare supported video consultation today, if it were available.

2.5.3 Vendor groups

In Australia, there are many established commercial providers of VC hardware, software, education and support. These vendors would be able to provide suitable products and would likely negotiate volume discounts (noting that actual supply would be subject to product availability).

Estimated timeline to achieve readiness

Vendor groups are ready today.

2.5.4 Governance arrangements

The addition of video consultation to the MBS, beyond tele-psychiatry and case conferencing, is new and therefore consideration should be given to appropriate governance arrangements. These arrangements will be required to mitigate risks and to ensure:

- That the implementation is managed effectively;
- That the resulting service is secure, private, safe and effective; and
- That it provides an overall sustainable, cost-effective investment of public funds.

These three issues are covered in the following sections with recommendations.

2.5.4.1 Effective management of implementation

Issue

Whether as a nationally managed, regional or local initiative, to be successful, the implementation of video consultation may require a range of issues to be carefully considered. In doing so, specific expertise in a number of areas will be required:

- Technical
 - Assessment of the suitability of products
 - Security and privacy audit of providers

- Administrative
 - Negotiation of bulk purchase vendor agreements for equipment and support
 - Establishment of support functions for clinicians
 - Establishment of MBS item numbers
 - Establishing new MBS processes and interfaces

- Marketing
 - Development and execution of a marketing plan for GPs and specialists
 - Development and execution of a marketing plan targeting patients

- Education and training
 - Development of practice guidelines for clinicians
 - Development and delivery of video consultation training

- Assisting practices in their implementation
 - Implementation advice
 - Equipment installation and configuration

➤ Adjustment of existing systems and workflow

As stated, each of these aspects will require specific expertise. In addition, overall co-ordination and project management will also be required during the implementation phase. Failure to attend to each of these individual aspects together with overall co-ordination will likely compromise the implementation. In addressing the above, the Divisions of General Practice and professional colleges and peak representative bodies are likely to have important roles to play in supporting their members in the introduction of telehealth into their practices.

Recommendations

GAR1 *To establish an effective telehealth service, suitably qualified individuals should be recruited to form a project management team which should be led by an experienced senior project manager.*

and

GAR2 *A high-level steering group should be established to provide oversight and advice during the implementation phase. This group should comprise representatives of stakeholder groups (executive, clinicians, and individuals with practical clinical telehealth and technology expertise).*

2.5.4.1 *Security, privacy, safety and effectiveness*

As is the standard in healthcare, it would not be appropriate to introduce a new intervention without assurance that it is safe, that it provides a benefit and that it meets legal requirements.

In the context of MBS supported telehealth, it is important to assess whether any proposed approach is safe, effective, secure and private. To do so will unavoidably require some national standardisation and regulation.

(a) Security and privacy

Issue

Video consultations raise issues of security and privacy. There is a need to ensure that all MBS funded activity meets all relevant state and federal laws. This is discussed in detail in Section 3 In addition to the specific security and privacy recommendations, there is an overall governance requirement to ensure that practitioners can access information regarding legal requirements.

Providing reimbursement for a healthcare intervention that is delivered in a way that not been shown to adhere to security and privacy requirements is high-risk.

Recommendations

As recommended in Section 3, to ensure compliance with all legal requirements, providers should undergo an annual security and privacy audit.

GAR3 *It is recommended that Divisions of General Practice, peak representative bodies and the professional colleges provide security and privacy advice to their members.*

(b) Safety and effectiveness

Issue

Video consultation is a different to the conventional in-person practice of medicine. In particular, patient examination has limitations and safety and effectiveness has not yet been shown for all circumstances. In healthcare, it is essential that a new intervention is shown to be safe (to avoid misadventure) and effective (to avoid resources being wasted). This is an established standard which should also apply to telehealth.

Providing reimbursement for a healthcare intervention that has not been shown to be safe and effective is high-risk.

Recommendations

In this report, video consultations are described as requiring diagnostic quality VC (for diagnostic or complex management work) or general quality VC, which can be used for other clinical work.

GAR4 *The choice of hardware and software for teleconsultation should be the responsibility of the individual health care provider subject to GAR5.*

GAR5 *Where a provider intends to use telehealth for diagnostic or complex management consultations, in circumstances where patients are unaccompanied by a health provider (~~unaccompanied patient~~), then products which have been demonstrated to be safe and effective should be used.*

2.5.4.2 2.5.4.3 Sustainable, cost-effective investment of public funds

Issue

The implementation of video consultation requires a significant investment of public funds. It is important that these funds are best used to develop a service which provides value for money and that is sustainable.

Recommendation

To measure progress towards a sustainable and cost-effective service, review of implementation, using suitable metrics will necessary. This is described further in Section 2.6.

GAR6 *Metrics for continuous review of the telehealth implementation should be developed.*

2.5.5 Estimated timeline to achieve readiness

Comment was made on the estimated timeline for infrastructure, stakeholders and vendors within each section. This section relates to governance readiness.

The implementation of Medicare item numbers will require a variety of processes and capabilities, which we have broadly categorised as immediate/short-term (0 to 3 years) and medium to long term (3 to 6 years).

In the immediate/short-term, where it is recommended that contemporary video systems are used, the following steps are required by government and its related health administrative capabilities.

- Definition of a fee structure, claim processes and rules;
- Consideration of approval agency and related processes for VC equipment and associated systems, including software;
- Consideration of approval agency and related processes for practitioners;
- Preparation of standards for privacy and security;
- Preparation of guidelines for video consultation practice;
- Development of audit processes and identification of responsible agency;
- Marketing, education and training strategy for clinicians and service administrators.

In the longer term the development of a fully featured health teleconsultation application which may be used anywhere that there is a PC, webcam and good broadband network access (described later in Section 3), would be beneficial. This application could be designed to meet the full requirements of clinical video consultation (as described in the functional and non-functional requirements in Section 3.3).

Since the government has a strong interest in encouraging the take-up of video consultation, there is a role for it in facilitating and promoting this activity.

2.6 Performance and monitoring

As has been seen with the development of other telehealth services, it is anticipated that take-up (and hence activity) in the short-term will be low. Activity will gradually increase with clinician and public awareness and as a range services are developed.

As a part of good governance, It will be important to monitor the performance of the initiative, and where necessary to provide adjustments to the implementation. This process will involve the identification of metrics and target thresholds for each indicator.

PMR1 Recommended key metrics that may be useful to this process include:

2.6.1.1.1 1. Clinician take-up per period

Analysed by:

- Overall
- By clinician
- By clinician subgroup, i.e. by GP and specialists
- By practice
- By specialty
- Geographic

2. Video consultation activity per period

Number of MBS telehealth claims per period

Analysed by:

- Overall
- By item number (in particular diagnostic/complex management vs. general)
- By clinician
- By clinician subgroup
- By practice
- By speciality
- Geographic

3. User satisfaction

Analysed by:

- Clinician subgroup
- Patients

4. Funds committed

Analysed by:

- Equipment and software costs
- MBS claims
- Clinician support
- Governance and administration
- Marketing

- Education and training

(e) An estimate of cost per consultation

In addition, routine budgetary review of initiative expenditure against projections will be important.

Performance targets

Threshold performance targets for each metric would need to be determined for the first and subsequent years of implementation.

PMR2 *It is recommended that a group, with appropriate membership, be established to estimate take-up and thus identify appropriate performance thresholds for each key performance metric.*

Independent evaluation

PMR3 *It is recommended that expert assistance is sought to provide input to the development of the evaluation of video consultation implementation.*

2.7 Risks

There are several risks associated with the introduction of Medicare supported VC, including:

- Low take-up of VC with failure to improve service access for patients and a perception of a failed policy initiative

The introduction of a funding allocation to support VC may be associated with an expectation in the general public, among professionals, and in political circles that the take-up will be high and immediate. However, this review has demonstrated that, even in ideal

circumstances, take-up is likely to grow slowly. A balance of positive messages to promote VC, without inflating expectation is required.

- High take-up of VC with associated expenditure blowout

There is a small risk that VC demand and take-up will accelerate beyond expectation. This would be a positive outcome from a patient perspective, but may be associated with expenditure beyond budget. If, as recommended, VC is funded on a time basis, in a similar manner to live consultation, then, provided the total availability of medical time is fixed, there will be a commensurate reduction in expenditure on conventional consultations, offsetting the cost of VC. However, if there is expenditure (such as incentive payments) associated with each episode that renders the VC more expensive than conventional consultation, there will be, to a degree, an increase in expenditure. It is expected that the additional cost of VC will be able to be reduced over time (as volume of activity increases, and per occasion of service cost declines), thereby reducing the risk of excessive expenditure.

- Medical error resulting from incorrect clinical assessment via VC

Clinicians constantly make judgements around their ability to make key clinical decisions in various contexts, and adjust their decision making accordingly. For example, they will moderate decisions according to the setting (e.g., on the telephone compared to at the bedside) or with whom they are communicating (e.g., a patient, junior doctor or senior specialist). To many doctors, VC will represent a new medium in which to make clinical judgements. Initially, they will need to be cautious in making critical decisions. Over time, it is expected that clinicians will become familiar with the advantages and weaknesses of the VC modality, and make appropriate judgements.

In many subspecialties, there is research available to guide clinicians around safety and reliability of conducting various types of consultation via VC. In others, the evidence is not yet available. It will be important, in the start up phase, to ensure that clinicians are advised of this evidence (relevant to their particular discipline), to guide them in the initial phases of implementation, when errors are most likely to occur.

2.8 Gap analysis

The establishment of a model for telehealth in Australia requires careful planning - and the implementation of a pragmatic strategy is essential. This report provides a comprehensive perspective on the current state of telehealth in Australia, guidelines and key

recommendations to ensure that the forthcoming funding for online consultations represents good value for investment.

This report clearly illustrates that there is considerable work to be done in order to reach the ultimate vision of a seamless multidisciplinary telehealth network shared between patients, primary care providers and specialists. Where a telehealth strategy has been demonstrated to be clinically safe and reliable, acceptable to patients and clinicians, with known equipment and systems, then relatively rapid rollout can be encouraged. Where there is less certainty, there is a case for further research, demonstration projects, evaluation and cautious or deferred implementation.

This gap analysis broadly reflects on the proposed telehealth implementation strategy and the strengths, weaknesses, opportunities and threats which apply.

Strengths

- The centralisation of specialist health services in major cities and the extensive distances separating smaller rural and remote towns easily justifies the suitability and need for telehealth;
- Many of the state health departments in Australia have some experience (of varying degree) with telehealth and this may be used as a starting point for the implementation strategy;
- The support shown by the Australian government in terms of promised funding for telehealth will help obviate one of the reported barriers associated with telehealth success. Importantly though, funding must be introduced alongside other strategies to facilitate take-up;
- The additional funding for telehealth will provide reimbursement for telehealth services which currently do not attract funding. This will act as an incentive for specialists and GPs to participate in telehealth work;
- The telehealth implementation will coincide well with the development of shared health records (EHRs, PCEHRs).

Weaknesses

- Given that there are very limited reports of telehealth experience in General Practice, throughout Australia and internationally; the telehealth implementation process will require more time than perhaps originally anticipated by some stakeholders;

- The telehealth recommendations will take time to develop properly. Short-cut approaches which do not incorporate a carefully planned approach may place the entire initiative at risk;
- Further consultation is required with GP's to ensure that appropriate telehealth services are introduced to enhance rather than inhibit their general practice role and capabilities;
- As per above, further consultation with specialists must also be continued to ensure that they share responsibility for the telehealth strategy;
- Current links (referral patterns) between GPs and specialists may not be matched by a telehealth component. A rapid, effective telehealth service requires both the GP and the specialist to develop a telehealth capability.

Opportunities

- The implementation of a successful model for telehealth in Australia which engages clinicians in general practice, specialists and patients has the potential to be useful for other countries;
- Assuming the success of telehealth in Australia; there are likely to be many benefits associated with equitable access to health care for all citizens regardless of geographical location;
- The implementation of telehealth services may act as a catalyst for redesigning various aspects of the health service – including referral mechanisms, access to clinical information, monitoring of patients in rural and remote locations and training of regional clinicians.

Threats

- The introduction of telehealth will require careful planning and engagement with key stakeholders; otherwise it is likely that the strategy will not be supported;
- If the strategic recommendations are ignored, there is a risk that investment in telehealth implementation will result in poor take-up and dissatisfaction amongst key stakeholders;
- If the necessary mechanisms are not put in place to encourage the use of telehealth (adequate reimbursement, technical support, coordination etc), the take-up of telehealth is likely to be very poor. Since the majority of funds are likely to be allocated to support clinician fees, and because a VC service will replace a conventional consultation, the additional cost of this telehealth initiative will relate to supplementary payments. These payments would be designed to (1) recognise the initial additional

cost of a VC, and (2) provide an incentive for health professionals to participate. It is conceivable that once the program is well established, with economies of scale achieved, and clinicians regularly involved, the level of these payments could be reduced. Therefore risk of major uncontrollable cost over-runs is low.

SECTION 3 ADVICE AND OPTIONS

This section presents technical advice and options relating to the future implementation of video consultations in Australia. Issues of security, privacy and authentication are discussed, technical options are described and in addition, advice on change management and budgetary costings are provided.

Since the lead time to the availability of MBS benefits is short, the development of a well designed solution, tuned to the needs of clinicians, of patients and suitable for mass deployment in the short-term is precluded.

Thus, in the immediate short-term, a pragmatic approach to implementation which makes use of readily available, off-the-shelf technical options is required, accepting that these options may not be the best fit to all of the requirements of telehealth. By implication, this will impact on the type of telehealth interactions that can be recommended as sufficiently safe, effective, secure and private to be billable items in the short-term. The decision to use, or not to use, telehealth together with the choice of particular hardware or software methods for consultation should rest with the clinician. In making their choices, clinicians should consider any legal (privacy and security), safety and clinical effectiveness implications.

In the medium-term, allowing for development time and experience with the short-term implementation, a solution for sustainable pervasive video consultation may be developed.

The implementation of telehealth video consultations should be seen as an iterative process that will require a number of years of gestation before maturity will be reached.

Aspects of both short-term and medium-term implementation of video consultation are discussed in this section. In some cases supporting services (e.g. backend systems for authentication, provider directories) are yet to be developed. Thus some of the recommendations should be considered as medium to long term aspirations which may be adopted as telehealth develops in Australia.

3.1 Security, privacy and authentication

3.1.1 Background

Privacy laws are intended to define principles to be followed and do not, therefore, prescribe any particular technological solutions for organisations to implement. Although this report

considers some of applicable technology to use, the main purpose is to provide guidance as to best privacy practice to ensure the technological solutions implemented ultimately meet the expectations of national privacy standards.

The privacy laws in Australia present a complex patchwork of legislative and contractual requirements that include: Commonwealth, State and Territory privacy legislation; Health specific privacy legislation; Privacy and confidentiality provisions within other laws; Codes of conduct; Health research guidelines; and the common law. These govern the collection and handling of personal information, including personal health information, in the public and private sectors. Information privacy legislation seeks to provide individuals with some control over the collection and handling of their personal information by balancing competing public interests between the individual's right to privacy and the benefits of the free flow of information.

3.1.2 Legislation

The Commonwealth Privacy Act 1988 applies to the Commonwealth public sector, and significant parts of the private sector:

1. Information Privacy Principles (IPPs) of which there are 11 that apply to Commonwealth and ACT government agencies;
2. National Privacy Principles (NPPs) which result from an amendment of the Privacy Act in 2001 to include 10 principles that apply to the private sector (but not all SMEs) and all Healthcare service providers.

The Commonwealth laws are currently under review. The NPPs are broadly applicable and closely reflect the proposed future changes for the Privacy Act.

State and territory legislation and administrative arrangements apply to the public sector bodies of most state and territories. NSW, Victoria and the Australian Capital Territory (ACT) have passed health specific privacy legislation that also applies to private sector organisations in those jurisdictions.

Recent Commonwealth legislation has been passed that relates to the use of Healthcare Identifiers. The Healthcare Identifiers Act 2010 together with the Healthcare Identifiers (Consequential Amendments) Act 2010 and the Healthcare Identifiers Regulations 2010, specify the use of unique identifiers for Individuals (known as healthcare recipients) for healthcare providers and for healthcare provider organisations. The use of such identifiers is

critical when using Telehealth technologies to ensure the right people and organisations are being connected. This report will therefore consider the role that the health identifiers will play in providing adequate security and privacy.

3.1.3 Privacy protection

When personal information is communicated outside of the security of the healthcare practice then it is necessary to manage any privacy risks. This is a situation which currently occurs using electronic and other means of communications. Australian privacy laws apply to personal information which can identify the individual concerned. The use of telehealth technologies can introduce new channels for information flows of personal health information. As with existing forms of communication, privacy breach will occur if personal information is disclosed using telehealth technologies to unauthorised third parties. Furthermore, in some circumstances, health information may be directly communicated via the same digital technology, for example, electronic prescriptions. Technology is readily available to manage the risk of unauthorised interception of personal information transmitted electronically through the use of data encryption.

The type and degree of protection depends on the cost to benefit ratio weighed against the risks of privacy breaches. A privacy risk has two factors: 1) the frequency of occurrence against 2) the consequence arising from a given disclosure. That is, probability of a breach occurring and the resultant damage from a given breach.

Use of Identifiers

When compared with traditional healthcare encounters, telehealth used across the Internet can add a dimension of remoteness and anonymity. While the ability to delivery health services remotely is a key benefit of telehealth, the potential anonymity of the users and/or the providers needs some careful consideration. In many other examples of electronic business, the only users permitted are those that have been identified by other means before an electronic account is registered. For example, the Australian Tax Office will supply registered small business users digital certificates by post before that can submit their Business Activity Statements electronically. In addition, banks will require traditional identification of their customers (point checks) before they set up electronic banking accounts.

For telehealth there can be more than one scenario that will give rise to different possible ways of identifying and accepting a user. The most secure and reliable method is when the

user and organisation is known in advance and has been identified by other traditional means. If the business case being adopted for telehealth allows for this it will permit the use of known proven identifiers. The recently passed Healthcare Identifiers Act 2010 permits unique identifiers to be assigned to individuals receiving healthcare, to each individual healthcare providers and each healthcare organisation. Medicare Australia is the organisation that assigns and manages these identifiers. The Act allows for use of the Individual Healthcare Identifier to correctly identify an individual for the purpose of electronic transfer of health information, including telehealth.

There are possible scenarios that allow for a telehealth user who has not been previously registered by alternative means, for example calling a triage nurse rather than visiting a hospital emergency department. Other situations are when a healthcare recipient is seeking medical advice from healthcare providers they have not previously contacted before. In this case the use of telehealth does not stop at the traditional borders of state or country and the provider may be providing the service internationally. Although the security can be established to accommodate this, the associated risks to the patient in these particular situations are very high. The majority of the population with acute healthcare needs and those with chronic illnesses who might most benefit from telehealth, are those that are most vulnerable to exploitation. It would therefore require a strong business case to support the use of telehealth in situations where the users or healthcare providers are not previously known to offset these risks.

Telehealth consultations at COH (A Case Study)

For ongoing care and consultation, videoconferencing has been adopted in the state of Queensland in Australia between clinicians and families. The clinicians and the care team members use facilities set up in the hospital to communicate with the patients and their family members using their home Personal Computer (PC). The technology employed makes use of readily available video streaming via Microsoft Messenger together with standard telephone calls for audio. Initially the separation of the audio and video channels was due to poor audio quality with the use of Microsoft Messenger together with the home speaker and microphone equipment on the family PC. This method of using two streams proved to provide greater privacy protection. That is, intercepting just the video stream would not readily reveal what was being said by the participants while intercepting just the audio stream would not readily reveal the identity of who was speaking. Furthermore, the security offered by the PSTN telephone network is much greater than the IP based Internet. That is, voice calls carried by the PSTN are less likely to be subject to interception.

A preliminary Privacy Impact Assessment identified a number of areas where supports for privacy are key in a telehealth service:

- data security – the information being exchanged can be highly sensitive and needs to be protected from unauthorised access;
- identifying the participants – an appropriate model needs to be in place for establishing that individuals are who they claim to be;
- appropriate collection and recording of information – an appropriate model needs to be in place to balance the need to collect information for identification and clinical purposes, and the need to avoid unnecessarily recording irrelevant information;
- consent – an appropriate model needs to be in place to explain and capture the scope of the consent needed; and
- notice – the participants need to know and understand their privacy rights and obligations.

Requirements to provide the levels of protection identified?

Technology alone cannot provide the protections necessary to ensure privacy compliance. A combination is required consisting of strong policy, good working practice together with the appropriate application of security technologies. For each of the above privacy issues the following are appropriate methods for providing best working practice solutions. These are detailed in the recommendations later in this section.

- To properly manage access to information an organisation needs to both establish and follow internal security and privacy policies about who has been authorised to access the telehealth system. To prevent any persons external to the organisation who have not been authorised access (e.g. as a registered patient) then suitable security technologies that require login and password access are required. This would be strengthened through the use of PKI certificates as detailed in later sub-sections below;
- An organisation's privacy policy and practices need to deter insiders from looking at information not relevant to their case load (this will include IT staff). Standard security technologies (as described in the previous bullet point) provide a degree of protection depending on how the organisation partitions its data base access. Specialised technologies can apply the necessary restrictions to include role based access controls but this is not universally adopted and can result in a high administrative management overhead in terms of ICT system adoption and maintenance. It should be noted that

such technologies only really minimise internal access by authorised people since unauthorised external adversaries (e.g. hackers) can bypass such technologies when they operate at the application layer. Technologies that provide the highest levels of security, e.g. mandatory access controls are not yet practical for health information systems and only really find application in military systems. Currently the most practical protection is through a combination of strong internal organisational policies and data partitioning to minimise the risk of inappropriate access to information and any identification of the individuals concerned.

- Appropriate collection and recording of information can be managed by a clear understanding of the purpose of the communication and facilitating access by an individual to their own information;
- Providing for appropriate notice and consent would flow from reviewing the privacy policy and notices which healthcare providers must develop under existing legislation, to reflect changes in business operations resulting from telehealth activities.

Practice Incentives Program (PIP) eHealth Incentive

The PIP eHealth Incentive program is a government initiative that commenced in 2008 to provide a number of incentives that aim to encourage general practitioners to improve the quality of care provided to patients. The PIP eHealth incentive aims to encourage practices to keep up to date with the latest developments in eHealth. This incentive has been developed in consultation with NEHTA and aligns with the directions set out in the Australian Government's National eHealth strategy.

To be eligible for the PIP eHealth incentive, practices must:

1. have a secure messaging capability, which is provided by an eligible supplier;
2. have (or have applied for) a location/site Public Key Infrastructure (PKI) certificate for the practice and each practice branch, and ensure that each medical practitioner from the practice has (or has applied for) an individual PKI certificate; and
3. provide practitioners from the practice with access to a range of key electronic clinical resources.

Each eligible practice must retrospectively apply for PIP incentive payments through Medicare and demonstrate that they have met the requirements of the eHealth Incentive for the entire preceding PIP payment quarter and are assessed as being eligible at a point in time.

PIP compliant practices would be providing enhanced privacy and security for any subsequent Telehealth services.

3.1.4 Assessing risk

Privacy Impact Assessment (PIA)

A PIA is a tool that can help determine if an organisation or agents are following their vision and values, can reduce the risk of not meeting their contractual and legal obligations and improve their position when, for example, tendering for new contracts. The Australian guidelines (www.privacy.gov.au) describe the PIA process as a story being told about a project that will identify privacy impacts and lead onto management recommendations:

–A PIA is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals – it tells the story’ of the project from a privacy perspective. The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts.”

The emphasis is on identifying when an organisation or government agency is collecting information that is unnecessary for the given project or whether the project will lack appropriate accountability or oversight processes. The aim is to identify, analyse and manage privacy impacts and seek out solutions that drive good privacy practice and underpin good public policy while still achieving the project’s goals.

The Australian guide states a number of key benefits that arise from undertaking a PIA. In brief these include: avoiding costly or embarrassing privacy mistakes; compliance with privacy laws; reflecting community values; avoiding function creep relating to privacy; future proof against known upcoming privacy law changes; ensuring stakeholders and the community are better informed; demonstrating that protecting personal information is important to the organisation concerned and this has been critically evaluated.

A full PIA is an involved process, and in a similar way with safety case analysis, can only be achieved when all the parameters are known and the implementation has been specified. When undertaking a full Privacy Impact Assessment (PIA) it is necessary to consider all the legislation that might apply. A Preliminary PIA’ can consider the viable options and give an indication of the key issues that may have an impact on privacy to help determine if the project is feasible. That is, an indication whether the risks be sufficiently minimised and that

any resultant risk be outweighed by the benefits to the community and the health and wellness of the individuals concerned.

The approach taken in this report was to provide three typical scenarios of telehealth consultations. A preliminary analysis is provided to ascertain if the services and technology could be compliant. The three scenarios selected include:

1. A link between a GP and a healthcare provider specialist with the patient and family members present at the GP's practice;
2. A patient is at home which is equipped with some basic telehealth monitoring equipment. He is linked to his healthcare provider who performs a remote diagnostic of his ongoing healthcare needs;
3. An individual wishes to contact a medical helpline using teleconferencing and is linked from their home to a triage nurse to make an assessment.

Scenario 1

General Practitioner Dr Lim is consulting with cardiologist Mr. Patel. The medical case here is Mrs. McCarthy, a long time patient with the practice. Mrs. McCarthy has brought her daughter with her for the telehealth consultation. The patient, her daughter and the GP are in the GP's practice and Mr. Patel is in his hospital room.

Dr Lim has sent Mrs. McCarthy's test results and X-rays to Mr. Patel along with her medical records via a health information system. Mr. Patel reads through the medical records and talks with Mrs. McCarthy and gives his treatment. The resulting notes are sent back to Dr Lim via the health information system. (Note: this scenario could occur with all participants being in separate locations when the National Broadband (NBN) is fully utilised.)

Telehealth technologies used in this scenario: Video conference, Electronic data access, storage and transfer, User Interface, Network connectivity wired and wireless access, devices and business models, business processes, Informatics.

A preliminary Privacy Impact Assessment for this scenario will involve a Threshold Assessment, Mapping the Information Flows and a Privacy Analysis.

Threshold Assessment for Scenario 1

This scenario involves the collection, use and disclosure of personal information. The personal information here is that of the patient Mrs McCarthy. This personal information includes personal identifiable information, including, name, address, date of birth, and medical and health information.

The key privacy elements here include:

1. The purpose for which the information will be collected, used and disclosed: Mrs. McCarthy's medical information will be used by the GP and the cardiologist in her treatment for her medical condition;
2. Any authority under which it is collected: Mrs. McCarthy has given her authority for her information to be collected. The GP and cardiologist have the authority to see her medical information;
3. The nature and sensitivity of the personal information: Mrs. McCarthy's medical information is private and personal and is treated accordingly.

The threshold assessment indicates that as private and personal information is being collected and used, a Privacy Analysis of this scenario is necessary.

Preliminary Privacy Analysis for Scenario 1

A Privacy Analysis investigates the following:

- how information flows affect individuals' choices in the way personal information about them is handled;
- the degree of intrusiveness into individuals' lives;
- compliance with privacy law, and;
- how the project fits into community expectations.

Mrs. McCarthy has to give up control of her information in this scenario. Her medical information is used by her GP and various health professionals to aid her medical treatment. However, she could choose to have her personal medical information access restricted. This scenario where the patient, GP and cardiologist interact via telehealth could change the way the patient interacts with the medical services. Identity checks to ensure that the patient is actually the patient in question have to be made.

There are costs involved in this scenario; in terms of the technologies used, the security to ensure privacy and authentication of patient and the health professionals' identities.

If the patient or the health professionals do not have identity documents, there would be an impact resulting in wrong diagnosis, treatments and non-compliance with the laws.

In this scenario, patients and health professionals are aware of the need to be compliant with the privacy laws.

The health services have adequate complaint-handling mechanisms. The health service is very aware of the importance of ensuring that personal information is kept private and secure. There are protocols in place to deal with any privacy breach. The health service has audit and oversight mechanisms which include emergency procedures to deal with system failure if any. There could be function creep with this scenario. The medical and health information of the patient could be used for research. However, the information would need to be de-identified before it would be used and the consent of the patient would have to be sought before this could happen. The medical and health information of the patient could be deemed valuable to unauthorised users. The privacy and security framework ensures that such breaches cannot happen.

This scenario is consistent with the health service's values about privacy. Privacy is always factored into any analysis of cost-benefits and investment return.

Scenario 2

Diabetic patient, Mr Donald, is consulting his General Practitioner Dr Martins. Mr Donald is at home as he finds it very difficult to travel to the clinic. He is disabled due to complications from his diabetes. Mr. Donald takes his blood pressure and the results are transmitted via the health information system to his GP. Dr Martins has the patient's medical records on his computer screen while he does his consultation. Mr Donald's family are in the same room while his consultation is taking place. Dr Martins wants to change Mr. Donald's prescription due to the changes in his blood pressure and sends the new prescription to Mr. Donald who can print it out and get a family member to get his new medication. Dr Martins explains the new medication and updates Mr. Donald's medical notes on the health information system.

Telehealth technologies used in this scenario: Video conference, Electronic data access, storage and transfer, User Interface, Network connectivity wired and wireless access, devices and business models, business processes, Informatics.

A preliminary Privacy Impact Assessment for this scenario will involve a Threshold Assessment, Mapping the Information Flows and a Privacy Impact Analysis.

Threshold Assessment for Scenario 2

This scenario involves the collection, use and disclosure of personal information. The personal information here is that of the patient Mr. Donald. This personal information includes personal identifiable information, including, name, address, date of birth, and medical and health information.

The key privacy elements here include:

1. The purpose for which the information will be collected, used and disclosed: Mr. Donald's medical information will be used by the GP his treatment for his medical condition;
2. Any authority under which it is collected: Mr. Donald has given his authority for his information to be collected. The GP has the authority to see his medical information;
3. The nature and sensitivity of the personal information: Mr. Donald's medical information is private and personal and is treated accordingly.

The threshold assessment indicates that as private and personal information is being collected and used, a Privacy Analysis of this scenario is necessary.

Preliminary Privacy Analysis for Scenario 2

- how information flows affect individuals' choices in the way personal information about them is handled;
- the degree of intrusiveness into individuals' lives;
- compliance with privacy law, and;
- how the project fits into community expectations.

Mr. Donald has to give up control of his information in this scenario. His medical information is used by his GP and various health professionals to aid his medical treatment. However, he could choose to have his personal medical information access restricted. Identity checks to ensure that the patient is actually the patient in question have to be made.

There are costs involved in this scenario; in terms of the technologies used, the security to ensure privacy and authentication of patient and the health professionals' identities.

If the patient or the health professionals do not have identity documents, there would be an impact resulting in wrong diagnosis, treatments and non-compliance with the laws.

In this scenario, patients and health professionals are aware of the need to be compliant with the privacy laws.

The health services have adequate complaint-handling mechanisms. The health service is very aware of the importance of ensuring that personal information is kept private and secure. There are protocols in place to deal with any privacy breach. The health service has audit and oversight mechanisms which include emergency procedures to deal with system failure if any. There could be function creep with this scenario. The medical and health information of the patient could be used for research. However, the information would need to be de-identified before it would be used and the consent of the patient would have to be sought before this could happen. The medical and health information of the patient could be deemed valuable to unauthorised users. The privacy and security framework ensures that such breaches cannot happen.

This scenario is consistent with the health service's values about privacy. Privacy is always factored into any analysis of cost-benefits and investment return.

Scenario 3

Nurse Paterson is on duty at the after hours helpline. A patient, Miss Younge, consults her via video conference from her home for advice regarding a recurring medical condition. The nurse has the patient's medical records on her computer screen whilst she talks to the patient and does an assessment. She makes a recommendation for the patient to come to the hospital as her condition needs medical intervention.

Telehealth technologies used in this scenario: Video conference, Electronic data access, storage and transfer, User Interface, Network connectivity wired and wireless access, devices and business models, business processes, Informatics.

A preliminary Privacy Impact Assessment for this scenario will involve a Threshold Assessment, Mapping the Information Flows and a Privacy Analysis

Threshold Assessment for Scenario 3

This scenario involves the collection, use and disclosure of personal information. The personal information here is that of the patient Miss Younge. This personal information includes personal identifiable information, including, name, address, date of birth, and medical and health information.

The key privacy elements here include:

1. The purpose for which the information will be collected, used and disclosed: Miss Younge's medical information will be used by the Nurse and the relevant medical professionals in her treatment for her medical condition;
2. Any authority under which it is collected: Miss Younge has given her authority for her information to be collected. The Nurse and the medical professionals have the authority to see her medical information;
3. The nature and sensitivity of the personal information: Miss Younge's medical information is private and personal and is treated accordingly.

The threshold assessment indicates that as private and personal information is being collected and used, a Privacy Analysis of this scenario is necessary.

Preliminary Privacy Analysis for Scenario 3

- how information flows affect individuals' choices in the way personal information about them is handled;
- the degree of intrusiveness into individuals' lives;
- compliance with privacy law, and;
- how the project fits into community expectations.

Miss Younge has to give up control of her information in this scenario. Her medical information is used by the nurse and various health professionals to aid her medical treatment. However, she could choose to have her personal medical information access restricted. This scenario where the patient, nurse and any other health professional interact via telehealth could change the way the patient interacts with the medical services. Identity checks to ensure that the patient is actually the patient in question have to be made.

There are costs involved in this scenario; in terms of the technologies used, the security to ensure privacy and authentication of patient and the health professionals' identities.

If the patient or the health professionals do not have identity documents, there would be an impact resulting in wrong diagnosis, treatments and non-compliance with the laws.

In this scenario, patients and health professionals are aware of the need to be compliant with the privacy laws.

The health services have adequate complaint-handling mechanisms. The health service is very aware of the importance of ensuring that personal information is kept private and secure. There are protocols in place to deal with any privacy breach. The health service has audit and oversight mechanisms which include emergency procedures to deal with system failure if any. There could be function creep with this scenario. The medical and health information of the patient could be used for research. However, the information would need to be de-identified before it would be used and the consent of the patient would have to be sought before this could happen. The medical and health information of the patient could be deemed valuable to unauthorised users. The privacy and security framework ensures that such breaches cannot happen.

This scenario is consistent with the health service's values about privacy. Privacy is always factored into any analysis of cost-benefits and investment return.

Secure Messaging

In order to meet the first requirement of the PIP eHealth incentive program, healthcare practices must have a secure messaging capability that will allow patient health information to be securely exchanged where possible.

The secure messaging capability may be provided as a direct extension to the practice management system, or indirectly via a separate messaging system.

What are 'Reasonable Steps' for Security?

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure (NPP 4.1 Data security).

- Encryption is considered a reasonable step for securing information (provided proven encryption methods are employed together with keys that are long enough, in terms of bit length, to make it highly unlikely for anyone to decrypt that message);

- Existing guidelines advise that when sensitive (health) information is involved, encryption should be used when messages, particularly emails, are transmitted across public networks. For example, the Royal Australian College of General Practice, RACGP Standards for general practices - Criterion 4.2.3 - Transfer of patient health information, states: “Some practices have begun to use encryption to transfer patient health information and it is anticipated more will do so in future. Practices should not transfer patient information via email unless it is encrypted.” Furthermore, the Office of the Privacy Commissioner’s Guidelines states that: “Wherever practical, personal information should not be transmitted across public networks, by fax or e-mail etc, in plain text. Particularly when handling sensitive personal information, Agencies should consider using encryption to protect it during transmission”;
- A further requirement in privacy legislation applies to an organisation’s Use and Disclosure of sensitive health information (NPP2 Use and Disclosure). That is: “An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless both: (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose”;
- Private networks that have good physical and electronic security from outside interference would not necessarily have to encrypt all their messages. However, according to the OPC Guidelines for NPP2, organisations still have an obligation not to disclose this information unless it relates to the ‘primary purpose’ for which it was collected, i.e. to diagnose and treat a particular condition or set of symptoms, or for a directly related purpose if the individual would ‘reasonably expect’ this to occur. It is unlikely that an individual would ‘reasonably expect’ information to be disclosed to third parties during a messaging process. To the contrary, it is likely that there would be an expectation that electronic transmission of health information would be secure. Note, there are some exceptions to this requirement for legal (e.g. requested by a court of law) and safety purposes but they would not apply here.

Encryption of personal information is a reasonable security step to prevent disclosure and ensure individual’s expectations around the security of their health information can be met. Although privacy legislation does not mandate encryption, there is an obligation on organisations to take ‘reasonable steps’ to secure personal information and prevent disclosure of the information beyond what is permitted by the legislation. Given that health

information is considered ‘sensitive’ information, encryption provides the most certain way of ensuring these legal obligations can be met. Any organisation that chooses not to take the reasonable step of encrypting messages would be expected to demonstrate equivalent or better security. That is, they may need to demonstrate for a given implementation that it is impractical to encrypt any messages that may contain identifiers and sensitive information and that other equivalent or better measures have been put in place to protect it.

The claim that encryption from source to destination is not current practice does not address the issue of what is a reasonable step. It only states what happens now regardless of what might be considered reasonable. Any claim that it is an ‘unnecessarily erroneous obligation’ would have to be well qualified.

Hence, for secure messaging, it is recommended that health related information should be encrypted from source organisation to destination organisation unless equivalent or better security can be demonstrated.

NEHTA have worked with the medical software industry to develop specifications and standards for secure messaging for healthcare providers. The documents which describe the Secure Messaging Delivery, Web Services Profile and the XML Secure Payload profile specifications are now Technical Specifications published by Standards Australia. The Endpoint Location Service specification is now a Technical Report also published by Standards Australia.

These documents can be downloaded from the “SAI Global website” at <http://infostore.saiglobal.com/store/portal.aspx?portal=Informatics>.

The Standards Australia document references are;

ATS 5820:2010 E-health Web Services Profiles

ATS 5821:2010 E-health XML Secure Payload Profiles

ATS 5822:2010 E-health Secure Message Delivery

TR 5823:2010 Endpoint Location Service

NEHTA is supporting these specifications by providing a Compliance and Conformance Assessment Scheme which allows implementers of the specification to verify their software. Details of this Scheme are available at <http://www.nehta.gov.au/connecting-australia/cca>

Current approach to encryption with regard to secure messaging

Based on previous privacy advice obtained in relation to developing specifications for sending clinically sensitive information which identified patients, NEHTA's Secure Message team has adopted the following approaches:

- Information in messages sent from the sender organisation to the receiver organisation must be encrypted;
- Information in messages should not be able to be decrypted by any third parties other than the sender organisation and the receiver organisation;
- It is not the responsibility of the sender to ensure information is secured beyond the boundary of the recipient organisation (i.e. it is not necessary to secure information at the individual to individual/clinician to clinician level);
- Although, NEHTA Secure Messaging specifications do not prescribe messaging standards at the individual to individual level, the technical capability is available/has been developed for outlier circumstances.

Ultimately, NEHTA Secure Messaging specifications aim to enable messages to be sent securely from a sender organisation to a receiver organisation without the requirement for both organisations to use the same messaging vendor. Consequently, these circumstances would not give rise to the contractual relationships between organisations and third party vendors. Rather, multiple intermediaries could potentially be able to view the information if it is not encrypted.

The key implications from a Privacy perspective are:

- the need to ensure reasonable steps' have been taken with regard to information security;
- that information collected by healthcare providers is regarded as sensitive' for which higher privacy standards apply; and
- an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection or directly related secondary purposes that the patient would reasonably expect to happen.

In response:

- encryption is a reasonable step for securing information from source to destination;

- it is likely that there would be an expectation that electronic transmission of health information would be secure from third parties; and
- it is unlikely that an individual would reasonably expect information to be disclosed to third parties during a messaging process.

3.1.5 Security, privacy and authentication framework for telehealth

This section presents technological solutions for the implementation of security mechanism and privacy-enhancing technologies and the application of these technologies to the practice of telehealth. The proposed solutions aim to leverage well established industry security standards i.e. not re-invent the wheel. The scope of the framework ensures patient information is: secured during transmission (across the Internet) and secured whilst stored. Further, the framework presents appropriate authentication and access control mechanism to secure telehealth sessions and data. The framework is applicable to both telehealth VC sessions and ancillary telehealth data exchange requirements e.g. transmission and access of electronic health records by say, web services.

Development of the National E-Health Security and Access Framework (NeSAF) is being led and facilitated by NEHTA as a national framework, addressing the needs of Commonwealth, state, territory and local healthcare organisations, with the prime objective of developing a common approach to information security and access controls that cultivates a “network of trust” between all participants in a patient’s healthcare journey.

The NeSAF will increase certainty that health information is created and accessed in a secure and trustworthy manner. It does not replace existing privacy principles, laws and governance for the handling of information, but provides guidance to people responsible for designing and implementing e-health systems on the way security and access controls should be established in their systems.

Many of the recommendations made in this section are taken from existing technical security frameworks. In particular, the *Australian Government Information Security Manual*, November 2010 in which the Defence Signal Directorate (DSD) list approved cryptographic protocols (including version information). Other such frameworks used to develop this telehealth framework include: the Queensland Government *Network Transmission Security Assurance Framework V1.0.1* January 2010 and the Australian Government *Protective Security Policy Framework V1.1* September 2010.

3.1.5.1 Ensuring data is secured during transmission

Transmission security can be achieved by a number of ways: encrypting data at the source and sending the encrypted payload e.g. Secure Socket Layer (SSL) or encrypted email or creating an encrypted path and sending data over this path (e.g. Virtual Private Network).

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a protocol where the sender encrypts data for Internet transmission and receiver decrypts data to human-readable format. The purpose of PKI cryptography is to prevent eavesdropping of data during transmission. There are additional benefits of PKI including: assuring the identity of the sender (non-repudiation) and ensuring the data has not been modified during transmission (digital signatures).

PKI uses two keys — one key for encryption and a second key for decryption. The two keys are mathematically related but not the same. The PKI process is also known as asymmetrical key cryptography (cryptographic processes that use the same key for both encryption and decryption are known symmetrical key cryptography). The encryption / decryption keys are also known as public key / private key pair. As the name implies the owner will keep one key private (the decryption key). The public key is distributed and used to encrypt data (once encrypted only the private key can decrypt the data).

So as not to compromise PKI the private key needs to be protected from theft or misuse. Technically this can be achieved by password or passphrase protection of the private key. However, there is an inconvenience overhead associated with this method and physical safeguards are often used in lieu of password protection — for example, storing the private on the server which has been afforded physical security, access control and network level security e.g. firewall.

The keys are issued by a trusted third party organisation called a Certification Authority (CA). There are many commercial CAs. Government agencies and other statutory bodies e.g. a university may also act as CAs. In addition to issuing a digital certificate and validating the key pair a CA also publish a certificate revocation list (CRL). A CRL is a published list of previously issued but now invalid certificates. A lost or compromised private key is one reason for invalidation of the certificate. Checking for the validity of certificate prior to exchange of information is an added safeguard of PKI.

The identity of the issuing CA is information included in a PKI certificate. Applications e.g. email clients or web browsers that encrypt data with a public key will need access to the root certificate of issuing CA. The root certificate essentially means you trust certificates issued by that particular CA. The process is known as “chain of trust”.

The key strength of PKI is measured in bits e.g. 1024 bit. This number refers to the size of the cryptographic algorithm. As the key strength increases the computational power to “crack” the encryption using a brute strength attack decreases. It is important to use a key strength where that makes a brute strength attack unfeasible. As computational power increases over time the key strength will need to increase. RSA Security (inventors of the RSA algorithm used in PKI) advise a 2048-bit keys will be able to resist brute force attack until 2030. (It is interesting to note symmetrical key strength recommendations are between 112-bit and 256-bit depending on the algorithm. Substantially lower than asymmetrical cryptography recommendations. This is due the nature of the algorithm and the number of possible combinations that can be achieved with each method.

Secure Socket Layer and Transport Layer Security

Client-server web services — that is, web- browser to web-server — communication can be encrypted using Transport Layer Security (TLS) or its predecessor Secure Socket Layer (SSL). Both TLS and SSL have been through a number of iterations. Version 1.0 of SSL was never released and version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS with the latest version being TLS 1.2 which was released in August 2008.⁶⁵

SSL/TLS uses PKI to exchange a random number. The random number is used to generate a symmetrical key which is used by the server and client to encrypt communication. The use of symmetrical key cryptography is less CPU intensive, hence faster than asymmetrical key cryptography which accounts for its use.

SSL/TLS is combined with Hypertext Transfer Protocol (HTTP) to create Secure Hypertext Transfer Protocol (HTTPS). Default support of HTTPS is built into most web browsers and is routinely used for secure communication e.g. financial transactions that occur on the World Wide Web (WWW). Telehealth services that use web-services may include video conferencing via secure web portal or static data exchange e.g. electronic health records. These services need to encrypt with HTTPS which uses the latest version of TLS.

Secure Email

Multipurpose Internet Mail Extensions (MIME) are the protocols developed by the Internet Engineering Taskforce (IETF) for the structure and encoding of Internet mail or email. The MIME standards have been extended to include cryptographic services with the Secure Multipart Internet Mail Extensions (S/MIME). S/MIME is a further application of PKI. Communicating parties exchange their public key. The public key is used by the sender to encrypt the email which can only be decrypted by the recipient i.e. the holder of the private key. If patient information is exchanged by email as part of the telehealth consultation the email need to be encrypted with S/MIME. As with most standards there are a number of versions of S/MIME. The Defence Signal Directorate recommends: *Agencies should not allow versions of S/MIME earlier than 3.0 to be used.* This is due to S/MIME 2.0 required the use of weaker cryptography (40-bit keys) than is approved for use by the government. S/MIME Version 3.0 was the first version to become an IEFT standard.

Hardware video conference security

IP-based hardware video conference units (e.g. Tandberg) that have the same security vulnerabilities as other information transmitted across in an unencrypted format across the Internet. This vulnerability is addressed by International Telecommunications Union (ITU) H.235 standard. H.235 provides the means for a H.323 video device to establish encrypted data exchange between endpoints. It works in a similar manner to SSL/TLS in which a PKI is used to establish and exchange a session key which is used for symmetrical data encryption of the VC session. Many hardware units by default have support of H.235.

Hardware based video conferencing units used for telehealth consultations should be chosen on the ability to support standards-based encryption algorithms. The ability to encrypt communication in point-to-point or multi-point sessions is a requirement.

Virtual Private Networks

The previous sections have described technological solutions for the encryption of data exchange between devices on a public network that involve the encryption of the payload transferred between communicating devices. Instead of encrypting payload, the connection between devices can be secured allowing data to be transferred securely. This technology is known as Virtual Private Network (VPN).

3.1.5.2 Authentication and access control

Authentication is a means safeguarding access to telehealth systems and associated data. The most common means of authentication is with a username and password. Other means of safeguarding access include: physical devices e.g. smartcard or hardware tokens, biometric e.g. fingerprint or retinal scanners. Biometric devices suffer from reliability issues.

One-stage authentication refers to the use of one of the above safeguards, say a password, to control access. Higher levels of security can be achieved by using a combination of two of the above safeguards e.g. password plus a RSA token code. Many Internet banking sites optionally offer customers two-stage authentication processes if the customer chooses to increase the security level for access to their banking details. Similarly, telehealth services should offer clients the ability to use a two-stage authentication process. Hence, telehealth application must support this.

Password strength refers to ability of the password to resist brute strength attacks or guessing or deducing the password. The strength of the password is dependent on a number of factors: its length, the characters (alphabetic, numeric, punctuation) that make up the password, the deductive ability (e.g. their dog's name) and whether the password would be contained in a dictionary. A password which is a dictionary word is considered a weak password, as would be a three-character password. Whereas, a password of greater than six characters that contains alphabetic, number and punctuation characters would be considered a stronger password. Telehealth applications should enforce a minimum password strength when creating user accounts.

Passwords can be intercepted if sent in plain text format from client to remote server. This vulnerability can be mitigated by secure network authentication protocols such as Kerberos. Kerberos is an encrypted password protocol that requires a third-party server containing a user database. The function of the Kerberos server is to issues a session encryption key to both the server and client and a "ticket" containing client permissions. A national infrastructure service providing network authentication services would be beneficial for telehealth applications. Clinicians could use the National Authentication Service for Health (NASH) infrastructure when available. The NASH will deliver digital certificates on tokens such as smartcards, for authenticating healthcare providers involved in eHealth communications, such as e-referrals, e-prescriptions, as well as when accessing an individual's PCEHR. The NASH will enable a range of certificates to be stored on a single smartcard allowing providers to use this single device to securely access a range of local

and national eHealth systems they are authorised to use and will be built to meet the standards and requirements of the National e-Authentication Framework, the Gatekeeper PKI Framework and the National Smartcard Framework managed by the Australian Government Information Management Office (AGIMO).

Authentication also identifies a user of a telehealth application. The user's access to patient information via telehealth systems should be recorded in an audit log and this audit log be stored. It is recommended future telehealth applications have the ability to create an audit trail; and administrative guidelines be developed that stipulate the retention period and technical storage guidelines.

3.1.5.3 Storage security

The scope of the storage security section is twofold. Firstly, some telehealth data will be stored routinely e.g. electronic health records and authentication databases. Secondly some data e.g. recorded VC teleconsultations would only be stored when there is a clinical imperative to do so. The clinical need would be ascertained by the consulting clinician and appropriate storage security is the responsibility of the telehealth service (including discrete practices, practitioners and service providers).

The storage of any health data, including telehealth data, is a privacy and security vulnerability. Hence, safeguards need to be applied. Three specific safeguards need to be implemented by telehealth agencies and personnel working with telehealth data namely: the physical security of ICT equipment used to conduct telehealth; the lifecycle management of media on which telehealth data is stored; and secure transportation of telehealth if it is stored outside of physically secure environment.

If storage is required, telehealth data (ancillary data and clinically determined recorded videoconference session) should be stored in a physically secure environment. The management (sanitisation, destruction and disposal) of media on which telehealth data is performed accordingly to legislative obligations and sound technological practice. Secure storage is the responsibility of the telehealth service (including discrete practices, practitioners and service providers).

It is inevitable that situations will arise when telehealth data will be stored outside of data centre e.g. on a clinicians laptop. If there is clinical imperative for this, the data stored on a portable device should only be stored for the period of clinical imperative and should ideally

be encrypted using commercial data encryption software to prevent unauthorised access that could arise if say, a laptop or memory stick is stolen or lost.

3.1.6 Recommendations

Recommendations which relate specifically to security and privacy are provided as follows:

- SPR1** *To ensure public trust in a teleconsultation, privacy protection and security mechanisms must be integral to any implementation.*
- SPR2** *Telehealth services should be compliant with all relevant state and federal laws.*
- SPR3** *Telehealth service providers should periodically review and update their privacy policies to ensure that they adequately address the management of information gathered during telehealth consultations.*
- SPR3A** *Telehealth service providers should periodically review and update their privacy notices to ensure that they adequately address the management of information gathered during telehealth consultations.*
- SPR4** *Telehealth service providers should periodically review and update their practices and procedures for managing personal information, including data security measures.*
- SPR5** *Protocols used to secure telehealth consultations should be non-proprietary, standards-based to foster interoperability, inspectability and trust.*
- SPR6** *Telehealth services, whether discrete practitioners or service providers should use a valid Public Key Infrastructure (PKI) certificate.*
- SPR7** *The PKI certificate should be signed by a Certification Authority who maintains a Certificate Revocation List (CRL).*
- SPR8** *The PKI certificate should use a minimum key strength e.g. 2048-bit encryption. As computing power increases then the level of encryption may need to be increased.*

- SPR9** *PKI certificates should be stored in a physically or technically secured environment.*
- SPR10** *All teleconsultation data (including ancillary data) must be secured for transmission across a data network either by use of encryption or VPN technology.*
- SPR11** *All web services used in teleconsultations — including web-based video conferencing, patient records, messaging systems must be secured by a minimum Transport Layer Security Version 1.2.*
- SPR12** *All emails containing patient data must be secured. This should be at a minimum by S/MIME Version 3.0 or later and/or the latest technical specifications published by Standards Australia for E-Health Secure Message Delivery.*
- SPR13** *Hardware based videoconferencing units must support H.235 allowing encrypted communication between end points in both point-to-point and multi-point videoconferencing sessions.*
- SPR14** *The National Authentication Service (NASH) or a similar service could be considered for telehealth service providers and telehealth applications when operational.*
- SPR15** *In the future infrastructure could be developed and implemented to provide the following solutions for telehealth service providers and telehealth application vendors:*
- *Credential user base of telehealth clinicians;*
 - *Encrypted authentication services for patients who will participate in clinician-to-patient telehealth services; and*
 - *Access control to limit teleconsultations to eligible clients and credentialed clinicians via links to health identifiers.*
- SPR16** *All telehealth applications must enforce strong passwords.*
- SPR17** *All telehealth applications support two-stage authentication.*

SPR18 *All telehealth applications record an audit trail of user's access to patient information.*

SPR19 *Policy guidelines for the retention and storage of telehealth records could be developed to assist those telehealth service providers which are not subject to specific legislative requirements for the retention and maintenance of health records.*

SPR20 *If storage is required, telehealth data (ancillary data and clinically determined recorded videoconference session) should be stored in a physically secure environment. The management (sanitisation, destruction and disposal) of media on which telehealth data is stored should be performed according to legislative obligations and sound technological practice. Secure storage is the responsibility of the telehealth service (including discrete practices, practitioners and service providers).*

SPR21 *If telehealth data is stored on a portable device it should be encrypted using a commercial data encryption application.*

3.2 Interoperability and integration

3.2.1 Interoperability

Interoperability relates to the requirement for devices to communicate in a heterogeneous environment. The foundations of interoperability are standards, including those developed by national and international standards organisations and de facto industry standards.

It is important to note that while standards *facilitate* interoperability between equipment of different manufacturers, in practice they do not *guarantee* interoperability. Reasons for failure to interoperate include errors of implementation and manufacturers' use of proprietary, or pre-standard extensions to implement new features. In a competitive environment, where there is a drive to get new features to market quickly, this practice is common. Further, it is not uncommon for manufactures to forego interoperability and create proprietary platforms in an attempt to exclude competitors.

IRR1 *To promote interoperability, where standards-based products are proposed, features that are provided by proprietary or pre-standard extensions should be avoided.*

In many established telehealth networks, the operators have opted for a single manufacturer approach to ensure interoperability. This may work well within the operator's network however in the authors' experience, where cross-jurisdictional sessions are required (and different manufacturer's equipment is in the path), problems of interoperability are common. Thus, while standards are extremely important, an expectation that they will ensure interoperability is misplaced.

Historically, most telehealth networks have been built using hardware video conferencing units. These systems are usually designed to implement international standards for communication, typically based around the H.323⁶⁶ family of protocols. In recent times, systems supporting Session Initiation Protocol⁶⁷ have been developed. Devices may implement SIP in place of, or in addition to the ITU-T standards. Endpoints that implement only one of H.323 or SIP are not interoperable without specific infrastructure to bridge between them.

Today, for communication with established telehealth endpoints, such as those installed within state health departments, compliance with the established communication standards are essential. New implementations, whether standards-based or not, must have a mechanism to interoperate with existing infrastructure.

A solution that may be considered or developed in the future is to have a national Video Conferencing cloud service which would connect jurisdictions and provide connectivity from anywhere to anywhere and provide interoperability between all products e.g. Skype, Attend Anywhere, Tandberg solutions, Polycom solutions etc.

Recognising that (i) standards are not an absolute assurance of interoperability; (ii) that teleconsultation must be provided in a heterogeneous environment and that (iii) most established Australian video conferencing implementations are H.323 based:

IRR2 *In the short-term, to communicate with endpoints on established networks, any new video consultation implementation should:*

- *Be either standards-based, or if proprietary, provide a mechanism to allow audio and video sessions between the proprietary and standards-compliant endpoints;*
- *Support a minimal subset of the following standards: H.225; H.245; H.261 QCIF, H.263, Q.931; RTP; G.711; G.722; G.728; G.723; G.729; TCP/IP;*
- *Manufacturers should demonstrate interoperability using the stated minimum subset in a heterogeneous environment.*

Such an approach will minimise, but perhaps not eliminate, issues of interoperability.

The communications landscape today is quite different to the environment that existed when international standards for video conferencing were developed. It is also changing rapidly. Broadband Internet is now pervasive in the developed world and PC and web-based communication applications are now commonplace. While some applications implement industry, or defacto standards, many popular communications applications (such as Skype and MS Messenger) use proprietary and unpublished communication protocols.

In the medium to long-term, for some telehealth communications, the relevance of some of the established international VC standards for some types of communication is likely to decrease as a result of technology convergence. Standards will remain important and while video communication is likely to have increasing relevance, particularly given the ubiquity of the PC and the Internet, communication is unlikely to continue only in the way described by legacy VC standards.

It is likely that both hardware-based VC and some kind of video consultation software products will be important to the medium and long term future provision of telehealth in Australia. Hence, there will be an ongoing interoperability requirement.

Since the communications environment is in a period of rapid change, it is not possible at this stage, to nominate a minimum standard for interoperability which would be applicable to the medium and long term.

For the medium and long term:

- High speed pervasive networking (eg. as promised by the NBN) will facilitate convergence;
- Convergence is, and will continue to, broaden the communication options which may be delivered by a PC and mobile consumer devices;
- Mandating standards-based VC endpoints for a patient/GP may not be feasible or necessary in a converged world (though the legacy standards may continue to have a place within the network, but not necessarily at all endpoints);
- Interoperability challenges of the future will likely be different to those of the past and new standards for future interoperability may need to be determined.

IRR3 *While it is not possible to foresee detailed interoperability issues of the medium and long-term future, new products, however delivered, should be tested for interoperability using the contemporary technical standards of the day.*

3.2.2 Integration

This section discusses the needs and benefits of integration between a video consultation system and other relevant systems. As with previous sections, a short-term and medium to long term view is presented.

Potential areas for integration of video consultation with other systems include:

- Practice management systems
 - Appointment scheduling
 - Billing
- Desktop clinical systems
 - Patient records
 - Decision support tools
 - Test results
 - Referrals

➤ Prescriptions

- Scheduling and co-ordination systems for inter-practice bookings

In considering integration for each of these areas, aspects of necessity, practicality, degree (loose/tight) and timeframe (short/medium to long) should be considered.

3.2.3 Practice management systems

Practices currently operate systems for the management of patient appointments and for billing. While these systems will need to be aware of video consultation bookings, there is no apparent necessity, in the short-term, to provide any integration between the systems and video consultation.

Further, the currently available video endpoints do not lend themselves to such integration without effort which may be disproportionate to the benefits achieved. In the short-term, it is recommended that a pragmatic approach be taken to incorporate video consultations into the activities of a practice through minor adjustments to the existing administrative workflow. This may be illustrated by the following three scenarios:

Scenario 1. GP consultation to a patient's home

For GP seeing a patient at their home by video, an appointment may be made in the practice's usual way. An indication can be made in the appointment record that the patient is being seen by video. Where the GP has video consultation facilities in their consulting room (ie. Hardware VC or PC-based VC software) then they conduct the link from their consultation room in the usual way. Where there is a dedicated telehealth room in a surgery, then a simple booking mechanism for that room would be required. A mechanism for billing for this type of activity would also be required. Options for billing could include taking credit card details over the telephone before/after the link, or allowing patients who are seen this way to have an account.

Scenario 2. GP Consulting with a specialist

For a GP consulting with a specialist, an appointment will be required in systems at both practices and there will be a need to manually co-ordinate such bookings between the GP and specialist practices. As with scenario 1 described above, consultations could be conducted from the usual consulting rooms, or from dedicated rooms at each facility where

they exist. Again, some kind of room booking mechanism may be required within each practice. Billing at the GP end could be carried out in the usual way since the patient would be present in the GP practice. The specialist component may either be billed by credit card over the telephone or by allowing the patient to take an account.

Scenario 3. GP out of hours consultations

For a patient calling the GP out of hours service, it is assumed that neither appointments nor payment by the patient will be required.

While the first two scenarios introduce additional administrative overhead for practices, they do allow video consultation to be accommodated without major changes to existing systems. It is important to appreciate that adding video consultation as a service will inevitably add some additional administrative overhead to a practice, this overhead may include: (i) booking rooms; (ii) cross-practice organisation; (iii) cross-practice co-ordination and synchronisation – particularly in circumstances where a patient, GP and specialist must be co-ordinated to be present simultaneously and (iv) ensuring that the patient is available by video at the appropriate time.

While video consultations may be integrated into existing workflows, they will also introduce unavoidable administrative overheads. These will need to be considered and accommodated within each practice intending to use telehealth.

In the medium to long-term, it may be desirable to incorporate specific telehealth related features into practice management systems. This necessity for, the benefits of, and the nature of such changes may be best identified through early experience of administering telehealth consultations using the pragmatic approaches such as those outlined above.

3.2.4 Desktop clinical systems

As with practice management systems, in the short-term there is unlikely to be a necessity for, or a benefit to be derived from, tightly integrating discrete video conferencing hardware or software with existing desktop clinical systems. Rather, video consultation may be seen as complementary to those systems. Thus, in the short-term, hardware-based video conferencing would be used for communication in much the same way as the telephone, albeit with the capability to provide visual information.

For the convenience of the clinician user, software based video conferencing systems may be loosely integrated into a sidebar for ease of launching. This level of integration is unlikely to require significant development and is therefore may be a worthwhile investment in the short-term.

In the longer-term, usability and workflow could be improved by integrating software type video consultation systems within desktop clinical packages. Benefits that may flow from this level of integration include the ability, while in a video consultation to:

- Conveniently reference relevant information and decision support systems;
- Interact with a patient record/directory for VC;
- Share and discuss relevant information remotely (such as imaging, test results, health promotion materials) with another clinician, and/or with the patient;
- Generate and deliver an electronic prescription;
- Generate an e-Referral, either electronically directly to a specialist, or by sending a referral letter to the patient by Email.

Again, as with practice management systems, the needs and potential benefits of integration could be identified though early use of telehealth in a standalone (ie. non-integrated) fashion. Until there is significant experience of the use telehealth in the general practice context, it is difficult to fully anticipate the requirements or practical implementation issues associated with integration.

IRR4 *In the short-term, tight integration with clinical systems is not achievable. In the medium to long-term there will be benefits of integration however not enough is currently known. Experience gained from early adopters could be used to inform future requirements.*

3.2.5 Scheduling and co-ordination systems

As mentioned previously, it will be necessary to have mechanisms to allow the co-ordination of telehealth activity. These mechanisms will need to take into account the patient, GPs and the specialists. This requirement must not be underestimated since while appointments may be scheduled without difficulty, it would be unrealistic to assume that such appointments will always run on-time.

As outlined in the discussion of practice management systems integration, it is suggested that co-ordination be initially addressed using a manual process and make use of existing

practice booking systems. In the shorter term, there does not appear to be a benefit in developing and integrating an inter-practice scheduling and booking system.

In the medium to long-term, an online booking and co-ordination system may be beneficial.

As with the preceding discussions, the requirements for such a system and its integration needs would be best determined in the light of early experience of telehealth in the primary care environment.

IIR5 *In the short-term, there is insufficient time, or perceived benefit, to recommend the development of a telehealth scheduling and co-ordination system. Early experience could inform the necessity of and requirements for such a system.*

3.2.6 Summary

In the short-term, investment in the integration of video consultation with existing software products is unlikely to yield a benefit for two reasons:

Firstly, most contemporary video communications systems may be viewed as being analogous to the telephone. That is they are a potentially useful tool for a clinical practice, but not one that may be easily (or even necessarily) integrated with existing electronic systems. Beyond the short-term, technology convergence is presenting new opportunities to integrate systems.

Secondly, because there is little practical experience of video consultation in primary care, the benefits and issues of integration with other systems is unknown.

Thus, the opportunity, necessity and benefits for integration in the short-term do not exist.

The new opportunities presented by technology convergence, together with experience gained from the early adopters of video consultation in the primary care setting will provide the necessary environment for proper consideration of integration opportunities and benefits. Such integration will likely allow video consultations to be conveniently and efficiently accommodated within practice workflows in the future.

IIR6 *Tight integration of video capabilities with other practice systems should be deferred to (i) allow converged applications to develop maturity and (ii) gain practical experience of video consultation in the primary care setting. Such experience will*

inform the need, degree and benefits of integration. Convergence will provide the opportunity to do so.

3.3 Hardware, software and support

A minimal set of functional (FR) and non-functional (NFR) requirements have been identified as necessary for the implementation of a safe and effective video-consultation service. These requirements are appropriate for video consultations in the following scenarios: (i) GP to specialist; (ii) GP to a patient's home and (iii) Patient at home to an after hours GP service.

3.3.1 Medium to long-term functional requirements

FR1 *Ability to position a camera, either manually or under remote control, to provide various views of a patient*

FR2 *Ability to capture and transmit video images of sufficient quality (frame rate and image quality) for a range of clinical work. This requirement is not necessarily asymmetric*

FR3 *Adequate quality audio to ensure clear communication*

FR4 *An ability to authenticate the user of the service (both clinician or patient)*

FR5 *Security of sessions, provided by strong encryption*

FR6 *A mechanism to allow audit of services provided*

FR7 *An electronic method for a patient to consent to access a shared EHR*

FR8 *A method of electronic patient billing*

FR9 *Adequate telecommunications at provider and recipient locations*

FR10 *A healthcare provider directory. The directory will be role appropriate (i.e. provide different views depending on whether the user is a patient or clinician. Presence functionality should be available in the clinician view.*

3.3.2 Medium to long-term non-functional requirements

NFR1 *Where possible, established industry standards should be used*

NFR2 *Pervasive access is required since many clinicians practice at multiple locations*

NFR3 *Ease of use with limited training*

NFR4 *Appropriate ergonomics for the surgery and for home*

NFR5 *Access to recorded sessions must comply with relevant federal and state privacy and security requirements*

NFR6 *Authentication could be integrated with a national health identifier back-end infrastructure, with consideration of two-factor authentication*

No specific requirement to record sessions, other than for educational purposes was identified.

3.3.3 Supporting systems

- Shared electronic health records – because telehealth implies distance between patient and provider, some form of shared electronic health record, either in the form of a summary or full access to records will be necessary.

Since MBS reimbursement for teleconsultation will be available before EHRs systems are implemented, manual systems will need to continue in the short-term

- Backend infrastructure – to provide authentication mechanisms for clinicians and patients to identify themselves and to allow interoperability between health-providers networks in a heterogeneous environment.

HSSR1 *MBS reimbursement will be in-place before there is an implemented electronic means for authentication. Therefore in the short-term, or until demonstrations show otherwise, it is recommended that consultations take place only to/from the premises of a recognised health provider, where an individual is known or can be reliably identified.*

- An online health provider registry in order that clinicians may locate suitable local practitioners for referral where necessary.

HSSR2 *A national provider registry that includes healthcare provider capacity to engage in telehealth sessions will be important for the future operation of telehealth.*

3.3.4 Supporting processes

3.3.4.1 Technical Support

Telehealth requires technical support, both at the time of establishment of a service and during ongoing operation. The degree of support varies according to the complexity of the implementation. It is unlikely that most practices will have sufficient experience or on-site resources to allow the establishment of new services, therefore external support may be required. Practices which are based away from metropolitan centres may also have difficulty to sourcing good quality local support. In addition, technical support may not be economically available to small practices irrespective of location.

HSSR3 *To achieve economies of scale, and to avoid disadvantaging small or remote practices, it is recommended that some form of aggregated support arrangement is put in place. This may take the form of a nationally, regionally or locally negotiated contract with accredited suppliers for service establishment and for ongoing support.*

HSSR4 *For the convenience of medical practices, it is recommended that access to telehealth helpdesk services be considered for support calls, management of problem resolution and to escalate issues with support providers as necessary.*

Under this arrangement, consideration should be given to the helpdesk, and external support contractors providing coverage of an extended working day in order to meet the requirements of practices.

HSSR5 *It is recommended that any contract with external support organisations ensures that sufficient expertise and equipment will be available to respond to problems, and to rectify problems, within a specified period of time. Response time should be fixed (eg. 4 hours from time of first call). Geography can preclude a fixed rectification time and hence such times would need to be negotiated based on the location of the equipment and distance to the nearest technical support.*

Specific arrangements should be considered to cover the video consultation component of the GP After Hours helpline when it becomes video enabled in 2012.

Telehealth is dependent on technology and hence technical support is critical to a successful and sustainable deployment. Poor, expensive or unavailable support is a significant risk to the take-up and acceptance of telehealth by clinicians.

3.3.4.2 Education, marketing and support – clinicians

As previously described, the stakeholder consultation process identified a number of concerns which should be addressed. In particular, the understanding of telehealth within the GP population appears to be limited and a number of the concerns of this group may result from that limited understanding (for instance, assuming that telehealth is intended to replace hands-on, in-person practice). Nonetheless, the concerns are legitimate and need to be addressed. For telehealth to succeed beyond use by enthusiasts, clinicians must be confident in its safety, effectiveness and efficiency.

A program of education, training and support for clinicians will be required both before and after the introduction of video consultation. It is understood that significant funding is available for this process but that a comprehensive education and training plan has not as yet been finalised. Given the timeframe to the implementation of MBS items, this is a risk to the successful implementation of telehealth.

It should not be assumed that the clinical workforce will be enthusiastic about the introduction of telehealth. A poor level of acceptance of this new modality is a significant risk to its success and substantial marketing and education may be required both before and during implementation.

HSSR6 *Given the short lead time and concerns expressed during the stakeholder consultation process, it is recommended that an engagement, education and communications process commences as a priority.*

HSSR7 *Practicing by telehealth is different to in-person practice. Clinical guidelines for consultation by video will need to be developed prior to the implementation of MBS item numbers.*

3.3.4.3 Education, marketing and support – patients

As telehealth is not covered regularly in the general media, it is important that the expectations of the public are appropriately managed. If not, there is likely to be mismatch between patients and the number and nature of video-based services that will be available to them, particularly in the short-term and even more so at home.

HSSR8 *It is recommended that any promotional activities directed to health consumers is carefully considered, both in terms of timing and content, prior to and following the introduction of video consultation.*

3.3.5 Technical requirements

Video consultation is a demanding application, both for the endpoints and for the networks which connect the participants. This section outlines why this is the case and proposes some minimum technical recommendations. These requirements are based on current common practice and experience with clinical telehealth.

3.3.5.1 Background

The user's expectations of video performance are radically different to that of other typically used networked applications such as Email or web-browsing. While a user may readily accept, or even expect, delay in the transmission of an email or the loading of a web page, any kind of delay or interruption that occurs during an interactive video conversation makes communication very difficult or impossible. Any degradation in performance will be directly reflected in the conversation in the form of poor video (e.g. pixelation), loss of lip-sync or audio drop out. In some cases, degradation may lead to calls failing to connect, or calls clearing mid consultation. Such issues have been commonly cited as reasons for poor acceptance of video-based telehealth by clinicians.

3.3.5.2 An overview of technical issues relating to video consultation

From a broad technical perspective, the key difference between video consultations and the other typical networked applications mentioned above is that they must be delivered, and sustained, in real-time without loss of information for the duration of the conversation. This puts heavy performance demands on endpoints and on the networks in the path of the consultations.

For video endpoints, the key performance issues relate to the need to encode images from a camera while simultaneously decoding a video stream received from a network for display on a monitor. Both activities must be conducted with the least delay. In hardware-based video conferencing systems, these functions are implemented in silicon and may be tuned for high performance. In software-based video applications, all functions (video encoding/decoding and call control) must be carried out by the host PC and hence the specification of that PC will be an important factor in the quality of the video link.

For networks, the performance challenge is to ensure that real-time video traffic is delivered between endpoints with the least delay and with the least loss of information. This is a significant problem on shared networks such as the Internet where many users and applications are competing for network resources and where both bursty and constant-bit rate traffic such as video must co-exist.

Aspects which impact on the quality and performance of video consultation are discussed below. Recommendations are presented for each aspect.

3.3.5.3 Software video conferencing - host PC

As previously mentioned, when a PC is used to implement a video endpoint, the specification of the device will impact on observed performance. It would not be meaningful to provide a minimum specification for a PC-based endpoint as the requirements would depend on the particular software application in use, and its configuration.

TRR1 *Where software-based products are proposed, careful consideration should be given to match the product requirements against PC specifications.*

3.3.5.4 Camera

Received video quality is dependent on the specification of the camera which captures the image. For most hardware-based video conferencing system, the quality of the captured images is sufficient for clinical work. For software-based products, designed to be used with a webcam, results will naturally vary dependant on the camera selected.

For diagnostic or complex clinical management (*diagnostic quality VC*), using hardware-based video conferencing, the following five recommendations (TRR2 to TRR6, supported on all commonly available equipment) are made:

TRR2 *Image sensor: minimum ¼ type CCD image sensor*

TRR3 *Horizontal resolution: 460 lines (PAL)*

TRR4 *Focus: autofocus*

TRR5 *Optical zoom ratio: minimum 10x*

TRR6 *Standards-based far-end control of pan/tilt/zoom*

For non-diagnostic and non-complex clinical management (*general quality VC*), TRR2 to TRR6 also apply for hardware-based products. For software-based products (i.e. which use a webcam for video input) then the following three recommendations are made:

TRR7 *Image sensor: CMOS or CCD type*

TRR8 *Minimum resolution: VGA (640x480)*

TRR9 *Frame rate: 30 FPS (at VGA resolution)*

3.3.5.5 Display

Modern displays are capable of displaying a range of image types and a range of resolutions. The choice of display may be made pragmatically depending on the type of video conferencing hardware. For instance, if high-definition (HD) hardware-based VC is being used, then HD displays should be used. If a software application is to be used then a standard contemporary PC monitor will be acceptable.

TRR10 *Choice of display should be made pragmatically depending on the circumstances. Contemporary display monitors are adequate for video conferencing.*

3.3.5.6 Frame rate

The importance of frame-rate depends on the clinical application. Where motion is being assessed then frame-rate is important.

Most video conferencing systems typically attempt to encode and deliver 30 frames per second (FPS) but will adapt according to need – that is, they may send less frames if reduced motion is detected in the field of view of the camera. At a sustained rate of 30 FPS, diagnostic and complex clinical work could be conducted. However, for many settings, such a high frame rate is unnecessary. In the authors' experience, 15 fps can be safe and effective for a wide range of clinical applications in the hospital setting, including those where motion is important such as assessment of gait. For many interactions relevant to primary care, a frame rate of greater than 25 FPS may be unwarranted.

TRR11 *A frame rate of 25 FPS is adequate for primary care video consultations*

3.3.5.7 Bandwidth

Bandwidth, or more properly, throughput (expressed in kilobits per second [kbit/s] or megabits [Mbit/s] is an important consideration for video communication.

In hardware-based video conferencing, dedicated switched digital connections achieved using ISDN (Integrated Services Digital Network) have often been used to provide guaranteed performance between endpoints. With this arrangement, video calls may be made, typically at 128kbit/s, 256kbit/s or 384kbit/s, though higher speeds are supported.

For most clinical applications, at standard-definition (SD), connections at a guaranteed rate of 356kbit/s are adequate for diagnostic work or complex management. Lower rates are also acceptable for routine non-diagnostic and non complex management. With the advent of HD, higher throughput is required to send the larger HD images.

TRR12 *For diagnostic or complex clinical management, using hardware-based SD VC, a minimum throughput of 384kbit/s should be available*

Where the Internet is used and throughput is not guaranteed, over-provisioning will be needed. Standards-based hardware video conferencing can perform well over symmetric BDSL connections at 512kbit/s and over asymmetric ADSL2 connections which have been significantly over-provisioned to achieve an adequate bit-rate in the upstream direction.

For software applications, it is not possible to nominate a minimum bandwidth since there are a multitude of software packages, each with their own performance characteristics.

Further work would be needed to assess video quality and performance against throughput.

3.3.5.8 Latency

Latency relates to delay. Most often, it is used to describe delays incurred within a network. However, for video consultations there are two additional important sources of delay - these are: encoding delay (which occurs as images from the camera are encoded for transmission) and decoding delay (incurred as images from the network are decoded for display).

For video consultations, low latency is required since as previously described, delay may result in poor video performance.

TRR13 *For video consultations, to avoid poor performance, round-trip latency must be lower than 300ms*

3.3.5.9 Packet loss

Packet loss relates to data which is lost in transit between endpoints. In busy networks this is a natural phenomenon and its impact on common applications such as web-browsing and email is managed through detection and retransmission of lost data.

In video applications, where a large amount of data is being exchanged, even a small level amount of lost data can have a significant impact on the resulting conversation. This for safe and effective video consultation, it is important that packet loss is minimised.

TRR14 *For video consultations, to avoid poor performance, packet loss should be less than 0.1%*

3.3.5.10 Audio

Audio quality must be sufficient for clinical consultation. Hardware VC systems typically encode and transmit audio at 64kbit/s which provides good intelligibility. However, lower bit rates may also be adequate and allow more efficient use of available network resources. Where network resources are limited, assuming the endpoints are configurable, using less bandwidth for audio will allow more to be available for video thus improving the overall experience. Although very low bitrate audio algorithms are available, they are typically offer only very low fidelity.

TRR15 *For clinical consultations, to avoid poor intelligibility, audio should be encoded at a minimum of 16kbit/s*

3.3.6 Technical options

This section provides a description and analysis of the technical options available for the provision of a video-based consultation service. These options are assessed against the functional and non-functional requirements identified in the previous section.

Two distinct technical areas are addressed: Firstly, the *endpoints* are considered, that is the systems and interfaces that the end-users, i.e. the clinicians and patients, use directly to establish, communicate-through and close the video interaction. Secondly, the *infrastructure*

is considered, that is the necessary back-end equipment and networking that is required to support a video consultation service.

3.3.6.1 Endpoints

There are two approaches to providing a video consultation endpoint: (i) using dedicated hardware or (ii) using a software application that runs on a computer. Where a software application is used, there are a number of different options.

This section presents four options (1 hardware, 3 software) which may be used to provide endpoints for video based consultations. Each option is described and subsequently assessed against the functional and non-functional requirements previously identified.

3.3.6.1.1 Option 1: Hardware standards-based video conferencing

For this option, dedicated hardware is required. There are a number of commercially available products, which while not designed specifically for the clinical environment or for clinical tasks, are used routinely for providing health services at a distance. Globally, Tandberg and Polycom hold the majority of the market share of hardware video conferencing systems in the health sector. The description of hardware base video conferencing which follows applies to most available systems irrespective of manufacturer.

A typical hardware-VC based configuration includes:

- At least one camera, additional cameras may be used to achieve multiple views;
- A terminal unit which provides audio and video processing capabilities and networking
- At least one display monitor;
- Built-in and/or external microphones;
- User interface, provided by a hand-held remote control;
- The ability to interface external devices such as document cameras, digital stethoscope, ultrasound imaging equipment;
- Third party add-ons can be used to provide alternative user interface system (e.g. AMX);
- Often dedicated space is used with attention paid to physical privacy and consideration of environmental features such as soundproofing and lighting.

Hardware-based video conferencing systems implement and conform to industry standards for call control, audio and video encoding/decoding, remote camera control and security).

These standards are described in the table below. By implementing key features, such as digital signal processing and encryption, in hardware these systems are able to offer a high level of performance. Systems usually implement a comprehensive range of facilities and are highly configurable.

For the office environment, desk top units which integrate the camera, microphone, terminal unit and display into a small form factor package are also available from several manufacturers. While these systems may be ergonomic for the desk top, they may implement only a subset of the video conferencing standards (e.g. supporting SIP but not H.323) and may offer lower performance (e.g. lower quality camera) and fewer options (eg. fixed camera, no positioning possible) than the non-integrated systems described above. This reduced performance and functionality may be important both for interoperability and for some clinical interactions.

Table 1: An overview of technical standards relating to video conferencing

Standard / Recommendation	Area of standardisation
<i>H.323 (ITU-T)</i>	<i>Non-guaranteed bandwidth, Packet switched networks</i>
H.225	Multiplexing
H.235	Authentication
H.245	Control
H.261 QCIF, H.263	Video
Q.931	Call signalling
RTP	Timing/Synchronisation for audio and video
G.711, G.722, G.728, G.723, G.729	Audio
TCP/IP	Network interface
<i>H.320 (ITU-T)</i>	<i>Narrowband switched digital (ISDN 64Kbit/s – 2Mbit/s)</i>
H.221	Multiplexing
H.230, H.242	Control
H.261, H.263	Video
G.711, G.722, G.722.1, G.728	Audio
T.120	Data
I.400	Network interface
<i>SIP (IETF) defined in RFC3261</i>	<i>Signalling protocol for call control, voice and video over IP</i>
Related standards	
H.263, H.264, H.264+	Video
G.711, G.722.1, G.722, G.729ab, MPEG4-AAC	Audio
SDP	Media stream parameters
RTP	Audio and video
TCP, UDP or SCTP	Network interface

In addition to the endpoint equipment, manufacturers offer a range of hardware to allow an enterprise to build a sophisticated video conferencing infrastructure. These devices include: (i) multipoint control units (MCU) (often described as “bridges”) for managing multi-party conferences; (ii) gateways to allow communication between networks which implement different standards; (iii) gatekeepers for address translation, bandwidth management and call admission and control and (iv) content servers for recording and distributing audiovisual material.

Hardware video conferencing devices are typically high-cost and only economically viable where sufficient consultations would take place to gain economy of scale. These options may also be over specified for some clinical applications where the requirement for high-quality real-time video is not indicated. In addition to hardware costs, licensing costs typically apply (e.g. to software options, MCU sessions etc).

Aside from cost, there are two limitations of hardware-based video conferencing: firstly, it is not possible to provide tight integration with software-based systems (e.g. practice management) and secondly off-the-shelf systems do not support features that are important to a health interaction, such as: a mechanism for billing; a mechanism to allow the patient to consent for clinicians to access shared health records and a mechanism for the patient to confirm that they have received a service (as per signing a Medicare form as occurs following a conventional in-person consultation).

3.3.6.1.2 *Option 2: Software/PC standards-based video conferencing*

3.3.6.1.3 *This option describes the use of PC-based software products that implement the same industry standard communications protocols as described in Option 1. The key difference between this option and Option 1 is that all capabilities are implemented in software and hence no dedicated video conferencing hardware is required. The only additional hardware items required to support a video consultation with this option are a webcam and a microphone.*

Subject to performance issues discussed below, video consultation may make use of existing PCs within a practice or at a patient’s home thus not requiring dedicated space but rather adding additional value to an existing system. In addition, the point-and-click interface will be familiar for users. For this option, dedicated video conferencing software is installed on the PC. Because this software requires technical and user support (installation and

configuration problems, dealing with user problems, version control) large-scale deployment has significant implications.

Because all capabilities must be implemented in software on a host PC, the performance of the PC is a critical factor in the overall performance of the video session. In particular, video processing and encryption have higher processor demands than most everyday desktop applications. Therefore, for a high quality video consultation, a minimal PC specification must be defined. This specification should be based on the video software manufacturer recommendations. It is possible that many existing desktop computers may need to be upgraded to provide an adequate level of performance using encrypted video conferencing standards.

While Option 1 provides high-quality cameras capable of electronic (local and remote) control, software based systems usually use Webcams for the capture of video and audio. These cameras are readily available, relatively inexpensive and with improving quality. They differ in a number of ways to the cameras used in hardware-video conferencing systems. Firstly, the optical capabilities of hardware VC systems (excepting the integrated systems) are superior. Secondly, the near-end and far-end cameras are able to be positioned (ie. Pan/tilt/zoom) electronically. Webcams are, in general, fixed devices (where motion capability is provided, it is usually provided in a proprietary manner). A webcam must be physically moved to achieve the desired view. This may have advantages in that a precise view may be requested and viewed, it may also have the disadvantage of being inconvenient and time-consuming achieving the desired view during a consultation. For laptop PCs with integrated cameras, achieving a suitable view (other than head and shoulders) may be awkward. For laptop PCs in particular, care must also be taken in selecting a system with an adequate camera and adequate processing power to support encrypted real-time video consultations. Unlike the hardware-based option, software-based VC does not allow the interfacing of external medical equipment.

While the cost of software-based video conferencing is less than the purchase of dedicated hardware, the software is a commercial product and is usually subject to purchase and per-user or per-machine licence costs. Since the market for mass home-based video conferencing for health does not yet exist, it is impossible to predict how manufacturers and vendors will respond with regards to pricing their products.

3.3.6.1.4 Option 3: Software/PC proprietary video conferencing

Option 3 describes the use of PC-based proprietary video conferencing software which requires a software client to be installed on the user's PC. Both PC-based software (eg. Skype, MS Messenger) and commercial products (eg. Video) are freely available. It is beyond the scope of this section to provide a full review of all available products, however a general outline of issues related to this option is provided.

In common with Option 2, this option makes use of an existing PC and requires the installation of dedicated software. Some of the advantages and disadvantages of this approach are also common to those identified in Option 2. In particular, they usually have an easy to use interface and the freely available products are popular with the public and have an established user-base. However, the support for the freely available software is very limited. Additional support would be needed to assist users with any installation or ongoing usage problems. The issues relating to camera positioning and image quality raised in Option 2 also apply to this option.

The freely available packages were typically developed for social networking or domestic use. While this type of software has advantages of being no-cost, easy to use and able to run on any PC there are some serious limitations, particularly pertaining to security and privacy, of relevance to video-based consultations which are summarised below:

- Proprietary software, networks and trust

Proprietary approaches (sometimes peer-to-peer) are often used for call control, routing and encryption. These methods are unpublished, unable to be inspected and hence not trustable. Further, since calls are mediated by third party systems there are implications for availability, security and privacy. While the level of risk presented by this situation may be acceptable to individuals for social use, it is not likely to be acceptable in the health provider-patient context.

- Authenticity of the end-user

With the freely available software, no identification check is made when a user registers to create an account. Therefore, the authenticity of the end-user cannot be guaranteed. There is therefore a risk of masquerading, either as a practitioner or a patient receiving a service.

- Audit

The requirement for audit is beyond the scope of the intended use of the freely available software products and networks.

The commercial products were developed primarily for the business market. Since they are also proprietary, their mechanisms are also unable to be inspected and difficult to trust. In contrast to the freely available products, commercial support is available. Since the software is priced on a per-copy or per user basis, it may be costly to scale. As with the previous options, it is unclear how the market would respond to a mass roll-out and hence it is difficult to comment precisely on the economics.

A review of a number of the technical capabilities of currently available video conferencing systems has been conducted. The results are shown in Table 2.

Table 2: Technical capabilities of currently available video conferencing systems

Product	Communications	Interoperability	Video standards	Audio standards	Supported video specifications ¹	Maximum resolution	Maximum bandwidth
Tandberg Set-top codec (e.g. 990 MXP ²)	ISDN, H.323, SIP	Standards-based	H.261, H.263, H.263+, H.263++ (Natural Video), H.264	G.711, G.722, G.722.1, G.728, 64 bit & 128 bit MPEG4AAC-LD	4CIF, CIF, QCIF, XGA, SVGA, VGA, w228p, w448p, w576p, w720p @ 30 fps	1280x720	IP: up to 2 Mbps ISDN: up to 512 kbps
Tandberg Desktop system (e.g. 1700 MXP ³)	H.323, SIP	Standards-based	H.261, H.263, H.263+, H.263++ (Natural Video), H.264	G.711, G.722, G.722.1, G.728, 64 bit & 128 bit MPEG4 AAC-LD	4CIF, CIF, QCIF, XGA, SVGA, VGA, w228p, w448p, w576p, w720p @ 30 fps	1280x720	Up to 2 Mbps
Tandberg Software (e.g. Movi ⁴)	H.323, SIP	H.323 requires VCS internetworking	H.264, H.263+, H.263	MPEG4 AAC-LD 48 kHz, G.722.1 24 kbps, G.722.1 32 kbps, G.711 A-law, G.711 μ -law	4CIF, CIF, QCIF, XGA, SVGA, VGA, w228p, w448p, w576p, w720p @ 30 fps	1280x720	24kbps to 8 Mbps

¹ SIF = 352x240, CIF = 352x288, FCIF = 432x240, QSIF = 176x120, QCIF = 174x144, 4SIF = 704x480, 4CIF = 704x576, XGA = 1024x768, SVGA = 800x600, VGA = 640x480, w288p = 512x288, w360p = 480x360, w432p = 768x432, w448p = 768x448, w540p = 960x540, w576p = 1024x576, w720p = 1280x720, w1080p = 1920x1080,

² http://www.tandberg.com/collateral/product_brochures/TANDBERG%20Set-top%20990%20880%20770%20MXP.pdf

³ http://www.tandberg.com/collateral/product_brochures/TAN_ProdSht_1700MXP_a1_FA.pdf

⁴ http://www.tandberg.com/collateral/product_brochures/TANDBERG%20Movi%20Product%20Sheet.pdf

Polycom Set-top codec (e.g. HDX 6000 series ⁵)	H.323, SIP	Standards-based	H.264, H.264 High Profile, H.263++, H.261, H.239 / Polycom People+Content, H.263 & H.264 Video Error Concealment	Polycom StereoSurround™, Polycom Siren™ 22, Polycom Siren 14, G.722.1 Annex C, G.722, G.722.1, G.711, G.728, G.729A	QSIF, QCIF, SIF, CIF, 4SIF, 4CIF, w720p @ 30 fps (from 512 Kbps), w1080p @ 30 fps (from 1 Mbps)	Send: 1280x720 Receive: 1920x1080	128 Kbps to 2 MBps
Polycom Desktop system (e.g. HDX 4000 series ⁶)	H.323, SIP	Standards-based	H.264, H.263++, H.261, H.239, H.263 & H.264 Video Error Concealment	Polycom StereoSurround™, Polycom Siren™ 22, Polycom Siren 14, G.722.1 Annex C, G.722, G.722.1, G.711, G.728, G.729A	QCIF, QSIF, CIF, SIF, 4SIF, 4CIF, w720p @ 30 fps (from 832 Kbps)	1280x720	Up to 4 Mbps
Polycom Software (e.g. CMA Desktop ⁷)	H.323	SIP not available	H.261, H.263, H.263+, H.264	G.719, Polycom Siren™ 14, G.722, G.722.1, G.711, G.728, G.729A	Dependant on capabilities of PC/webcam/remote end	1280x720 *subject to computer specifications	
LifeSize Set-top codec (e.g. LifeSize Team 220 ⁸)	H.323, SIP	Standards-based	H.261, H.263, H.263+, H.264 and H.239	G.711, G.722, G.722.1C, G.728, G.729, MPEG-4-AAC-LC	912x512, w575p (from 512 Kbps), w720p (from 768 Kbps), w720px60 (from 1.1 Mbps), 1080p (from 1.7 Mbps)	1920x1080 *with suitable camera	128 Kbps to 6 MBps

⁵ http://www.polycom.com.au/global/documents/products/telepresence_video/datasheets/hdx6000-datasheet.pdf

⁶ http://www.polycom.com.au/global/documents/products/telepresence_video/datasheets/hdx4000-datasheet.pdf

⁷ http://www.polycom.com.au/global/documents/products/telepresence_video/datasheets/cma-desktop-datasheet.pdf

⁸ http://www.lifesize.com/~media/Media_Kit/Product_Datasheets/Team/Team_220/LifeSize_Team220_Datasheet_EN.ashx

LifeSize Desktop system (e.g. LifeSize LGExecutive ⁹)	H.323, SIP	Standards-based	H.264, H.263, H.261 & H.239, H.239 transmit uses H.264	G.711, G.722, G.722.1C, G.728, G.729, MPEG-4-AAC-LC	FCIF, 720x400 (from 384 Kbps), 800x488 (from 512 Kbps), 1024x576 (from 768 Kbps), w720p (from 1.1 Mbps) @ 30 fps	1280x720	128 Kbps to 2 Mbps
LifeSize Software (e.g. LifeSize Desktop ¹⁰)	SIP	H.323 not available	H.264, H.263+, H.263-2000	AAC-LC, G.722.1c, G.722, G.711	Dependant on capabilities of PC/webcam/remote end	1280x720	128 Kbps to 1.1 Mbps
Vidyo Set-top codec (e.g. VidyoRoom HD-100 ¹¹)	Vidyo (proprietary)	H.323 and SIP via VidyoGateway	H.264 SVC, H.264 AVC, H.263+	SPEEX Wideband, G.711, G.722	w360p, w540p (from 512 Kbps), w720p (from 1 Mbps), receive w1080p (from 2 Mbps) @ 30 fps	Send: 1280x720 Receive: 1920x1080	2 Mbps
Vidyo Software (e.g. VidyoDesktop ¹²)	Vidyo (proprietary)	H.323 and SIP via VidyoGateway	H.264 SVC		Dependant on capabilities of PC/webcam/remote end (up to w720p @ 30 fps)	Send: 1280x720 Receive: 2560x1440	
Sony Set-top codec (e.g. PCS-XG55 ¹³)	H.320, H.323, IEFT SIP	Standards-based	H.261, H.263, H.263+, H.263++, H.264, MPEG-4SP@L3 (SIP only)	MPEG-4-AAC (mono/stereo), G.711, G.722, G.728	QCIF, CIF, 4CIF, w288p, w432p, w576p, w720p	1280x720	IP: 64 Kbps to 4 Mbps ISDN: 56 Kbps to 768 Kbps

⁹ http://www.lifesize.com/~media/Media_Kit/Product_Datasheets/LGExecutive/LGExecutive_powered_by_LifeSize_Datasheet.ashx

¹⁰ http://www.lifesize.com/~media/Media_Kit/Product_Datasheets/Desktop/LifeSize_Desktop_Datasheet.ashx

¹¹ http://www.vidyo.com/documents/datasheets-brochures/VidyoRoomHD-100_DS-US.pdf

¹² http://www.vidyo.com/documents/datasheets-brochures/VidyoDesktop_DS_US.pdf

¹³ <http://www.sony.com.au/product/pcs-xg55>

Skype ¹⁴	Proprietary	Phone calls (via Skype servers)	Not published	Not published	Dependant on capabilities of PC/webcam/remote end	Dependant on capabilities of PC/webcam/remote end	Dependant on computer internet connection
Windows Live Messenger ¹⁵	Proprietary	None	Not published	Not published	Dependant on capabilities of PC/webcam/remote end	Dependant on capabilities of PC/webcam/remote end	Dependant on computer internet connection
Ekiga ¹⁶	H.323, SIP	Standards-based	THEORA (SIP only), H.264 (SIP only), H.263 (SIP only), H.263+ (SIP only), H.261 (SIP and H323), MPEG4 (SIP only)	G.711-Alaw, G.711-uLaw, Speex (NarrowBand/WideBand), G.722 (wideband), iLBC, GSM-06.10, MS-GSM, G.726, G.721, CELT ultra-low delay	176x144 to 704x576	704x576	Dependant on computer internet connection

¹⁴ <http://www.skype.com/intl/en/home>

¹⁵ <http://explore.live.com/windows-live-messenger?os=other>

¹⁶ <http://ekiga.org/ekiga-softphone-features>

3.3.6.1.5 Option 4: –Skype 4 Health”

The three options presented so far have described general purpose video communication tools. The systems are designed for general rather than clinical use and hence are not tuned to clinical interactions. This fourth option or concept presents an alternative approach for the medium to long term which proposes the design and development of a custom PC-based system. Such a system, designed with clinicians, patients and health interactions in mind, may provide the opportunity to overcome some of the deficiencies of the options previously described. This option presents the most flexibility for developing a scalable and pervasive telehealth service that may be integrated with relevant back end systems such as billing, EHR and authentication.

In outline, this option is similar to the –Skype 4 Health” concept suggested by NICTA whereby a product, similar to Skype, could be developed but –with better quality video, auxiliary data streams and appointment scheduling”.⁶⁸ This option further refines the concept and presents alternative priorities for development. Since the option involves the development of a software product, there is great opportunity to embed useful features that are problematic or impossible, to provide with the aforementioned options.

As per the NICTA concept, video of greater quality than that currently offered by services such as Skype would be essential for some diagnostic work, particularly in situations where a doctor is not present locally with the patient during the consultation. For consultations between a GP and specialists, it appears unlikely that additional data streams would be useful. However, for monitoring of patients at home this would be an essential function.

The development of a new application offers the opportunity to integrate features that are important to interactions between clinician and patient. These include:

- *Electronic billing*

Since telehealth implies distance between patient and provider, the usual method for receiving payment (i.e. immediately following consultation) does not exist. Since this option is software based, it would be possible to include an electronic payment method within the teleconsultation product.

- *Electronic consent for access to EHR*

Successful implementation of telehealth requires that clinicians have access to health records for their patients. With a custom developed software-based product it would be possible to incorporate a mechanism within the application whereby the patient may electronically consent to the access of their health record.

- *Electronic patient confirmation of service provided*

In the conventional in-person mode of consultation, the patient signs a Medicare form to confirm that a service has been provided. A video-based encounter does not offer this possibility. While a physical form could be mailed to the patient for completion, as with billing and EHR consent, an electronic mechanism for confirming receipt of service could also be embedded into the application.

- *Authentication of the patient using the national health identifier*

A method of authentication of the user (patient and clinician) using an individual healthcare identifier to a national back-end infrastructure could be embedded into the application. This is simply not possible within the other options previously presented.

- *Appointment scheduling*

The NICTA concept suggests appointment scheduling could be a feature of the “Skype 4 Health” concept. While it will be important to have a mechanism to schedule the attendance of the various parties involved in a consultation, it should not be assumed that a new technological approach is the most appropriate. Practices already have existing scheduling systems and introducing a second system to the practice, for which the only purpose is to book video-based work, may be unattractive. In a heterogeneous environment and in the short-term, for consultations involving GPs and specialists, it may be more pragmatic for practices to schedule video consultations in the same way that they schedule face-to-face consultations, using existing systems. Verbal co-ordination between practice administrators may be sufficient to ensure that bookings may be scheduled between GPs and a specialist. For GP or specialist consultations with a patient at home, existing booking systems may be used for arranging appointments with a flag to indicate that the consultation is to be conducted by video, rather than in-person. Such approaches imply least change to practice

systems and are a pragmatic approach to integrating video consultations within the usual practice workflow.

Options for implementation

There are two distinct options for the implementation of a custom –Skype 4 Health” type application:

- Using client software which is installed on the user’s PC (similar to Option 2 and option 3), or
- Using a clientless secure web-based personal health access portal – that is, a service accessed via a web browser that provides an integrated suite of health-related facilities, including:
 - A role-based interface – that is, the clinician and patient receive different and appropriate interfaces;
 - Access to an online provider directory for clinicians;
 - Authentication based around a unique national health identifier;
 - Security based around https;
 - Video consultation;
 - The ability for a clinician to send, and a patient to receive an e-Prescription;
 - The ability for a clinician to send, and a patient to receive an e-Referral letter;
 - Payment;
 - A personalised patient interface with access to control their PCEHR;
 - Access to health promotion information;
 - Future extensibility, since all content is delivered via the web;

The former has disadvantages in common with Options 2 and 3, including the need to provide support for the software on many PCs without any knowledge or control of the user’s environment, and version control. This may be a significant support burden with a large implementation.

The latter option, which would be entirely web-based, obviates the need to install, maintain and support any software on the client’s PC. Thus, technical support and version control are all at the server-end.

Importantly, the option satisfies the need for ubiquity of access, provided that the user has access to a PC of sufficient specification, access to a network and a webcam. It offers a

good option to integrate a range of health specific services into a single secure portal with a high-degree of flexibility and the ability to add future services and content.

Since both sub options require significant development work, neither represents realistic considerations in the short-term. However, in the medium to long-term, supported by the pervasive communications network promised by the NBN, they offer strong options for a converged health-oriented application which combines video consultation with other relevant health resources.

3.3.6.1.6 Endpoints options against functional and non-functional requirements

Table 3: Compliance with functional and non-functional requirements - a comparison of endpoint options

Requirement	Option				
	1	2	3	4 (a) ¹⁵	4(b) ¹⁵
	Standards based Hardware VC	Standards based Software VC	Proprietary Software VC	“Sykpe 4 Health” (Client)	“Skype 4 Health” (Secure web portal)
FR1	Yes ¹	Yes ⁹	Yes ⁹	Yes ⁹	Yes ⁹
FR2	Partial ²	Partial ¹⁰	Software dependent	Yes	Yes
FR3	Yes	Yes	Software dependent	Yes	Yes
FR4	Partial ³	Partial ³	No	Yes	Yes
FR5	Yes	Yes ¹¹	Software dependent	Yes	Yes ¹²
FR6	Partial ³	Partial ³	Software dependent	Yes	Yes
FR7	No	No	No	Yes	Yes
FR8	No	No	No	Yes	Yes
FR9	Location dependent	Location dependent	Location dependent	Location dependent	Location dependent
FR10	No ⁴	No ⁴	No ⁴	Yes	Yes
NFR1	Yes ⁵	Yes ⁵	No	Yes	Partial ¹³
NFR2	Yes ⁶	Yes ¹⁴	Yes ¹⁴	Yes ¹⁴	Yes
NFR3	Yes ⁷	Yes	Yes	Yes	Yes
NFR4	Partial ⁸	Yes	Yes	Yes	Yes
NFR5	Implementation dependent	Implementation dependent	No	Yes	Yes
NFR6	Yes, but requires development	Yes, but requires development	No	Yes	Yes

¹integrated units may not have a controllable/adjustable camera; ²Demonstrated feasibility and effectiveness in some areas of clinical work with specific configurations. It has not been shown that all clinical tasks may be feasible or safely conducted using video-conferencing; ³Not supported by all manufacturers and may require further hardware; ⁴The authors did not identify any compliant off-the-shelf systems during their research; ⁵in the authors experience, standards do not guarantee effortless interoperability between manufacturers equipment; ⁶feasible, though replication of hardware would be expensive; ⁷though without regular use, the clinician will not be skilled and efficient user. Technical support is required at design and installation stage. Some ongoing technical support is required; ⁸some of the hardware systems are very space consuming; ⁹may be very awkward with a laptop with integrated camera; ¹⁰dependant on camera, PC specification, software and network; ¹¹subject to adequate PC specification; ¹²using https; ¹³VC standards would not be used for server to client video, industry standards would be used for other functions where appropriate and to provide a gateway function to industry standards based VC infrastructure; ¹⁴feasible, but may be expensive depending on the vendor's cost model; ¹⁵concept products that would require development

3.3.6.1.7 *Endpoint interoperability*

In both the short-term and long term, it is expected that systems must interoperate. Only Options 1 and Options 2 offer a high level of interoperability in the short-term. Some, but not all, of the proprietary systems offer a gateway device to allow interoperability with standards-based VC.

For options 4(a) and 4(b), where video is provided at the server-end, centralised gateway services would need to be designed into the solutions to provide interoperability with standards-based systems.

In the short-term, Options 1 and 2 are deployable and will offer interoperability. Within manufacturer interoperability will likely be more reliable than between-manufacturer interoperability.

3.3.6.2 *Infrastructure*

For video consultation, additional infrastructure, other than the endpoints previously described are required. This infrastructure includes networking (to the home, within organisations and interconnectivity via public networks). Hosted on these networks is infrastructure to support the VC endpoints (such as gateways; gatekeepers and MCUs); and backend systems for authentication and audit. These items of infrastructure are essential to allow endpoints to communicate with each other irrespective of their location. In addition, health related systems such as EHR, pathology and imaging results will also be important to support clinical consultation conducted using video.

Communications Infrastructure/Networking

Interconnectivity is essential to the functioning of telehealth. All elements in an end-to-end path between endpoints must be able to support minimum requirements for reliable video communication.

Unlike many contemporary networked applications such as web browsing and email, video requires a constant bit rate to be sustained, low latency and a low level of packet loss. Outside of well managed corporate networks, none of these requirements can be absolutely guaranteed. In particular, the consumer grade networks of today should be considered as nothing greater than best effort, that is the network will do it's best to deliver your traffic

according to the service that you have paid for, but nothing better than that. Performance will vary according to distance from the exchange, contention ratios and the activity of other subscribers in the area. Over provisioning, that is selecting, and paying for, a service that is much larger than your needs is currently the only approach to avoiding degradation, again this has no guarantee of success.

Some studies in the literature have attempted to identify minimum technical requirements such as bandwidth and latency for specific clinical applications (eg. Remote echocardiography, foetal ultrasound etc) however these studies usually have limitations and may not be generalised. Limitations include that most of the studies took place on ISDN networks, which guarantee throughput, and important features such as audio, video codec, frame rate generally were not described. Further, in the context of this report, the services were not carried out in a primary care setting and may not be directly relevant. A table of example studies is included in Appendix 1.

For general consultations, in the authors experience, while not gained in primary care, a video endpoint configured for 384Kbit/s, with 64Kbp/s audio, QCIF video at 25fps is sufficient for clinical consultations. Further, the authors reliably deliver telepaediatric and telegeriatric telehealth consultation services using a total available bandwidth of 288kbit/s, with 16Kbit/s audio and 15fps. This has been found to be reliable for all clinical services, except for echocardiography (which has not been attempted at this rate). Such services have worked well over ISDN and ADSL2 (over provisioned as described above) networks within Queensland. Experimental video work with ADSL1 and third generation wireless has not been found to be reliable enough for routine clinical use.

It is not possible to provide a comprehensive, evidence-based table of cross references of bandwidth/latency to clinical consultation type as appropriate data (that may be generalised) does not exist.

The Internet and video consultation

Access to the Internet is increasing and the National Broadband Network (NBN) promises ubiquitous, high-bandwidth network access. Today, there are a number of issues relating to the Internet that such be considered in the context of video consultation:

- Access – the Internet is not yet economically available to all Australians;

- Performance – may be good in cities, but is patchy, variable and unpredictable elsewhere. ADSL2 is not available in all exchanges. ADSL1 is unlikely to be sufficient for reliable clinical work;
- Technology - ADSL is the most common presentation of Internet access in Australia however, is not ideally suited to real-time video consultations due to its asymmetry. Further, the available “upload” bandwidth (traffic from the consumer) is a fraction of the bandwidth in the “download” (traffic to the consumer) direction. In addition, carriers make no guarantee that actual performance is equal to the carrier’s quoted link rates. To achieve adequate video performance in the upload direction, a consumer may need to select a plan with a very large, and hence costly, download link rate and a large upload/download quota. Quality of Service (QoS) - As described above, VC, and hence video consultation works best in a low latency, guaranteed bandwidth environment. While historically, VC was used on ISDN, which provided guarantees, the Internet is a shared environment which operates on a best-efforts basis. While there are protocols to allow an end-user application to request a level of service from the network, in practice, carriers do not always honour the requests. Importantly, for QoS to work, each carrier in the path between endpoints must honour the requests, requiring agreements between carriers to be in place. QoS will not be supported in the short-term. It is unclear whether the NBN will support service guarantees;
- End user’s network environment - Within the practice, or the home, there will be applications competing for wide area network access. This is particularly relevant in the home where members of the family may be using networked applications at the time of a video consultation and hence reduce the video performance. While there are technical approaches to manage this on a local area network, it would be beyond unreasonable to expect home users to implement them.

In summary, the Internet as it is currently deployed to Australian homes and practices is not ideally suited to video consultation, except where over provisioned. It is anticipated that the NBN will offer new options which will better support video to the home.

Today, if the public Internet is to be used for video consultation, then ADSL2 or cable, with a high-end configuration (upload/download/quota) is the only way to currently “guarantee” adequate performance.

Symmetric, business grade services with low contention rates would be preferable for practices who expect to provide regular video consultations.

State Health Networks

Since many specialists practice (publically and privately) in public hospitals within the state health systems, an option is to use the existing infrastructure within the state health departments to provide the “specialist end” of some consultations. The state health networks usually provide bandwidth for video work and some departments have extensive deployments of video endpoints and related infrastructure to allow gateways to the public Internet.

Further investigations are required to determine whether:

- ***This kind of interaction is acceptable within the framework of MBS funded telehealth;***
- ***The state health departments would support such use, and any conditions they would impose (eg. Receiving an episode based fee).***

3.3.7 Recommendations

3.3.7.1 Endpoints

This section provides recommendations on which of the identified video endpoint options may be used for video consultation and hence be eligible for MBS funding. In doing so, safety, effectiveness, security and privacy have been carefully considered.

Short-term

TOR1 *Where a patient is unattended by a local physician, then it is recommended that, at the patient end, Option 1, is a minimum requirement for diagnostic or complex management decisions.*

TOR2 *Where a patient is attended by a local physician, then Option 2, at the patient end (and Option 1 or Option 2 at the specialist end) is acceptable for follow-up consultations.*

TOR3 *Proprietary software video systems (Option 3) whether client-based or clientless, should be used only where requirements of privacy and security have been fully addressed and that a specific product or approach has been formally demonstrated as being safe and effective in clinical use. Such products will require individual assessment.*

Medium to long term

The medium to long term will see the deployment of the NBN and hence the provision of a pervasive high-quality broadband network. Experience will also have been gained with the short-term deployment of telehealth.

TOR4 *It is recommended that a dedicated application, or a personal health portal, which satisfies the functional and non-functional requirements identified earlier in the report be developed. This, with the promised capabilities of the NBN may facilitate mass deployment of video consultation.*

3.3.7.2 Software

Short-term

TOR5 *It is recommended that commercial off the shelf, standards compliant software (ie. Option 2) is used in circumstances where a software, rather than hardware, approach to VC is used.*

The medium to long term recommendation for software video consultation was provided in Section 3.3.7.1

3.3.7.3 Support

Recommendations for technical support were provided in Section 3.3.5.1

3.4 Change management

While the provision of adequate infrastructure and suitable equipment are prerequisites for the successful implementation of telehealth using VC, the provision of such equipment is not sufficient to ensure that telehealth will be successfully adopted within routine clinical practice. Beyond the technical aspects, the successful implementation of a telehealth service is primarily about effective change management⁶⁹ and involves integrating the technical aspects of telehealth within the social and organizational aspects of the workplace. Change management strategies that have been shown to be effective in easing the transition are outlined in Table 5.

Table 4: Change management strategies to overcome barriers to implementing telehealth using video conferencing

Issues	Change Management Strategy
<p>Professionals' concerns regarding the cost of implementing the infrastructure and operating systems.</p>	<ul style="list-style-type: none"> • Adequate reimbursement must be provided.
<p>Reluctance of professionals to invest the required time and effort to change existing work practices and routines.</p> <p>Professionals attitudes towards technology</p> <ul style="list-style-type: none"> • fear of technology; • concerns regarding the adoption of telemedicine systems into existing organisational systems • concerns that telehealth might undermine the psychosocial aspects of the consultation • concerns that telehealth might not be as effective as face-to-face consultations or might introduce additional risks to the patient. 	<ul style="list-style-type: none"> • Collaborate with users throughout every stage of the project to engender <u>ownership</u>' at the local level to enhance the likelihood of success. • Identify and engage <u>champions</u>' who will promote telehealth. • Collaborate with all users involved to ensure the technology suits the requirements of the work place. • Respect established referral practices. • Clearly communicate with potential users and address all users' concerns (e.g. regarding patient confidentiality). • Develop a marketing strategy to promote the benefits of using the equipment. Clearly articulate the benefits and advantages of using the system (what problem will the telemedicine system address?). • Provide evidence that telemedicine is effective and safe. • Ensure adequate technical support is readily available. • Provide adequate training in the use of the equipment, particularly at the outset. • Provide ongoing training (e.g. in the case of system or staff changes). • Ensure there are sufficient opportunities to use the equipment in order for users to become comfortable and competent in using it. • Integrate the service within existing work practices so that telehealth becomes a routine part of service delivery (e.g. ensure the equipment is conveniently located). • Ensure the equipment and processes (e.g. booking a videoconference) are easy to use and user-friendly. • Develop comprehensive protocols for conducting VCs. • Clearly define the roles and responsibilities of telehealth users.

3.5 Initial costing

The establishment costs of a new generation of telehealth services in Australia cannot be explicitly provided due to the extreme variability of clinical telehealth applications, the equipment (hardware, software, PC, room-based) and the mechanism employed for the delivery and coordination of telehealth services. On a small scale, the costs of doing telehealth may seem high compared to large scale (high activity) applications where economies of scale can be achieved.

As already emphasised in this report, there is substantial work to be done to develop a service from demonstration (proof of concept) to mainstream routine operations.

The following costs are based on information provided by two Queensland Audiovisual companies* and do not include potential volume discounts negotiable through individual vendors.

Equipment

Component description	Estimated unit cost (AUD)
Dedicated telehealth room with commercial videoconference system (including equipping with suitable soundproofing and lighting)	\$60,000
Office-based, desktop videoconference system	\$15,000
Standards-based, PC software	\$250 (per single licence, per annum)
Non-standards based, PC software (eg. Vidyo): commercial	Unable to ascertain
Non-standards based, PC software (eg. Skype, MSN Messenger): freely available	Nil
Skype4Health, software (web based portal)	Currently not available (investment in development required)

*Sources: i-Vision - <http://www.ivation.com.au/>

Advanced Video Integration - <http://www.advancedvideo.com.au/>

Telecommunications

Component description	Estimated unit cost per annum (\$AUD)
DSL (symmetric business grade)*	\$2,400

*Costed at 500kbit/s symmetric BDSL with a low contention rate

Funding models should take into account two stages of development – establishment (short-term) and maintenance (long-term). Establishment costs may be relatively higher due to the initial costs of service planning, marketing and communications, equipment procurement, installation of telecommunications, staff training and coordination. In comparison, the maintenance costs – such as coordination, telecommunications, software licence agreements, equipment depreciation costs, training etc. may be expected to be slightly lower.

SECTION 4 RECOMMENDATIONS

In this section a series of high level –Strategic Recommendations” are presented. These recommendations draw on research findings and interpretations detailed in preceding sections of this report. Many of these recommendations are based on data drawn from multiple sections of this report, and were thus difficult to embed within a particular section.

Those recommendations that can be related to specific technical sections of the report are entitled –Technical recommendations” and are embedded in the relevant section. A full list of these recommendations, without any supporting text, is provided at the conclusion of this section for completeness.

4.1 Strategic recommendations

Each recommendation is preceded by some explanatory text. However, for a full account of the evidence from which the recommendation is derived, reference to the preceding sections of the report may be required.

To establish a working VC system, several important elements are required, including evidence of safety and reliability, definition of standards, availability of suitable equipment and software, installation, reimbursement, scheduling, training and marketing. While some of these aspects are now in place in Australia, many require development. Therefore the full potential of VC will evolve over time. Initial implementations should focus on interactions which are well researched, and which are currently successfully operating in Australia or internationally.

SR1 *Video-consultation should be phased in over several years, with a primary focus, in the first instance, on Patient-GP-Specialist interactions, reflecting well established telehealth practice.*

In home VC has great potential, particularly for persons who have difficulty in travelling to a health professional. Medical consultation with persons at home, who are unaccompanied by another health professional, may require high quality VC to ensure diagnostic certainty and ability to administer complex medical interventions until demonstrations indicate otherwise. Such VC is currently not available at sufficiently low cost to permit widespread home

consultation. However, this situation is likely to change in the next few years, perhaps dramatically, as PC based systems, linked to the NBN, evolve.

SR2 *Home based VC could be considered in some scenarios as suitable systems become available, and after demonstrations have shown good levels of acceptability, reliability, security, safety and affordability.*

The majority of existing clinical VC services use dedicated VC hardware with diagnostic quality images and sound, at both the clinician and patient endpoints. The research evidence which pertains to safety, reliability and acceptability relates to this configuration of equipment. Alternative configurations of equipment may be suitable for VC, provided that a suitably qualified health professional (usually a GP) accompanies the patient, to assist in examination, interpretation and explanation.

SR3 *In the short-term, clinical consultations involving complex diagnostic and management decisions, where the patient is not accompanied by another health professional, may have to be limited until standards-based VC equipment is available for use at the patient endpoint. PC based equipment may be suitable at the health professional endpoint.*

SR4 *PC based equipment may be appropriate at the patient endpoint when there is another health professional accompanying the patient, who can assist in diagnostic and management decisions.*

SR5 *In hospitals and residential aged care facilities, where there is a high probability of diagnostic uncertainty and where complex medical decisions may be required, dedicated VC equipment should be utilised at the patient endpoint. PC based equipment may be suitable at the health professional endpoint.*

When a patient interacts with a health professional, several important processes may occur. A booking is required, a record must be assembled or retrieved, the patient must be correctly identified, a billing procedure may be involved, a suitable room and equipment for VC is required, and a health professional should be available should any ancillary procedures or advice be needed.

SR6 *Until demonstrations indicate otherwise and for the purpose of claiming MBS items for online consultations, VC at the patient endpoint should primarily occur in a health setting where conventional clinical consultations occur, to ensure authentication of the patient, and to provide technical and clinical assistance when required. This includes GP surgeries, community health centres, hospital outpatient clinics, hospital wards and residential aged care facilities.*

The majority of Australian doctors have no experience of clinical VC however, many may have domestic level experience of PC based VC. There are important clinical implications to be considered when conducting clinical VC. There is a growing body of research around the advantages and limitations of VC, which varies depending on the nature of the consultation and the problems which are being addressed.

SR7 *Colleges and other professional bodies should consider developing guidelines for the safe and effective use of VC by their members.*

The majority of video-consultations require a similar time period as conventional face to face consultations. The clinical history (or conversation) is similar in duration, the clinical examination, if required, will be shorter, but time taken to assemble ancillary information may be longer. Regardless, there is a relationship between duration of consultation and cost, as the majority of cost is related to the health professional's time.

In the special circumstance where the patient is accompanied by a GP in a consultation with a specialist, there will be a need to provide appropriate payment to the GP as well as the specialist. The GP cost will also relate closely to time. However, the GP may not need to be present for the entire consultation, in which case the duration of the consultation for the GP will not necessarily match that of the specialist.

The current Medical Benefits Schedule provides a wide array of Items to support GP and specialist consultation, the majority of which are time based. The Schedule includes Items where specialists and GPs are both present at a consultation. The current schedule already includes an Item for doctors to participate in case conferences by VC.

SR8 *Funding for VC could be on the same basis as equivalent face to face consultations listed in the Medical Benefits Schedule.*

The cost on conventional clinical consultation includes the health practitioner's time, support staff, consulting rooms and office space, equipment and consumables. Economies of scale, including group practice, serve to attenuate the cost of all elements other than the health professional's time.

VC is associated with special costs, primarily pertaining to the need for special equipment (VC) and space (studio for VC), and scheduling of the appointment with a 3rd party at a different location. In the short-term, VC use in most practices is likely to be sporadic, and thus economies of scale will not be achieved. This will result in additional costs when compared to conventional consultations.

SR9 *Payments to compensate for the higher cost of VC and to encourage the use of VC could be introduced. This could include a loading to each consultation referred to in Recommendation SR8.*

The persons most disadvantaged, in terms of access, in the current health system include those living in rural communities and those with significant disability that interferes with the ability to travel. In order to attenuate this disadvantage, it would seem appropriate to encourage the use of VC in these patient groups.

SR10 *Additional incentive payments might be offered to GPs operating in rural settings to encourage their participation. In metropolitan areas, similar incentive payments could be offered when the consultation involves a person living in a rural setting or a person with significant disability. The latter group should include persons living in Residential Aged Care Facilities.*

In addition to the legal requirements there are high expectations of privacy and security in healthcare. Telehealth introduces a new dimension – where health information is transmitted and stored. Therefore additional measures of protection are needed.

SR11 *Telehealth service providers should periodically review and update their privacy practices, policies and notices to ensure that they adequately address the management of information gathered during telehealth consultations..*

As stated earlier in this section, and repeatedly within this report, implementation of a telehealth system is complex. A key consideration is the need to adapt practice patterns and supporting systems. To optimise the rate of take-up, a change management strategy should be developed and implemented.

SR12 *A successful telehealth implementation will require an active change management strategy. This would entail consultation with clinicians, the development of guidelines and marketing of the initiative.*

4.2 Governance arrangements

Six recommendations governance arrangement recommendations arose from Section 4.5.4:

GAR1 *To establish an effective telehealth service, suitably qualified individuals should be recruited to form a project management team which should be led by an experienced senior project manager.*

and

GAR2 *A high-level steering group should be established to provide oversight and advice during the implementation phase. This group should comprise representatives of stakeholder groups (executive, clinicians, and individuals with practical clinical telehealth and technology expertise).*

GAR3 *It is recommended that Divisions of General Practice, peak representative bodies and the professional colleges provide security and privacy advice to their members.*

GAR4 *The choice of hardware and software for teleconsultation should be the responsibility of the individual health care provider subject to GAR5.*

GAR5 *Where a provider intends to use telehealth for diagnostic or complex management consultations, in circumstances where patients are unaccompanied by a health*

provider (~~un~~accompanied patient”), then products which have been demonstrated to be safe and effective should be used.

GAR6 *Metrics for continuous review of the telehealth implementation should be developed*

4.3 Performance and monitoring recommendations

Three recommendations relating to performance and monitoring arose from Section 4.6:

PMR1 Recommended key metrics that may be useful to this process include:

4.3.1.1.1 *1. Clinician take-up per period*

Analysed by:

- Overall
- By clinician
- By clinician subgroup, i.e. by GP and specialists
- By practice
- By specialty
- Geographic

2. Video consultation activity per period

Number of MBS telehealth claims per period

Analysed by:

- Overall
- By item number (in particular diagnostic/complex management vs. general)
- By clinician
- By clinician subgroup
- By practice
- By speciality
- Geographic

3. User satisfaction

Analysed by:

- Clinician subgroup
- Patients

(f) Funds committed

Analysed by:

- Equipment and software costs
- MBS claims
- Clinician support
- Governance and administration
- Marketing
- Education and training

(g) An estimate of cost per consultation

PMR2 *It is recommended that a group, with appropriate membership, be established to estimate take-up and thus identify appropriate performance thresholds for each key performance metric.*

PMR3 *It is recommended that expert assistance is sought to provide input to the development of the evaluation of video consultation implementation.*

4.4 Security and privacy recommendations

Twenty one recommendations relating to security and privacy arose from Section 3.1:

SPR1 *To ensure public trust in a teleconsultation, privacy protection and security mechanisms must be integral to any implementation.*

- SPR2** *Telehealth services should be compliant with all relevant state and federal laws.*
- SPR3** *Telehealth service providers should periodically review and update their privacy policies to ensure that they adequately address the management of information gathered during telehealth consultations.*
- SPR3A** *Telehealth service providers should periodically review and update their privacy notices to ensure that they adequately address the management of information gathered during telehealth consultations.*
- SPR4** *Telehealth service providers should periodically review and update their practices and procedures for managing personal information, including data security measures.*
- SPR5** *Protocols used to secure telehealth consultations should be non-proprietary, standards-based to foster interoperability, inspectability and trust.*
- SPR6** *Telehealth services, whether discrete practitioners or service providers should use a valid Public Key Infrastructure (PKI) certificate.*
- SPR7** *The PKI certificate should be signed a Certification Authority who maintains a Certificate Revocation List (CRL).*
- SPR8** *The PKI certificate should use a minimum key strength e.g. 2048-bit encryption. As computing power increases then the level of encryption may need to be increased.*
- SPR9** *PKI certificates should be stored in a physically or technically secured environment.*
- SPR10** *All teleconsultation data (including ancillary data) must be secured for transmission across a data network either by use of encryption or VPN technology.*
- SPR11** *All web services used in teleconsultations — including web-based video conferencing, patient records, messaging systems must be secured by a minimum Transport Layer Security Version 1.2.*

SPR12 *All emails containing patient data must be secured. This should be at a minimum by S/MIME Version 3.0 or later and/or the latest technical specifications published by Standards Australia for E-Health Secure Message Delivery.*

SPR13 *Hardware based videoconferencing units must support H.235 allowing encrypted communication between end points in both point-to-point and multi-point videoconferencing sessions.*

SPR14 *The National Authentication Service (NASH) or a similar service could be considered for telehealth service providers and telehealth applications when operational.*

SPR15 *In the future infrastructure could be developed and implemented to provide the following solutions for telehealth service providers and telehealth application vendors:*

- *Credential user base of telehealth clinicians;*
- *Encrypted authentication services for patients who will participate in clinician-to-patient telehealth services; and*
- *Access control to limit teleconsultations to eligible clients and credentialed clinicians via links to health identifiers.*

SPR16 *All telehealth applications must enforce strong passwords.*

SPR17 *All telehealth applications support two-stage authentication.*

SPR18 *All telehealth applications record an audit trail of user's access to patient information.*

SPR19 *Policy guidelines for the retention and storage of telehealth records could be developed to assist those telehealth service providers which are not subject to specific legislative requirements for the retention and maintenance of health records.*

SPR20 *If storage is required, telehealth data (ancillary data and clinically determined recorded videoconference session) should be stored in a physically secure environment. The management (sanitisation, destruction and disposal) of media*

on which telehealth data is stored should be performed according to legislative obligations and sound technological practice. Secure storage is the responsibility of the telehealth service (including discrete practices, practitioners and service providers).

SPR21 *If telehealth data is stored on a portable device it should be encrypted using a commercial data encryption application.*

4.5 Interoperability and integration recommendations

Six recommendations relating to interoperability and integration arose from Section 3.2:

IIR1 *To promote interoperability, where standards-based products are proposed, features that are provided by proprietary or pre-standard extensions should be avoided.*

IIR2 *In the short-term, to communicate with endpoints on established networks, any new video consultation implementation should:*

- *Be either standards-based, or if proprietary, provide a mechanism to allow audio and video sessions between the proprietary and standards-compliant endpoints;*
- *Support a minimal subset of the following standards: H.225; H.245; H.261 QCIF, H.263, Q.931; RTP; G.711; G.722; G.728; G.723; G.729; TCP/IP;*
- *Manufacturers should demonstrate interoperability using the stated minimum subset in a heterogeneous environment.*

IIR3 *While it is not possible to foresee detailed interoperability issues of the medium and long-term future, new products, however delivered, should be tested for interoperability using the contemporary technical standards of the day.*

IIR4 *In the short-term, tight integration with clinical systems is not achievable. In the medium to long-term there will be benefits of integration however not enough is currently known. Experience gained from early adopters could be used to inform future requirements.*

IIR5 *In the short-term, there is insufficient time, or perceived benefit, to recommend the development of a telehealth scheduling and co-ordination system. Early experience could inform the necessity of and requirements for such a system.*

IR6 *Tight integration of video capabilities with other practice systems should be deferred to (i) allow converged applications to develop maturity and (ii) gain practical experience of video consultation in the primary care setting. Such experience will inform the need, degree and benefits of integration. Convergence will provide the opportunity to do so.*

4.6 Hardware, software and support recommendations

Eight recommendations relating to hardware, software and support arose from Section 3.3:

HSSR1 *MBS reimbursement will be in-place before there is an implemented electronic means for authentication. Therefore in the short-term, or until demonstrations show otherwise, it is recommended that consultations take place only to/from the premises of a recognised health provider, where an individual is known or can be reliably identified..*

HSSR2 *A national provider registry that includes healthcare provider capacity to engage in telehealth sessions will be important for the future operation of telehealth.*

HSSR3 *To achieve economies of scale, and to avoid disadvantaging small or remote practices, it is recommended that some form of aggregated support arrangement is put in place. This may take the form of a nationally, regionally or locally negotiated contract with accredited suppliers for service establishment and for ongoing support.*

HSSR4 *For the convenience of medical practices, it is recommended that access to telehealth helpdesk services be considered for support calls, management of problem resolution and to escalate issues with support providers as necessary.*

HSSR5 *It is recommended that any contract with external support organisations ensures that sufficient expertise and equipment will be available to respond to problems, and to rectify problems, within a specified period of time. Response time should be fixed (eg. 4 hours from time of first call). Geography can preclude a fixed rectification time and hence such times would need to be negotiated based on the location of the equipment and distance to the nearest technical support.*

HSSR6 *Given the short lead time and concerns expressed during the stakeholder consultation process, it is recommended that an engagement, education and communications process commences as a priority.*

HSSR7 *Practicing by telehealth is different to in-person practice. Clinical guidelines for consultation by video will need to be developed prior to the implementation of MBS item numbers.*

HSSR8 *It is recommended that any promotional activities directed to health consumers is carefully considered, both in terms of timing and content, prior to and following the introduction of video consultation.*

4.7 Technical Recommendations

Fourteen technical recommendations arose from Section 3.3.6:

TRR1 *Where software-based products are proposed, careful consideration should be given to match the product requirements against PC specifications.*

For diagnostic or complex clinical management (*diagnostic quality VC*), using hardware-based video conferencing, the following five recommendations relating to video cameras (TRR2 to TRR6, supported on all commonly available equipment) are made:

TRR2 *Image sensor: minimum ¼ type CCD image sensor*

TRR3 *Horizontal resolution: 460 lines (PAL)*

TRR4 *Focus: autofocus*

TRR5 *Optical zoom ratio: minimum 10x*

TRR6 *Standards-based far-end control of pan/tilt/zoom*

For non-diagnostic and non-complex clinical management (*general quality VC*), TRR2 to TRR6 also apply for hardware-based products. For software-based products (i.e. which use a webcam for video input) then the following three recommendations (TRR7 to TRR9) are made:

- TRR7** *Image sensor: CMOS or CCD type*
- TRR8** *Minimum resolution: VGA (640x480)*
- TRR9** *Frame rate: 30 FPS (at VGA resolution)*
- TRR10** *Choice of display should be made pragmatically depending on the circumstances. Contemporary display monitors are adequate for video conferencing.*
- TRR11** *A frame rate of 25 FPS is adequate for primary care video consultations*
- TRR12** *For diagnostic or complex clinical management, using hardware-based SD VC, a minimum throughput of 384kbit/s should be available*
- TRR13** *For video consultations, to avoid poor performance, round-trip latency must be lower than 300ms*
- TRR14** *For video consultations, to avoid poor performance, packet loss should be less than 0.1%*
- TRR15** *For clinical consultations, to avoid poor intelligibility, audio should be encoded at a minimum of 16kbit/s*

4.8 Technical Option Recommendations

Five technical option recommendations arose from Section 3.3.7

In the short term:

- TOR1** *Where a patient is unattended by a local physician, then it is recommended that, at the patient end, Option 1, is a minimum requirement for diagnostic or complex management decisions.*
- TOR2** *Where a patient is attended by a local physician, then Option 2, at the patient end (and Option 1 or Option 2 at the specialist end) is acceptable for follow-up consultations.*

TOR3 *Proprietary software video systems (Option 3) whether client-based or clientless, should be used only where requirements of privacy and security have been fully addressed and that a specific product or approach has been formally demonstrated as being safe and effective in clinical use. Such products will require individual assessment.*

In the medium to long term:

The medium to long term will see the deployment of the NBN and hence the provision of a pervasive high-quality broadband network. Experience will also have been gained with the short-term deployment of telehealth.

TOR4 *It is recommended that a dedicated application, or a personal health portal, which satisfies the functional and non-functional requirements identified earlier in the report be developed. This, with the promised capabilities of the NBN may facilitate mass deployment of video consultation.*

The use of software based VC in the short-term:

TOR5 *It is recommended that commercial off the shelf, standards compliant software (ie. Option 2) is used in circumstances where a software, rather than a hardware, approach to VC is used.*

The medium to long term recommendation for software video consultation was provided in Section 3.3.7.1

APPENDIX 1 BANDWIDTH REQUIREMENTS - PUBLISHED STUDIES

Application	Bandwidth Recommendation	Source
Tele-ultrasound	–The quality of dynamic ultrasound images transmitted at 384 kbit/s was diagnostically acceptable, but was unsatisfactory at 128 kbit/s.”	<p>The diagnostic acceptability of low bandwidth transmission for tele-ultrasound</p> <p>John A Brebner, Hugh Ruddick-Bracken, Eileen M Brebner, A Patricia M Smith, Karen A Duncan, Andrew J McLeod, Suzanne McClelland, Fiona J Gilbert, Angus Thompson, J Ross MacLean and Lewis D Ritchie</p> <p>http://jtt.rsmjournals.com/cgi/reprint/6/6/335</p>
Fetal tele-ultrasound	–Further testing with foetuses affected by various anomalies confirmed that the majority could be diagnosed using a 384kbit/s link, with slight improvement in evaluation when the bandwidth was increased to 1Mbit/s.”	<p>Minimum requirements for remote realtime fetal tele-ultrasound consultation</p> <p>F Y Chan, J Whitehall, L Hayes, A Taylor, B Soong, K Lessing, R Cincotta, D Cooper, M Stone, A Lee-Tannock, S Baker, M Smith, E Green and R Whiting</p> <p>http://jtt.rsmjournals.com/cgi/reprint/5/3/171</p>

Fetal tele-ultrasound	-Over 95% of these consultations were completed with six ISDN channels (384 kbit/s) and the clinicians were satisfied with the image quality in the majority of cases.”	<p>Randomized comparison of the quality of realtime foetal ultrasound images transmitted by ISDN and by IP videoconferencing</p> <p>F Y Chan, A Taylor, B Soong, B Martin, J Clark, P Timothy, A Lee-Tannock, L Begg, R Cincotta and R Wootton</p> <p>http://www.jtt.rsmjournals.com/cgi/reprint/8/2/91</p>
Fetal tele-ultrasound and foetal tele-therapy	-The transmission bandwidth was 384 kbit/s in the majority of the consultations.	<p>Fetal tele-ultrasound and tele-therapy</p> <p>Fung Yee Chan</p> <p>http://jtt.rsmjournals.com/cgi/content/abstract/13/4/167</p>
Neonatal echocardiology	For ISDN: 128kbps/256kbps sometimes satisfactory, 384kbps required to maximise image quality	<p>Assessment of the quality of neonatal echocardiographic images transmitted by ISDN telephone lines</p> <p>A Houston, K McLeod, T Richens, et al.</p> <p>http://heart.bmj.com/content/82/2/222.full.pdf</p>

<p>Paediatric echocardiograms</p>	<p>“512 kbps was the minimum for consistently clear imaging of all cardiac structures examined.”</p>	<p>The effect of bandwidth on the quality of transmitted paediatric echocardiograms John P Finley, Robert Justo, MD, Maria Loane, MSc, Richard Wootton, DSc http://www.onlinejase.com/article/S0894-7317%2803%2901086-1/abstract</p>
<p>Paediatric echocardiograms</p>	<p>“Three or more ISDN lines are necessary to ensure minimum Degradation of the live image.”</p>	<p>Accuracy of paediatric echocardiographic transmission via telemedicine Mark Lewin, Cathy Xu, Mary Jordan, Heidi Borchers, Catherine Ayton, Dennis Wilbert and Sanford Melzer http://www.jtt.rsmjournals.com/cgi/content/abstract/12/8/416</p>
<p>Paediatric telecardiology</p>	<p>“In our paediatric telecardiology program, we utilize dial-up live videoconferencing over three bonded ISDN lines (384 Kbps).”</p>	<p>Telecardiology: potential impact on acute care. Sable C. http://www.ncbi.nlm.nih.gov/pubmed/11496038</p>

<p>Speech therapy</p>	<p>...planned and conducted the sessions over the INTEGRIS video network using 384kbps on a dedicated T-1 line” ... -Satisfaction was high with parents and school administrators, despite technical difficulties.”</p>	<p>Two Year Results of a Pilot Study Delivering Speech Therapy to Children in a Rural Oklahoma School via Telemedicine C. Scheideman-Miller, P. Clark, S. Smeltzer, J. Carpenter, B. Hodge, D. Proutry http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2002.994136</p>
<p>Tele-oncology</p>	<p>-All tele-oncology sites in the Kansas Telemedicine Project ... are linked by leased lines normally running at 384kbit/s.”</p>	<p>Practising oncology via telemedicine Gary C Doolittle and Ace Allen http://jtt.rsmjournals.com/cgi/reprint/3/2/63</p>
<p>Mental health (schizophrenia)</p>	<p>-Zarate et al (1997) compared the reliability and acceptability of a telemedicine system using ISDN at 128 kbit/s and 384 kbit/s for patients with schizophrenia and found that the lower transmission rate could be used reliably for administering psychiatric rating and screening scales.”</p>	<p>Applicability of telemedicine for assessing patients with schizophrenia: acceptance and reliability. Zarate CA Jr, Weinstock L, Cukor P, Morabito C, Leahy L, Burns C, Baer L. http://www.ncbi.nlm.nih.gov/pubmed/%209055833 quoted by: Telemedicine and telecare: what can it offer mental health services? Paul McLaren http://apt.rcpsych.org/cgi/reprint/9/1/54</p>

<p>Mental health (obsessive compulsive disorder)</p>	<p>-At Harvard, USA, Baer et al (1995) demonstrated the reliability and acceptability of telemedicine, using an ISDN bandwidth of 128 kbit/s, for patients with obsessive-compulsive disorder. They found near perfect reliability (intraclass correlation of 0.99) for both video and in-person agreement on the Yale-Brown Obsessive Compulsive Scale.”</p>	<p>Pilot studies of telemedicine for patients with obsessive-compulsive disorder. Baer L, Cukor P, Jenike MA, Leahy L, O’Laughlen J, Coyle JT. http://www.ncbi.nlm.nih.gov/pubmed/7653700 quoted by Telemedicine and telecare: what can it offer mental health services? Paul McLaren http://apt.rcpsych.org/cgi/reprint/9/1/54</p>
<p>Teledialysis</p>	<p>-In South Australia, the regional dialysis unit in Adelaide has carried out several thousand consultations using low-bandwidth video links (128 kbit/s).”</p>	<p>Realtime telemedicine Richard Wootton http://www.jtt.rsmjournals.com/cgi/content/abstract/12/7/328</p>
<p>Teledialysis</p>	<p>-A bandwidth of 768 kbit/s was required for satisfactory teledialysis.”</p>	<p>Telemedicine in haemodialysis: a university department and two remote satellites linked together as one common workplace Markus Rumpsfeld, Eli Arild, Jan Norum and Elin Breivik http://jtt.rsmjournals.com/cgi/content/abstract/11/5/251</p>

Medical imaging	-The system can transfer medical images (e.g. X-ray images, CT scans and ultrasonograms) with no distortion. It has been successfully demonstrated for a teleconsultation between Shanghai and Beijing via a 128 kbit/s line”	<p>A review of telemedicine in China</p> <p>Zhelong Wang and Hong Gu</p> <p>http://jtt.rsmjournals.com/cgi/content/abstract/15/1/23</p>
Radiotherapy	-Both radiation oncologists concluded that videoconferencing at a bandwidth of 512 kbit/s was sufficient for remote guidance.” ... -We employed a bandwidth of 384 kbit/s. This was sufficient when the patient was moved slowly during imaging.”	<p>Telemedicine in radiotherapy: a study exploring remote treatment planning, supervision and economics</p> <p>Jan Norum, Øyvind S Bruland, Oddvar Spanne, Trine Bergmo, Tor Green, Dag R Olsen, Jan H Olsen, Elisabeth E Sjøeng and Tatiana Burkow</p> <p>http://jtt.rsmjournals.com/cgi/content/abstract/11/5/245</p>
Audiology/ general	-For videoconferencing, a 384 kbit/s connection is desirable as a lower bandwidth will result in a poor quality interaction between the parties.”	<p>Audiology telemedicine</p> <p>Mark Krumm</p> <p>http://jtt.rsmjournals.com/cgi/content/abstract/13/5/224</p>

Telegenetics	The videoconferencing equipment was connected at a bandwidth of 384 kbit/s, using three ISDN lines." ... No new diagnoses were made face-to-face that had not been identified by telemedicine. No diagnoses made by telemedicine were judged to be wrong when the child was evaluated face-to-face."	Telegenetic medicine: improved access to services in an underserved area H J Stalker, R Wilson, H McCune, J Gonzalez, M Moffett and R T Zori http://jtt.rsmjournals.com/cgi/content/abstract/12/4/182
--------------	--	---