

The Department of General Practice

In affiliation with the:
Department of Rural Health, The University of Melbourne
Monash Division of General Practice

The GPCG Computer Security Project

Final report

February 2004

Authors

A/Prof Peter Schattner
Monash University
Department of General Practice
Monash University
867 Centre Rd
East Bentleigh Vic 3165
Phone 03 8575 2222
Phone 03 8575 2232
Email: peter.schattner@med.monash.edu.au

Catherine Pleteshner
University of Melbourne
Department of Rural Health
Parkville Campus location:
c/o Department of General Practice
200 Berkeley Street
Carlton Vic 3052
Phone 03 83443373
Email: c.pleteshner@unimelb.edu.au

Contents

1.	INTRODUCTION	7
2.	AIMS AND OBJECTIVES OF THE GPCG SECURITY PROJECT	7
3.	METHODS	8
3.1	LITERATURE REVIEW	8
3.2	INFORMATION FROM DIVISION SURVEYS	8
3.3	QUANTITATIVE RISK ASSESSMENT	9
3.4	KEY INFORMANT INTERVIEWS	9
3.4.1	<i>Aim of the interviews</i>	9
3.4.2	<i>Objectives</i>	9
3.4.3	<i>Semi-structured interview schedule</i>	10
3.4.4	<i>Sampling</i>	10
3.4.5	<i>Interview method – theory</i>	11
3.4.6	<i>Interview method – practice</i>	11
3.4.7	<i>Data analysis</i>	12
3.5	DEVELOPMENT OF THE SECURITY GUIDELINE AND IMPLEMENTATION STRATEGIES	12
4.	RESULTS	12
4.1	LITERATURE REVIEW (INCLUDING DIVISION SURVEY REPORTS)	12
4.1.1	<i>Literature search results</i>	12
4.1.2	<i>Summary of the literature</i>	13
4.1.3	<i>Australian surveys on data security</i>	16
4.2	QUANTITATIVE RISK ASSESSMENT	24
4.3	KEY INFORMANT INTERVIEWS: THE RISK ASSESSMENT	24

4.3.1	<i>Background</i>	24
4.3.2	<i>The Context of Computer Security In General Practice</i>	26
4.3.3	<i>The most important IT Security issue facing general practice at present</i>	26
4.3.4	<i>The lay of the land: what is to be changed?</i>	27
4.3.5	<i>General Practice IT Security Risks: through an organizational change management framework</i>	28
4.3.6	<i>General Practice IT Security Risks: from a practice-based Information and Communication Technologies (ICT) infrastructure management perspective</i>	31
4.3.7	<i>Evaluating security risks in general practice: setting the priorities</i>	37
4.3.8	<i>Other risks</i>	38
4.3.9	<i>Managing security risks in general practice: identifying 'cost effective' strategies and solutions</i>	41
4.3.10	<i>Managing technical risks</i>	53
5.	SECURITY GUIDELINE AND CHECK-LIST	68
6.	IMPLEMENTATION STRATEGIES	68
6.1	INTRODUCTION	68
6.2	COMMONWEALTH GOVERNMENT STRATEGIES	69
6.3	GPCG STRATEGIES	70
6.4	OTHER KEY PROFESSIONAL ORGANISATIONS	70
6.5	PUBLICITY THROUGH THE MEDIA	72
6.6	CONCLUSIONS ON AN IMPLEMENTATION FRAMEWORK	74
7.	PROJECT OUTCOMES	75
8.	REFERENCES	76
9.	APPENDIX	79
9.1	KEY INFORMANT SEMI-STRUCTURED INTERVIEW SCHEDULE (SHORT VERSION)	79
9.2	ACRONYMS AND DEFINITION OF TERMS	87
9.3	THE GPCG COMPUTER SECURITY CHECK-LIST	89

Table of Figures

Figure 1:	Security practices before and after feedback	18
Figure 2:	Back-up procedures	19
Figure 3:	Other Security Practices	19
Figure 4:	Written policies for computer management incorporated into practice policy documentation	22

Table of Tables

Table 1:	Frequency of virus definition files update by computerized practices with virus protection software	21
Table 2:	Use of passwords for data security and privacy by computerized practices	21
Table 3:	Organisational framework: summary of experts' GP IT security risk analysis	29
Table 4:	Technical framework: summary of experts' GP IT security risk analysis	32
Table 5:	Experts' prioritization of IT security risks needing to be addressed	38
Table 6:	Experts' individual prioritisation of which IT Security risks in general practice should be addressed first	39
Table 7:	Managing the risk (IT policies in the practice): summary of experts' proposed strategies	42
Table 8:	Managing the risk (Practice IT Coordinator): summary of experts' proposed strategies	47
Table 9:	Managing the risk (Practice Disaster Plan): summary of experts' proposed strategies	49
Table 10:	Managing the risk (Email and Internet Policies): summary of experts' proposed strategies	52
Table 11:	Managing the risk (backups and restorations): summary of experts' proposed strategies	53
Table 12:	Managing the risk (screen savers): summary of experts' proposed strategies	55
Table 13:	Managing the risk (passwords): summary of experts' proposed strategies	56
Table 14:	Managing the risk (malicious code and firewalls): summary of experts' proposed strategies	58
Table 15:	Managing the risk (power surges): summary of experts' proposed strategies	59
Table 16:	Managing the risk (encryption of data transmission): summary of experts' proposed strategies	60

Table 17:	Managing other technical risk: summary of experts' proposed strategies	62
Table 18:	Strategy Summary	73

Acknowledgements

I wish to thank the Commonwealth Department of Health and Ageing, the General Practice Computing Group and its Privacy and Security Working Group, and the 'key informants' who were interviewed and who provided valuable insight into general practice computer security from their different perspectives.

I extend a personal thanks to Catherine Pleteshner for her highly significant role in this project, her engagement with numerous stakeholders, division people and many others, and especially for the key informant interviews and their write-up in this report.

I also wish to thank several other people who have assisted with this project. They include Dr Britt Klein and Prof Jeff Richards from Monash University, Ms Leslie Stanger and Dr Nathan Pinskier from the Monash Division, Ms Deanne Keetelar from the Medical Defence Association of Victoria, and Ms Elizabeth Deveny and Ms Jennifer Dunlop from the University of Melbourne.

There are quite a number of other people who have made significant contributions and some of these are referred to within this final report. I apologise if I have neglected to mention anyone by name.

Finally, this work has built on the solid achievements in general practice computing by the RACGP, the AMA, the GPCG and, in particular, the initial developmental work done by Frank Quinlan on the GPCG Interim IT Security Guidelines (2001) which provided a springboard for this work. My personal experience in this field was based on collaboration with Karen Young and Laurie Barrand from the Monash Division of General Practice.

Peter Schattner
Monash University
27 February 2004

1. Introduction

Information security has been defined as a process for ensuring confidentiality, integrity and accessibility of data. In the context of this consultancy, information security refers to electronic data, including clinical, demographic and financial information held in general practice.

Information security has demonstrated benefits in general practice for both patient health and the efficient running of the practice as a small business. However, there has been concern expressed by a number of people involved with GP informatics (e.g. from the Commonwealth government and divisional information technology (IT) officers, among others) that general practitioners (GPs) do not currently take adequate steps to ensure the security of their patients' data within general practice. Preliminary evidence from surveys conducted by divisions of general practice show that backing up data, using firewalls and maintaining up to date anti-viral software could be done with greater diligence.

Lack of attention to information security is unlikely to be limited to general practice – how many people perform adequate computer back-ups for their home systems? – but the consequences for patient health are potentially significant. This is an emerging area of concern, and the development of standards to help ensure patient rights is necessary in the light of the inexorable shift from paper-based to computer-based health records.

Advice on how to avoid computer viruses, do back-ups or use passwords is widely available. Why is it then that GP adoption of such practices and adherence to these guidelines seems to be less than optimal? In part, this might be due to a failure to appreciate the consequences of not taking preventive action. Many of us take risks such as skimping on house contents' insurance. However, when GPs take inadequate preventive action in relation to computer security, they may be basing their risk taking behaviour on uncertain notions of what needs to be done, how much it will cost, how much effort will be required by themselves and their staff, and what may happen if a threat to the security of patient data actually materialises.

To give GPs a more informed perspective on the relative risks associated with computer security, this project has conducted a risk assessment. This was considered integral to the process of prioritising what needs to be done to keep patient information as secure as possible.

In 2001, the General Practice Computing Group (GPCG) developed a set of computer security guidelines. However, guidelines such as these, in order to be of practical benefit, need to be disseminated and considered by individual practices (both GPs and staff). Moreover, an associated strategy, involving national, local and practice-based initiatives, also needs to be developed to facilitate their adoption in a more systematic way. The GPCG Security Project was designed to accomplish this task. However, the ultimate purpose for doing this promulgation work is to improve the overall standard by which patient electronic data is maintained in general practice.

One of the major 'products' of this GPCG project is a revised security guideline and check-list tailored for general practice. However, the challenge remains to ensure their implementation. Given that the majority of GPs have only recently adopted computers on their clinical desk-tops, the technical aspects of computer security might be seen as peripheral to clinical care. Moreover, the costs involved in obtaining ongoing IT technical support are at present not easy to offset in general practice. To compound the problem further, the practical assistance available from divisions is now also variable given the withdrawal of the specific Commonwealth mandate to provide IT support to general practice. This project has been a phase 1 (pre-implementation) undertaking; the GPCG will auspice the second phase in the near future.

2. Aims and objectives of the GPCG security project

The main aim of this project was to develop practical IT security guidelines for general practice. To help achieve this, the following project objectives were set:

- To identify security-relevant technical and organizational issues in general practice

- To identify minimum security standards
- To conduct an IT security risk assessment in general practice
- To develop a self-assessment security check-list and guideline
- To develop an IT security dissemination and implementation strategy

The GPCG Security Project did not set out to produce a technical manual. GPs wishing to ascertain which operating systems have less security holes, or the difference between various back-up media, will have to seek technical advice. Technical matters change fairly rapidly, and as soon as any such manual is produced, a new IT security recommendation is sure to present itself. This project set out to produce a practical guideline for the GP (and practice staff) of 'average' computer literacy, written with sufficient depth so that it explains fundamental standards for computer security, but not in so much detail that the vast majority of GPs cannot follow it

We appreciate that some GPs will complain that technical solutions for their computer systems will require expenditure on IT consultants, and that computer-based systems are more costly than paper-based ones. That may be so, but the increasing use of the Internet by clinicians, the gradual introduction of electronic health records and the increasing sophistication of decision-support software indicate that the need for computer security is only going to increase over time.

3. Methods

3.1 Literature review

A literature review was undertaken to investigate previous research done in the field of computer and patient data security in medical practice, and especially, in general practice. The following databases and search engines were used: Medline, ProQuest and Google. Various key words were tried, depending on the database. These included various combinations of: computer security, information security, general practice, information technology, computers, IT, training doctors, health informatics, and doctors and the Internet.

The first two databases (Medline and ProQuest) yielded a few research papers and many opinion pieces. Google led to a number of computer security guidelines, discussions about risk assessments, IT disaster plans and other papers, which, although not peer-reviewed, were quite informative.

Non-research literature was also reviewed. We thoroughly familiarised ourselves with the following Standards Australia articles: Information technology – code of practice for information security management (AS/NZS ISO 17799:2001); Risk management (AS/NZS 4360:1999); Information technology – guidelines for the management of IT security (AS 13335 [set]:2003); and Information security risk management guidelines (HB 231:2000); Information security management – implementation guide for the health sector (HB 174:2003).

3.2 Information from division surveys

In December 2003, all 123 divisions of general practice were emailed through both ADGP and GPCG online discussion lists with a request to advise us if they had conducted surveys on how GPs do (or do not) keep their electronic data secure. In January 2004, using the same channels, they were then asked if they had developed any generic proformas for any of the following: practice IT policies and procedures manuals, practice IT coordinator job descriptions, disaster recovery plans, and other policy documents such as staff use of email and the Internet.

By 20 January 2004, three divisions provided us with comprehensive survey information, although the response rates in these were under 50 percent of their GP membership. Several divisions and state-based IT officer networks had forwarded to us information based on practice visits and other forms of divisional contact with GPs. While, these represent useful anecdotal opinion, they do not constitute high level 'evidence' in research terms. We are not certain whether other divisions do not have survey data, but feedback from some of them indicates that since the end of specific Commonwealth IT funding for divisions, there has been no explicit request made for such data in divisional reporting (to the Commonwealth) requirements.

3.3 Quantitative risk assessment

Quantitative risk analysis is the process of establishing the actual consequences of a risk event in terms of time and money. For example, breakdown of a power supply in a four-year old server in a practice might be rated at a risk of 4 hours of disruption to the practice costing \$1000.

As most IT security risk assessments are qualitative in nature, that is, they rely on the opinions of those most directly involved, we considered it important to try to establish if anyone had conducted a quantitative risk assessment. We therefore made enquiries with organisations we thought might be relevant because of their involvement with software solutions or risk assessments, mainly in the private sector. Some were involved in general practice, others in hospitals and other health care providers, and some with the non-health commercial sector.

The following were approached: IBA Health; iSOFT Australia; Cerner Corporation; Trak Health; HCN (the largest supplier of clinical software to GPs in Australia); KPMG, PriceWaterhouseCoopers, Pitchers Partners, and Medical & Dental Accounting Consultancy, Betrusted (the organisation that issues PKI certificates on behalf of HeSA), the Australian Medical Association, the Medical Software Industry Association (MSIA) and the Medical Defence Association of Victoria (MDAV).

We asked them whether they either conducted quantitative risk assessments themselves, or knew of firms that did. Further, they were asked if they knew of any group that not only might do risk assessments for an individual practice or organisation, but also compiled data so that they could provide an industry-wide quantitative risk assessment.

3.4 Key informant interviews

3.4.1 Aim of the interviews

The risk assessment had, as its primary purpose, the collection of information to inform *priorities* for the project's GP security guideline and check-list.

3.4.2 Objectives

The objectives of the interviews were:

- to obtain risk data (i.e. conduct a risk assessment) on the likelihoods and consequences of threats occurring (including estimated losses in staff time and other costs)
- to obtain risk management information
- to obtain suggestions for the implementation of security guidelines in Australian general practice

3.4.3 Semi-structured interview schedule

An interview schedule was developed by reviewing the Standards Australia literature and the GPCG security guidelines (draft version 2001). The aim was to conduct a risk assessment by asking respondents to indicate on a scale what were the consequences and likelihoods in general practice of a series of IT risk categories. They were also asked about suggestions on how these risks could be best managed in general practice, and how the profession could ensure the best possible uptake by GPs of IT security guidelines.

3.4.4 Sampling

The sampling method adopted for this study was a hybrid of a stratified purposive one (Trost, 1986), where study participants have been selected from previously identified subgroups, and criterion sampling (Rice & Ezzy, 1995) whereby all study participants meet a set of selection criteria.

The key informants were chosen for their ability to represent the varying and currently relevant perspectives and organisational interests of a range of stakeholders, i.e. GPs in practice, consumers, practice managers, government, the medical computing industry, and so on. However, it is important to note that although a small number of informants were nominated, for the majority, their views were expressly their own and did not necessarily represent the interests of any particular organisation or representative group.

We developed a list of more than 20 key informants with whom interviews were to be conducted, but found that by the time 14 extensive and 6 other interviews had been conducted, that there was little, if any, new information forthcoming. We therefore decided not to proceed with interviewing the remaining people on the list.

The key informants were selected using at least one of the following criteria:

- a practicing GP who was not only an early adopter and current user of IT for both clinical and practice management purposes, but who also is highly regarded by peers for developing and implementing practice-based IT solutions in their own practice
- a practicing GP who has also been an advocate of 'informatics' and an office bearer in a relevant GP informatics 'linkages' organization (GPCG, AMA) for more than 5 years
- a practicing GP who has also been an advocate of 'informatics' and who has also been actively involved in a relevant general practice accreditation organization (AGPAL, AAPM) for more than 5 years
- a practicing GP who is also currently actively involved in developing GP and other Australian medical software industry (MSIA) solutions
- a consumer representative and advocate with a long-standing involvement in the consultation process associated with health informatics
- a nominated senior manager or office bearer currently responsible for the management and implementation of key Commonwealth health-related IT infrastructure systems (DoHA, HIC, HESA, *HealthConnect* and ADGP)
- a key informant authorized by the GPCG Security Project Working Group

The identities of the respondents have been kept confidential.

3.4.5 Interview method – theory

The risk analysis (refer to Section 4.3 of this report) is primarily based on data collected from interviews with key informants - experts in GP computing. Such interviewing, however, as a data collection strategy, is sometimes criticized, or seen to have limited generalisability. Rice and Ezzy (1999) respond to such criticism as follows: *'First [such a perspective] assumes that it is possible to avoid bias, perhaps through quantitative methods. However, a structured questionnaire does not eliminate this problem of bias, it just changes its form. Similarly, in-depth interview styles that attempt to be non-interventionist have an equally powerful 'biasing' influence on the interview narrative. Second, it assumes that the in-depth interviewer is not aware of this problem. However, the active interview method grows out of an attempt to constructively respond to the problem of subjectivity in interviews rather than to pretend it can be avoided.'*

The 'active interview' as a research method, provided an opportunity for the field officer to find out what the best questions and answers might be *with* the interview participants. As Holstein and Gubrium put it, *respondents [were] not so much [treated as] repositories of knowledge – treasures of information awaiting excavation – as they [were] constructors of knowledge in collaboration with the interviewer* (Holstein & Gubrium, 1995). Furthermore, the field officer also engaged the respondents with an insider-outsider approach, referred to in ethnographic research as the 'emic/etic distinction' (in Headland, Pike & Harris, 1990). Doing so, better enabled the field officer to work *with* the organisational cultural and other 'community of practice' assumptions of the respondents, in order to stimulate further reflection on their part; particularly in relation to how their suggestions for how to address the issue of IT Security in general practice fitted into the bigger picture along with the other influences therein. And finally, the field officer encouraged all experts participating in the study to 'ground' any evaluation of risk on their own experience and that of colleagues, rather than on postulated or hypothetical IT Security incidents.

3.4.6 Interview method – practice

Telephone interviews were scheduled with all participants in advance. Practicing GPs were reimbursed by the project to compensate for the interruption to their patient consultation time. All participants were notified in advance that they would receive (by email) a brief primer pre-interview document approximately half an hour prior to the commencement of the actual interview.

The purpose of the primer document was to provide background information related to the purpose of the interview (and thus the scope of the GPCG Security Project) as well as to focus the forthcoming detailed discussion around specific organizational and technical security risks, and their management. Participants were asked to identify other such risks that they considered were important, and that needed to be addressed, and that had not been included thus far. These additional risks were then systematically incorporated into the flow of the interview schedule.

In keeping with the project's timeframe, the research field officer (CP) conducted a series of telephone interviews in mid-December 2003. With the informed consent of all study participants, using the hands-free function on the telephone in the interviewer's office, the confidential interviews were digitally recorded. Field notes were also taken during the actual interviews.

The WAV files for all 14 comprehensive interviews (with each averaging around 50 minutes in length) were then downloaded from the digital recorder (Olympus) onto the desktop computer for reviewing. To enable individual members of the team to work in parallel [CP, PS and the project's research assistant (JD)], CDs containing the interview audio files were burnt on site at the Department of General Practice, University of Melbourne.

3.4.7 Data analysis

The views and illustrative direct quotes from each key informant were transcribed into the themes outlined in the original data capturing framework (refer to the Appendix for details of the design for the semi-structured interviews). The edited extracts were then compared with the handwritten notes taken by the field officer (CP) during the interviews to ensure consistency, and any omissions were noted. The edited transcripts were then transferred into the one Word document in preparation for systematic searching of the text using key words related to the themes and topics on which information was being sought.

The views of the key informants were summarised in a risk assessment 'matrix'. This included expert opinions on:

- the most important IT security issues facing general practice at present
- any additional organisational and technical risk categories to those already listed in the schedule
- their evaluation of the nominated risk (in terms of likelihood and magnitude of consequences *for the practice* (in relation to patient risk and cost to the business))
- their proposed solutions and strategies for managing these risks

As the interviews were structured, analysis was straightforward in that the themes had been arranged at the outset. A summary of the main ideas is presented in the results section.

3.5 ***Development of the security guideline and implementation strategies***

The content of the draft security guideline is based on the literature, the GPCG 2001 interim guidelines and interview data from key informants. The interviews provided important perspectives on the priorities in general practice and also were invaluable in developing an implementation strategy.

The format of the guideline was not based on precedent, although other guidelines were reviewed. It just seemed that a briefer, easy to read format would appeal more to GPs than a detailed tome. However, the guideline is still in its 'first cut' – hence its labelling as first edition - and may be modified once further feedback is obtained, especially from other GPs in the field.

4. Results

4.1 ***Literature review (including division survey reports)***

4.1.1 Literature search results

The peer-reviewed literature search was disappointing in that there were almost no studies of computer security in general practice. A few were based on overseas studies in nursing, specialist medicine or hospital settings, none of which necessarily apply to Australian general practice. The few surveys that have been published have used less than rigorous research methods.

The majority of the literature is of the review or commentary type. Some refer to the laws that pertain to privacy and confidentiality of patient clinical information and stress that medical practitioners have a legal as well as an ethical obligation to ensure that patient data remain secure.

4.1.2 Summary of the literature

4.1.2(a) Standards Australia

Six papers were reviewed. Topics covered were; a general overview of risk management (i.e. not specifically in IT); risk management as it pertains to information security; some of the more technical aspects of computer security; and guidelines for computer security. Many of the papers overlapped in content and only one was health industry-specific, albeit not for general practice. Nevertheless, these papers provided an excellent theoretical framework for this project's risk assessment. The guidelines for computer security were carefully reviewed and they were used to ensure that the GPCG Security Project's guideline addressed the important computer security issues. However, the Standards Australia guidelines were far too detailed to serve as a direct model for the GP guidelines.

4.1.2(b) GPCG interim security guidelines (2001)

The GPCG interim security guidelines (2001) provided the basis for the current version. These original guidelines identified the key security and privacy risks that GPs encounter when they work in an electronic environment. Risks to confidential patient information included: loss, theft or unauthorised access; data reaching the public domain (e.g., email sent to an incorrect recipient); misuse, abuse and loss of data integrity (e.g., administrative staff inappropriately updating patient clinical records); and the lack of availability of data (e.g., the network 'crashing' for one reason or another). In addition, the associated report also listed twelve IT security guidelines and described practical measures that could be taken to reduce the security risks involved. Given the importance of the original guidelines to the current version, the 2001 security categories, risks and practical measures to reduce the risks are worth reviewing briefly.

(i) Privacy of personal health information

This section referred to the need for GPs to be aware of current privacy laws, what confidentiality means and how to maintain privacy when communicating patient information (e.g., via email). Practices also need security and privacy policies for patient records.

(ii) Basic security and computer guidelines

The guidelines suggested a variety of basic precautions including the creation of an emergency repair disk, use of passwords, sensible positioning of terminals so that the public could not view confidential information, and logging out of the system when leaving the computer unattended. Other advice included obtaining basic security training, storing sensitive information on a network drive rather than on a stand-alone computer, and storing a minimum amount of data on laptops and palmtops as they carry a greater risk of theft or unauthorised access.

(iii) Backing up of practice data

There was a strong recommendation that all clinical and practice information be backed up regularly (i.e., daily), logged, verified and tested. The back-up should be scheduled when the computers are not in use to prevent any data integrity problems (i.e., when the practice is closed). Data back-ups should also be stored securely offsite (e.g., in case of a fire) and documented.

(iv) *Screen savers*

Screen savers with password protection should be set to activate at a minimum time of inactivity. There was no discussion about the *relative* importance of screensavers for data security, or how often data misuse had occurred without a practice having screensavers on their computers.

(v) *Passwords*

Fairly detailed advice about passwords was provided including the use of at least six characters, limiting the number of incorrect attempts (i.e., three to five) when trying to log on and using different passwords to access different systems. Users should create passwords that are difficult to guess (i.e., not related to one's job or personal life), change them on a regular basis (especially when using default passwords and privileged accounts), not share 'generic' passwords, and not write them down where others can gain access to them. As was the case for screensavers, there was no discussion on how significant a threat the lack of passwords had been in general practice, or whether it was likely that GPs would comply with this fairly complicated protocol for password use.

(vi) *Anti-virus measures*

The guidelines recommended the installation of anti-virus programs on all computer workstations and network servers, regularly checking computer files for viruses, checking all external sources of data before using them on the computer, regularly downloading virus updates and terminating computer use the moment a user suspects an infection.

(vii) *Accessing the Internet*

It was suggested that practices establish a staff Internet usage policy (i.e., acceptable uses of the Internet and email). Also, firewalls should be set up to secure the connection between the internal network and the Internet. In addition, it may be wise to limit the number of users who have access to the Internet or, alternatively, to use a proxy server in larger practices. Users should not publicly disclose patient and practice details via the Internet without permission and when files are downloaded from the Internet or purchased from an external provider, these sources of data need to be verified and scanned for viruses before being used. Confidential information sent over the Internet should be encrypted. Public Key Infrastructure (PKI) is an encryption system made available by the Health Insurance Commission; it is a secure method of transmitting information electronically by providing authentication and confidentiality.

(viii) *Communication by email*

Practices should develop policies for staff to protect confidential information sent or received by email. This might include the use of encryption and digital signatures, and scanning attachments for viruses. Work-related emails need to be stored and deleted in accordance with current legislation as most electronic correspondence is regarded as being part of the medical record. It was suggested that when sending emails the user must clearly state that their personal opinion is their own, and does not reflect the opinions of the practice.

(ix) *Access controls*

Practices need to develop and implement staff policies on 'access rights' to patient data. Approved people should use unique user-IDs and passwords for access, thereby holding personnel individually accountable for their own usage. This enables an audit trail which identifies a user's transactions.

(x) *Physical security*

This means the creation of appropriate levels of protection against unauthorised entry or damage to places where health information is physically stored. The recommended security measures included storing computer systems away from where they could be accessed by the public, ensuring building and environment security precautions are in place (e.g., theft alarms and smoke detectors), locking up medical records (e.g. those on back-up discs or tapes), not locating computer network access points in public areas, and physically securing equipment, especially laptops.

(xi) *Disaster recovery*

All IT systems and equipment are vulnerable to ‘disasters’ that result in information loss and server downtime. Dealing with these issues *a priori* assists in the reduction of information loss and the subsequent chaos created when such an incident occurs. Having practical measures in place to deal with a disaster should also allow a rapid business recovery. Security measures include the development of a recovery plan that outlines what to do when a disruption occurs (e.g. due to loss of electric power). Such a plan needs to be reviewed and tested periodically, and a copy stored offsite. Service agreements with service providers should also be obtained and documented. There needs to be up-to-date back-ups of key programs and their data, with copies kept offsite. It was also recommended that practices consider purchasing uninterruptible power supply devices, so that in the event of a power failure, IT systems can shut down appropriately. Lastly, practices were encouraged to consider a variety of technical solutions to hardware failure (e.g., the use of a Redundant Array of Independent Disks or RAID in which a second ‘mirror-image’ hard disk is used as a back-up).

(xii) *Third party connections*

Incoming information needs to be authenticated and internal practice data must be protected to minimise the possibility of disclosure to unauthorised third parties.

While the GPCG interim guidelines are very detailed, perhaps too much so, there is much information in them that could still be very useful to GPs and practice staff. It might be helpful to practices that specific sections of the 2001 guidelines remain available on the GPCG website as material that is additional to the more concise computer security guideline that this project has produced.

4.1.2(c) Other literature on computer security

Very little *research* literature exists in this area. In spite of extensive searches using numerous subject headings and text words, most of the articles in refereed journals were opinion pieces or guidelines. The latter were usually based on ‘expert opinion’ rather than data acquired through formal risk assessments. The British Medical Association have produced computer security guidelines (Anderson, 1996) as has the United States (Allender, 2002). Other guidelines have also been published, though not based on risk assessments (Caruso, 2003; Millman, Lee and Brooke, 1995). As an example, it is not hard to find information about encryption processes but little debate – let alone evidence - about its necessity. After all, paper-based records, faxes and even telephone calls seem much less secure than electronic data transfer, and the more stringent requirements for email may not be obvious to clinicians (Sardinas and Muldoon, 1998).

As other published guidelines cover similar issues to those found in the GPCG interim ones, it is not necessary to describe them in detail in this review.

Not surprisingly, there has been little argument opposing the view that the security of patient information is important for the proper ethical, legal, and professional functioning of the practice (Milstein and Tongo, 2001). Medical practitioners should be encouraged to put in place IT security behaviours to achieve efficient and safe management of patient data.

Unfortunately, the underlying protocols of the Internet were not designed to provide secure communication services. As a result, added security measures are required in healthcare (Georgiadis, Mavridis and Pangalos, 2003).

The relationship between confidentiality of personal health information and the use of computers and the Internet has been raised in Australia (National Health Information Management Advisory Council, 2001). The Privacy Commissioner (1995) reported that many Australians believe there is *less* privacy now than there was in previous years and that computers make it easier for confidential information to fall into the wrong hands. Therefore, policies are needed to guide the processing of, and receiving, modifying, disseminating, sending, storing and disposing of healthcare data (Allender, 2002). The Commonwealth Government has responded to the privacy issue by passing the Privacy Amendment (Private Sector) Act 2000 to safeguard personal information in the private sector.

Two related national projects which are examining the privacy and security issues in detail are *HealthConnect* which aims to establish a national electronic health record and *MediConnect*, an electronic medication record. *HIC Online* provides medical practitioners with secure data transfer for Medicare claims (www.health.gov.au/). GPs need to be aware of legal and technical developments in IT and comply with new laws and regulations governing its use (Milstein and Tongo, 2001).

However, information security is not simply a techno-legal issue (Caruso, 2003). Compliance with guidelines depends to a large extent on medical practitioners and practice staff believing in the value of the data they hold. This will encourage them to develop appropriate IT policies and procedures. Therefore, what the healthcare community needs is a 'culture of security' (Caruso, 2003).

4.1.3 Australian surveys on data security

Surveys on computer security behaviours of Australian GPs are few and far between. Divisional surveys are beset with low response rates and the validity of their findings is sometimes open to question. Nevertheless, they are likely to give us some idea of how large the gap is between ideal security procedures and what happens in practice, and are therefore worth describing. There were only three substantive surveys forwarded to the GPCG Security Project team by divisions of general practice: Adelaide Central and Eastern (ACE), Australian Capital Territory (ACT) and Monash Divisions.

4.1.3(a) ACNielsen (1998) survey

ACNielsen (1998) found that 70% of those GPs who had electronically sent out patient records did not take any security measures. They did find that 88% of GPs who had Internet access from their practices stated that their records were protected and secure from outside access.

They also found that 77% of practices were backing up data daily, 15% reported backing-up between every two days to a few months and 8% percent stated that they were unsure. Sixty percent of GPs in the ACNielsen study stated that they had a disaster recovery plan, 31% did not and 9% were uncertain whether they had one.

The Western et al (2001) results were similar (i.e., back-ups were typically done daily – although no percentage figure was provided - and 60% stated that they had a data recovery plan in place).

ACNielsen (1998) found that most GPs reported that their practices required the establishment of security protocols and that issues of privacy and security needed addressing.

4.1.3(b) ACE Division survey (2003)

Schiller (2003) in the ACE Division survey found that 32% of GPs used email to communicate with other health professionals but only 15% had applied for PKI certificates and keys from the Health Insurance Commission. That is, most electronic communication was sent in an unsecured form. Schiller also found that only 76% of practices had anti-virus software in place and only 33% updated virus definitions daily. In addition, Schiller found that only 60% of general practices were using firewalls (either software or hardware systems).

Ninety three percent of practice managers stated that they backed up data. From these, most practices indicated that they backed up on a daily basis (82%), every two days (4%) and every week (7%). In addition, Schiller found that 69% had tested their backup, 71% stated that they had a battery back up, and 73% said they had a disaster plan in case of system failure.

Less than half of the computerised general practices had formal IT policies and procedures. In terms of actual policies written, Schiller found that 36% stated they had written policies on virus protection, 22% on the use of staff email, 27% on staff access to the Internet, 49% on electronic patient practice data backup, 40% on the implementation of software upgrades, 42% on ensuring unauthorised persons can not access, and 44% had written policies on using passwords for electronic patient data security.

4.1.3(c) ACT Division survey (Rose, 2003)

A total of 45 practices in the ACT region (which represents a little over a third of total practices) undertook comprehensive IMIT audits between May 2002 and November 2003. Some of the key findings are presented below.

Sixty percent of general practices indicated that not all of the machines in the practice had antivirus software installed. Although most practices did have an antivirus program on their server, many didn't think that it was necessary to offer the same protection to other computers on their network.

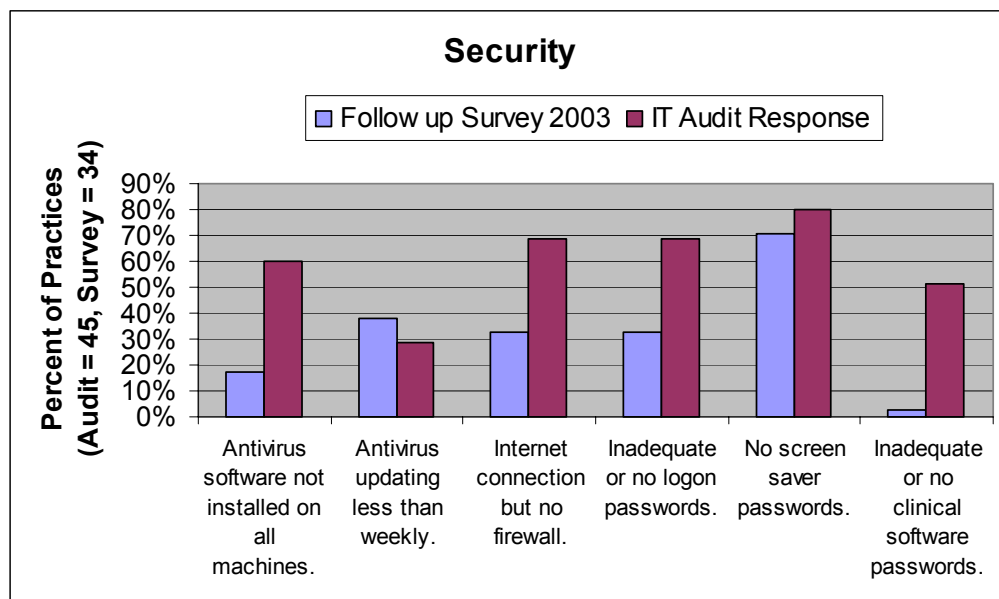
Of those that did have antivirus software installed on at least some of the computers in their practice, 29% indicated that this software was not being regularly updated. In some instances, antivirus software had never been updated since it was first installed, with many practices being unaware of the necessity for this.

Although most practices have an Internet connection, 69% of those that did indicated that they did not have a firewall. In a few cases, this included practices with a permanent broadband connection. The general response of practices without a firewall was either an indication that they weren't aware of what one was, or a feeling that it was unnecessary for their practice as they didn't use the Internet much.

Password security in practices is lacking with 69% revealing that they had inadequate or no passwords to log onto their computer networks. Eighty percent did not use screen saver passwords to protect their data when away from their machines, while illegal access to patient clinical records could easily be obtained in the 51% of practices who indicated that they had inadequate or no passwords for their medical software. In many cases, practices indicated that the doctor's name or initials were used for access to clinical data.

Figure 1 summarises the security procedures undertaken by practices before and after feedback on the original audit.

Figure 1: Security practices before and after feedback



(i) Backups

Forty-seven percent of practices surveyed indicated that they weren't sure whether all of the important files on their network were being backed up. In many cases, practices had their backup processes set up by external providers (often a matter of years ago) and could not be sure that software upgrades and changes had been taken into consideration.

Another 47% of practices also indicated that there were important files - usually patient letters or financial data - saved on workstations that weren't ever being backed up.

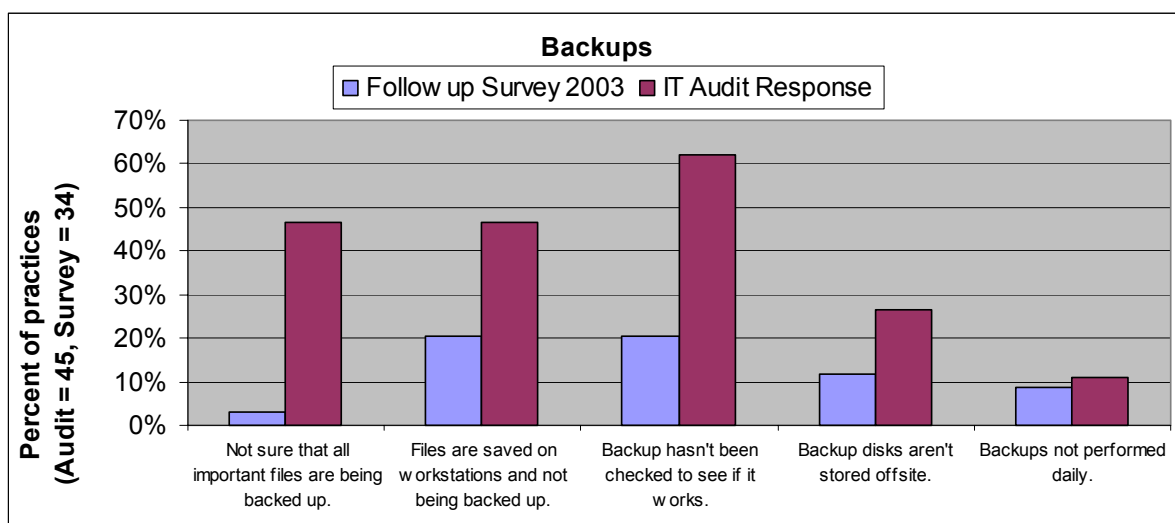
Sixty-two percent of all practices surveyed revealed that their backup media had never been tested to see if it worked. In following up some of these practices, the ACTDGP IT team discovered a couple of practices whose backups had not been working properly for years, if ever.

A further discovery from the audit was that 27% of practices were not storing their backup media offsite each day, leaving patient data prone to loss through fire or theft. A couple of practices indicated that their backups were being stored in a fireproof safe, however the likelihood of electronic media being compromised in high temperatures would be far too high to ensure that data would be protected in fire.

Despite daily backups being a fundamental process for any business, 11% of practices indicated that this was not happening.

Figure 2 summarises back-up practices before and after the initial audit.

Figure 2: Back-up procedures

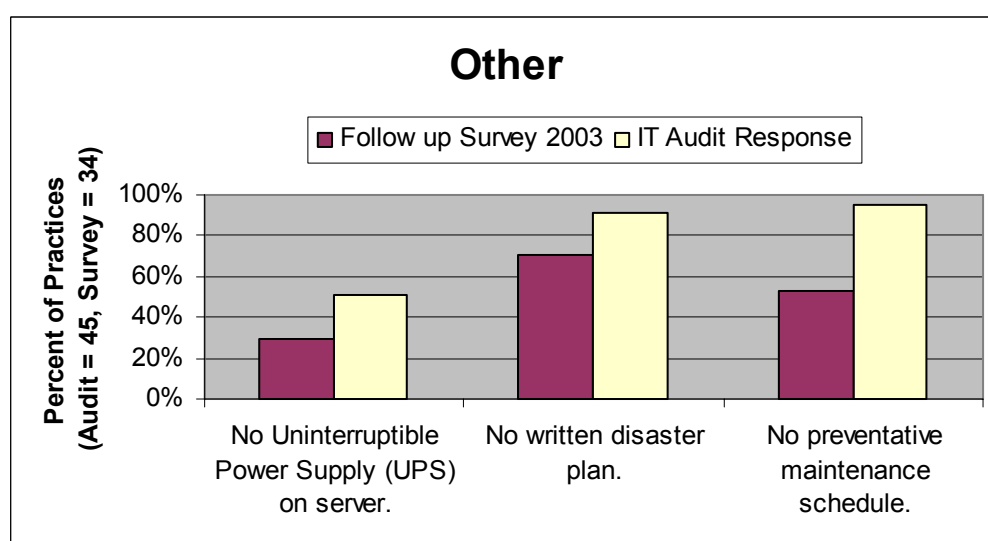


(ii) *Other Areas of Concern*

- Fifty-one percent of practices indicated that they did not have an uninterruptible power supply (UPS) installed for their server.
- Very few practices had plans in place to deal with or prevent computer problems, with 91% indicating that they did not have a written disaster plan and 96% indicating that preventative maintenance of their computer network was not taking place on a regular basis.

Figure 3 summaries some of the other security issues before and after the audit.

Figure 3: Other Security Practices



(iii) Summary of Findings

The follow-up survey indicates that practices that underwent the initial IT audit and received the subsequent report improved in the areas addressed by approximately 48%. While the process of auditing practices and supplying them with a report was successful in motivating practices to make improvements to their security and data protection, it does have its shortcomings. Some of these difficulties are summarized below.

- Auditing practices and supplying them with a report takes several hours for each practice (depending on size)
- If the cost of the audit and report process was charged to general practices it is highly unlikely that GPs would have had the opportunity to complete anywhere near as many audits
- While the follow-up survey indicates large improvements in many areas, there is no guarantee that these will continue to be maintained
- There is no compulsion for general practices to maintain any standard of IT security or data protection and therefore no guarantee that patient information is kept private
- Few general practices (and possibly divisions of general practice) are equipped with the knowledge or expertise required to safely protect data adequately
- There is a vast difference between practices that 'think' that they are taking the necessary measures to secure and protect their data and those that actually are. Accurately determining how well a practice's data is protected is difficult and time consuming

(iv) Conclusions made by the ACT Division

Most general practices are small to medium businesses that cannot afford to employ the expertise to competently maintain all aspects of their computer network systems from basic system administration to network security.

While a practice may make efforts to ensure that they have backup systems, firewalls, antivirus software etc. in place they do not necessarily have the expertise (or time) to regularly ensure that all of these things are working properly. Although commercial vendors could be (and are) employed to address these issues in general practice - usually at a significant cost - there are still no guarantees.

The lack of any minimum standard for general practice IMIT systems means that general practices are free to do as little as they like, which in the long run could be to their own and their patients' detriment.

A virtual private network (VPN) maintained by the division might provide a solution. The purpose of such a network would be to realise the benefits of economies of scale by remotely maintaining and protecting numerous practice systems from a central point.

4.1.3(d) Monash Division survey (Young and Schattner, 2002)

A total of 71 surveys were posted with 40 (56%) surveys being returned. Of those surveys returned 17 (43%) were completed by the practice manager or practice staff member and 15 (38%) were completed by a general practitioner

Of those practices using computers, all indicated that they employ routine backup procedures. Magnetic tape and compact disc were the most commonly used media, these being used by 11 (41%) and 9 (33%), respectively. Twenty-two computerized practices (82%) performed a daily backup of

their data, 3 (11%) performed a weekly backup and 2 (7%) performed their backup procedures less often than weekly. Of the practices performing regular backup procedures, 16 (64%) had checked that their backup was functional within the previous six months.

Fourteen computerized practices (54%) had an uninterruptible power supply (UPS) installed, 12 practices (86%) using a UPS had these installed on the server computer only. Seventeen computerized practices (71%) indicated that they had power surge filters installed.

Virus protection was used by 25 practices (96% of computerized practices). The frequency of virus file updates was as follows:

Table 1: Frequency of virus definition files update by computerized practices with virus protection software

FREQUENCY OF VIRUS FILES UPDATE	N (% OF COMPUTERISED PRACTICES)	
Daily	20	(74)
Weekly	3	(13)
Every 2-4 days	1	(4)
Less often than weekly	13	(57)
No response	2	(9)

In relation to data privacy issues, screensavers were employed by 22 practices (82%) using computers. Passwords to access computers and data were employed as follows:

Table 2: Use of passwords for data security and privacy by computerized practices

USE OF PASSWORDS	N (%OF COMPUTERISED PRACTICES)	
Passwords to log on to computers	20	(74)
Passwords to access programs containing patient data	18	(67)
Different levels of access for staff members	16	(59)
Passwords changed on a regular basis	3	(14)

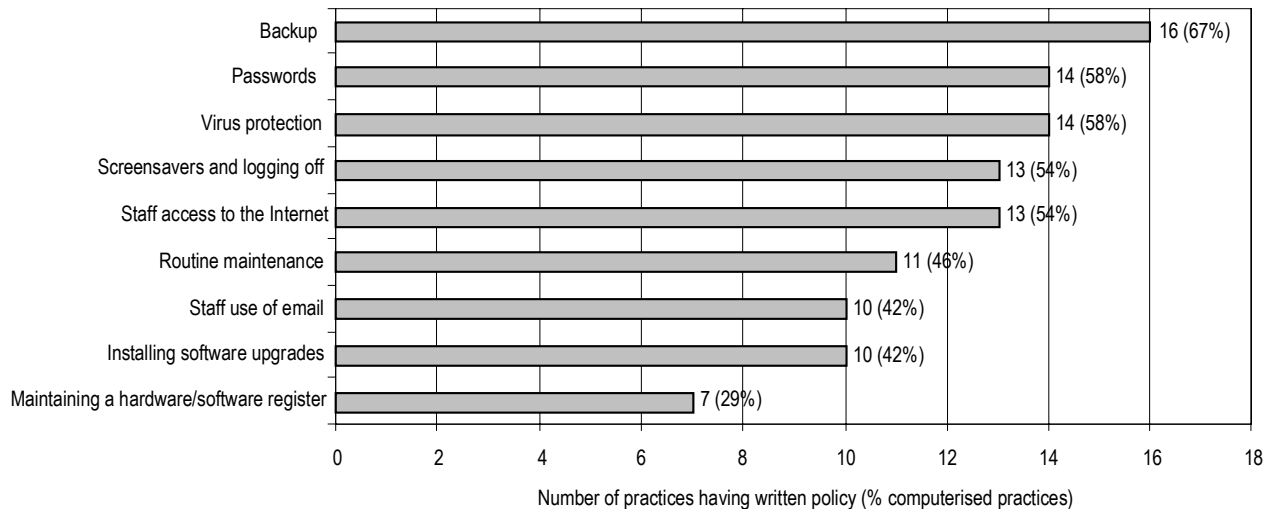
Twenty-three practices (85%) using computers had an Internet connection in the practice, with the vast majority of these, 23 (87%), being dial up connections. Six practices (32%) with Internet connections indicated that they were using a firewall (either software or hardware).

Only one practice (4%) indicated that it already had Public Key Infrastructure (PKI) technology in place for encryption of electronic data transmission. Another 6 (26%) indicated that they had applied for PKI encryption software certificates.

Sixteen practices (78% of computerized practices) reported that they have a practice IT coordinator. In 7 (47%) cases this person was a general practitioner at the practice and in 6 (40%) cases this person was the practice manager. Fourteen computerized practices (61%) have an IT disaster management plan.

Written policies for computer management are incorporated into practice policy documentation as follows:

Figure 4: Written policies for computer management incorporated into practice policy documentation



Over 50% of computerized practices had written policies regarding data backup, use of passwords, virus protection, the use of screensavers and staff access to the Internet.

There were thirteen practices (52%) using computers that identified having a domain name registered to the practice. Five practices (20%) using computers reported having a practice website.

4.1.3(e) Literature on increasing the use of the guidelines by medical practitioners

There is an extensive literature examining the evidence for the uptake of guidelines in general by medical practitioners. While a review of this literature is not required here, it is worth keeping in mind that systematic reviews on the adoption of guidelines (Grimshaw et al., 2004) conclude that there are no ‘magic bullets’ to achieving this. Encouraging medical practitioners to follow guidelines often takes a number of strategies working in tandem and the effects are sometimes surprisingly small. Researchers in this field argue that more time should be spent on developing implementation strategies than on the content of the guidelines themselves.

Some of the common barriers to the uptake of guidelines can be summarized as follows (Cabana, 1999):

- Lack of awareness of the guideline (don’t know it exists)
- Lack of familiarity (don’t know what is in it)
- Lack of agreement with content (don’t like what’s in it)
- Lack of self efficacy (don’t know how to use it)
- Lack of outcome expectancy (don’t believe it will make any difference)

- Inertia of previous practice
- External barriers
 - Practice staff attitudes
 - Patient attitudes
 - Lack of technical IT support

Grol (1997) has suggested a classification on approaches to changing the behaviour of clinicians which includes the uptake of guidelines:

(i) Internal processes

- Educational
 - Use a problem based learning approach
- Epidemiological
 - Rational information seeking, i.e. medical practitioners want to learn – information via the media, journals, etc.
- Marketing
 - Attractive product ('package')

(ii) External processes

- Behavioural
 - Audit and feedback
 - Reminder systems
 - Economic incentives
- Social interaction
 - Peer review
 - Academic detailing ('outreach')
- Organisational
 - Continuous quality improvement (CQI) approaches
 - Changing system structures (teams)
- Coercive
 - Accreditation

A number of these approaches are directly relevant to encouraging the uptake of computer security guidelines in general practice. Their application will be described in the section in this report on implementation strategies.

4.1.3(f) Conclusions about the literature

The surveys indicate that there is a considerable gap between what might appear in guidelines on computer security and what takes place in practice. Health consumers need to be assured that the privacy of their own health information will be adequately protected (National Health Information Management Advisory Council, 2001). The challenge is to ensure that GPs take up the advice provided in security guidelines as they now work in an increasingly electronic environment. Additional training for GPs will be required, as well as effective implementation strategies.

The most important resources drawn on for the development of security guidelines for this project were the Standards Australia papers and the GPCG interim security guidelines (2001). The Australian divisions of general practice survey reports have further reinforced the need for better security standards in general practice. Unfortunately, most of the health sector guidelines that have been produced are based on opinion; we have been unable to discover another one that has used as detailed an investigative method as this project has adopted.

4.1.3(g) Acknowledgements

The contributions of Grant Schiller from the ACE Division, Matthew Rose from the ACT Division and Karen Young previously from the Monash Division are gratefully acknowledged. The sections from ACE and Monash are edited versions of their original reports.

4.2 Quantitative risk assessment

No quantitative risk assessments were found – not at an individual or organisational level let alone a collated, industry-wide one. Most of the organisations that undertake risk assessments do so in a qualitative way, using their own checklists, and they provide individualised feedback to their clients.

The firms do not combine the information they obtain from their service in a quantitative fashion across a whole industry. We are therefore convinced that there are no suitable existing figures on likelihoods or cost consequences that one could use in general practice. Risks are so dependant on the particular circumstances that pertain to a practice or organisation that one would not expect there to be ‘average’ figures that would be relevant to an individual case. We are satisfied that our approach to risk assessment in general practice is both relevant and methodologically sound.

4.3 Key informant interviews: the risk assessment

4.3.1 Background

All experts in GP computing recruited for this risk assessment were generous (in terms of providing illustrative detail) and considered with their evaluations and suggestions as to ‘the way forward’ to progress the GP IT Security agenda. However, their perception of priorities and their associated proposed solutions varied depending on where these individual experts were working in the healthcare system.

The majority of GPs recruited to participate in the ‘expert’ interviews were able to systematically work through the risk assessment schedule and give informed, considered and detailed responses to the issues being raised and the questions being posed, thereby yielding particularly rich data for the study. However, experts in GP computing purposively recruited from elsewhere in the healthcare system, in order for the study to adopt a health-system-wide perspective, were less able to provide

considered or informed responses, particularly in relation to estimating the likelihood and potential magnitude of the consequences for the nominated and other security risks. This was the case both within the organizational and technical frameworks adopted for the purposes of the interview.

It is also crucial to point out, that although these study participants did not provide the field officer with clear-cut estimates and likelihoods of individual risks, they did however, all agree that the technical and organizational risks listed in the interview schedule were all important. None of the nominated risks were dismissed as non-essential. It is suggested therefore, that the tabulated data presented in the 'no direct response given' of the risk assessment be considered in this context. Moreover, these experts did provide the field officer with valuable information and insight into the technical and organizational 'interface' between general practice and a number of national and state e-health systems reform initiatives, the details of which have been incorporated into this risk analysis.

Many experts in the study, when asked to identify strategies to manage security risks in general practice, did so, understandably, with a focus on individual or 'sectional' interests. However, in order to derive greater benefit from the current substantial investment in evolving national IT standards and common infrastructure, individual business units may like to consider the potential benefits from harmonising their current strategies with others on whom their activities may have an impact.

Lack of explicit reference to such harmonisation by the informants, although implicit in the vision of the auspicing agencies, emerged as a potential risk as the outcome of the actual process of conducting the interviews with experts working in different situs. The suggested implementation strategies and computer security program implementations that have emerged from this project, if adopted, will then, in order for the 'diffusion' (Rogers, 1995) of the security checklist to occur, will need to flow through a number of key stakeholder organisations which all have 'politics of their own' (Winner, 1989).

The project's risk analysis details what informants considered to be the likelihood and magnitude of potential consequences of a number of risks. However, once this was completed, the field officer focused on exploring the details of implementing and coordinating change management at a national and practice-based level. Our reading of the tender and the current discourse within the wider GP IT community encouraged us to put considerable effort into the risk analysis primarily to illuminate the organizational, implementation frameworks and other processes currently at play.

And finally, the process of conducting the interview provided the participants with an opportunity for critical reflection on their 'position' on GP IT Security. As a consequence of this, three outcomes may have emerged:

- (i) Firstly there was a 'shift' in what some experts considered to be the *most* important IT issue facing general practice from that which they originally stated at the commencement of the interview. Their prioritization changed after having gone through the comprehensive organizational and technical risk analysis which formed the bulk of the interview;
- (ii) Secondly, some of the questions challenged study participants who were not practicing GPs, and their initial enthusiasm for the task evolved into a more reflective and considered discourse. They began to see the ramifications and complexities *from the GPs perspective* of implementing an effective change management process in order to improve IT Security in their practice;
- (iii) And finally, as a consequence of their serious investment in the active interview process, the potential for stakeholder 'buy in' to future GP IMIT collaborative problem solving may have improved.

4.3.2 The Context of Computer Security In General Practice

Please note that in this section of the final report, the authors have taken license to edit down or rephrase some suggestions from key informants in order to facilitate their inclusion, not only into the following series of matrices, but also into any subsequent policy or implementation schedules which may draw on this work. In some instances quotation marks have been used within the matrices to retain the specific 'flavour' of the intervention strategy being proposed. However, all *italicised text* in the risk analysis is original text taken from the interview transcripts. Care has also been taken to retain the original meaning and context in which the experts' comments were made. (CP)

4.3.2(a) Personal health information

This general practice IT Security risk analysis is being undertaken in a much broader context: described by one informant as, *the culture of how personal health information is handled*. As another expert in the study noted, *although often used for functional purposes, such information is actually part of a person's life... and the community at large benefits from general practice being vigilant and adopting appropriate work practices in this regard*.

4.3.2(b) Patient information: data quality and perceived value

Another important issue raised by experts in the study was the actual *quality* and *value* of the data being *stored or preserved by the business*. As one GP outlined, *now, in a lot of practices ... and mine is no exception, the quality of the information that's on the database is still not worth [very much] ... In this kind of situation, IT maintenance and backup are only slightly important ... because if the information's lost, hey, it's just like losing your script pad and there's no great problem, you'll reconstruct it next time around*.

4.3.3 The most important IT Security issue facing general practice at present

Losing our patient and financial records (GP, interview transcript)

At the commencement of each telephone interview, experts in GP computing were asked what they considered to be the one most important IT Security issue facing general practice at present. Based on the opinions of these 14 experts, the most important issue is the organisational and technical aspects of ensuring the successful backup and protection against loss of practice e-data.

Experts presented this key risk within a range of contexts. Those that were practicing GPs raised this issue with a positive attitude, and in the context of developing effective solutions that were trialled and currently work in their own practice. They also acknowledged that this was a complex undertaking. On the other hand, respondents who were senior managers of health systems 'infrastructure initiatives' and were working in Commonwealth and State Government Departments, reiterated the same need, albeit with a different imperative. Their focus was on the need *to address IT risks around patient and [business process] data exchange*. They were concerned with general practice *coming up to speed*, in terms of installing and managing a physically secure, *adequate* [in terms of performance] *and reliable hardware* infrastructure at their *data collection nodes*. *Physical encryption* and *e-signatures* were also high on their list of security risks in general practice.

Physical and Internet security (firewalls, anti-virus solutions and problems with encryption) were noted, as was the need to address the *confidentiality of patient records*. Furthermore, a number GPs expressed the perception that *a large number of general practices were extremely small businesses, and many of whom had limited in-house knowledge of, and expertise in, IT Security*, and therefore, considered the notion of *having a really secure systems beyond their reach*. GPs interviewed in this study also suggested that for IT Security to be improved across the wider general practice community, that a range of interventions should target *the attitude that GPs adopted* in terms of *the manner in which they approached the management of their hardware* infrastructure and the data stored therein.

4.3.3(a) How GP IT security issues differ to those of other parts of healthcare system

The majority of specialists do not own their own [IT] systems ... they are not in a position to make decisions about which [IT] system they have [as they work within a hospital IT infrastructure]... [Some] have systems they can carry around with them ... [For example] their clinical records are only copies of letters they've written to referring doctors plus pathology results. (GP, interview transcript)

Although the *management of information* was considered to be similar in many ways, in terms of patient records, GPs considered the *comprehensiveness* of their patient records a key difference from records kept in other parts of the healthcare system. They were *custodians* of *complete histories* rather than just *small aspects*.

Unlike the Commonwealth and State Government *systems*, GPs *own and use their own practice systems*. *There are many of them and they vary in sophistication*. The *individual rate of adoption* [of IT] *was also variable*. General practice was considered to be *a hybrid of private and public*. Hospitals were considered to *have fully-fledged information services... and had time to put policy into place*. They also were also thought to have *skilled and appropriate IT support on tap*. *Specialists* were thought to be *either better off or worse off - no systems or much better systems* and the larger *hospital technical infrastructures* were considered to be *fragmented*. The *sensitivity of patient information* was noted by all.

4.3.3(b) How GP IT security issues different to those of other small businesses

The primary security issue noted by experts in the study which differentiated general practice from other small businesses was *the sensitivity of the [patient] information* and therefore the need for *privacy*. One informant commented that, *by and large, general practice is a small business*, with the difference that the data kept is of a sensitive nature. Another said that general practice is the same as the other small businesses adding that it is *basically the same except for the storage of clinical data*. However, this patient data, unlike financial records, is not easily *reconstructable ...and failures may have negative health outcomes*.

In terms of business operations, experts working with the government sectors who were interviewed considered general practice to be just like other small businesses. On the other hand, practicing GPs who were also experts in GP computing, considered general practice, from an organisational perspective, to be *intense and poorly resourced*, and in terms of business, in most cases *generally less sophisticated*. Unlike *more autonomous* small businesses, general practice was *increasingly being expected to be reactive and responsive... working with small funding pools and temporary [financial] incentives and initiatives*.

However, in the context of the National Privacy Principles (NPPs) the *sensitivity of patient clinical information* was considered more acute by these same experts. As one expert from the government sector put it, *you're dealing with an area where consumers are very concerned about what happens with that information and [therefore] need far more guarantees than other small businesses about what happens to their [personal] information and how it is secured*.

4.3.4 The lay of the land: what is to be changed?

Experts who were also practicing GPs, came from a range of practice settings. Some were principals of small rural practices, others from much larger metropolitan practices. However, although these clinicians were software and *systems-savvy*, a number worked in practices where although they were *able to positively influence* they were *not directly able to control the security of either their systems or the [security-related] work practices of their professional colleagues*. The following is a description of a 21 doctor metropolitan practice.

Practice IT Security vignette A: does this sound like your practice?

There are no written policies. Backups are done with restorations of the financial files (but not the clinical information!) Screen savers exist on the front desks, but some doctors turn off the screen savers. (I have not seen a screen saver on any of the 18 clinical workstations!). Passwords are only in relation to accessing the system – once the workstation is turned on, anyone can get into it. Access to [name of clinical software] is limited to passwords and different levels of access set by [name of clinical software]. Virus protection and firewalls exist. There is a UPS that allows the orderly shutdown of the server in the event of power interruption. There is no data encryption. [GP, interview transcript]

Although some IT security-specific technical procedures have been put in place in this relatively large practice, the absence of any formal *written policies* suggests that this has not been done in a co-ordinated and systematic way. Furthermore, it does little to convey information about the actual IT security practices and approach to the confidentiality of electronic (and other) patient health information of the business as a whole.

4.3.5 General Practice IT Security Risks: through an organizational change management framework

Its part of a bigger picture...it's the who behind the what (GP, interview transcript)

Experts in GP computing were then asked to look at a series of organizational IT Security risks, and in doing so, consider what would be the likely potential magnitude of the consequences for the both the patient and the practice.

The following scale with three levels of magnitude was used during the telephone interviews:

Consequences (magnitude)	
High	of major significance to the business or to the patient
Medium	important, but not of critical importance
Low	a nuisance, but can cope with this without too much difficulty

Refer to **Table 3: Organisational framework: summary of experts' risk analysis** for a summary of what experts in GP computing considered the greater (and lesser) potential IT Security risks. Each risk is then discussed in detail.

Table 3: Organisational framework: summary of experts' GP IT security risk analysis

RISK ANALYSIS	Potential magnitude of risk			
	High	Medium	Low	No direct answer given *
Organisational Risks				
Practice IT Policy				
Risk to the Patient	6	2	2	4
Risk to the Business	7	3	0	4
IT Practice Coordinator				
Risk to the Patient	2	5	3	4
Risk to the Business	8	2	0	4
Practice Disaster Plan				
Risk to the Patient	3	3	3	5
Risk to the Business	6	4	0	4
Practice Email & Internet Policies				
Risk to the Patient	7	0	2	5
Risk to the Business	7	2	1	4

* Respondents from the government sector indicated that they were either not in a position to make an *informed* comment or expressed their reticence to do so.

4.3.5(a) IT Policies in the Practice

*In my experience, where there are **no IT policies** there is generally **no IT focus** ... there is no investment in developing a proper IT system ... you end up with a dog's breakfast of bits and pieces that don't work.* (GP, interview transcript: original emphasis)

In terms of *patient risk*, experts interviewed considered the potential magnitude of the consequences of *not* having a sound practice IT policies in place as high. However, IT policies, and any other elements of a *co-ordinated plan* need to be considered in a broader organizational context. One GP describes it thus, *patient risk is probably less of an issue ... there may well be other things [such as] managing confidentiality of records ... keeping doors locked. These sort of non-IT policies still impact on the way in which access to the machine is maintained.*

Interestingly, two GPs who were early adopters and advocates of ICT in general practice, considered the potential risk to patients of not having an IT policy in the practice, to be low. However, these same GPs, along with others, considered the potential magnitude this risk posed *to the business* to be high. Overall, experts drawn from the Government and other sectors ranked the potential magnitude lower in both domains.

4.3.5(b) Practice IT Coordinator

While most respondents indicated that there was a high risk of damage to the business aspects of general practice if there were no Practice IT Coordinator, the view about risk to patients is less clear. One GP reflected that were there was no designated Practice IT Coordinator it was *more likely* [that] *empiric decisions* [would be made rather than] *properly thought-through business decisions*.

Respondents reflected on the role of a practice IT coordinator within a wider *user competency* framework: that is, their current perceived lack of in-service training and formal induction for practice staff in most practices.

4.3.5(c) Practice Disaster Plan

*Start with a basic **immediate** computer disaster plan... you don't need a lot... a bit of training and documentation for how to deal with the front desk issues for example... such as when patients come in and the computers aren't working...the immediate problem is to get patients seen, to get bookings made...have money taken, invoiced and receipted...its simple...use a paper-based system **that** needs to be documented.* (GP, interview transcript: original emphasis)

After some open reflection on the potential range and nature of what could be described as *disasters* (such as power outages, *floods, typhoons and other acts of God*) respondents, through their own narrative and logic, reached a similar conclusion whereby, whatever the nature of the disaster, *the system had gone down or was out cold*. Given that scenario, respondents indicated that they thought there was considerable risk in not having a practice disaster plan in place, albeit different in scope, particularly in relation to the functioning of the business. For them, it was considered *vital* to have an alternative system in place whereby they could keep booking and treating patients. One GP explains that, *we receive the vast bulk of our pathology results electronically, and don't get paper copies at all*. This GP expressed concern about the potential outcomes of a scenario where the IT system was unserviceable. In this GP's opinion, the practice could increase its medico-legal risks in such a scenario: *we could well find ourselves in the situation of not having and, perhaps more importantly, not being aware that we don't have certain results*.

When considering the potential magnitude of risk to their patients of not having a sound disaster plan in place, these same participants again responded to the interviewer's question with open narratives to support their logic. However, on this occasion, when assessing the potential risk, clinicians' stories were case-based vignettes, where GPs were contemplating the potential risk with specific patients (and their needs) in mind. These vignettes, although variable, drew to a similar conclusion: the magnitude of the risk to the patient depended on the nature of the patient's illness, and the immediate need (or otherwise) on the part of the clinician or *practice* to access vital information [for clinical decision making purposes] *stored in the system*.

4.3.5(d) Email and Internet policies

It's complex because the techos say anything is possible and it's actually not the techo issues, is it? (GP, interview transcript)

*It's been high on the agenda in our practice ... since there has been a firewall nothing gets in. If I try to look at a Word or a PDF document I've **got to go home** to do it 'cause I **can't download** it and **that's a nuisance**. It's gone from one extreme to the other.* (GP, interview transcript: emphasis in original)

Respondents considered the potential magnitude or risk, to both patients and to the practice [as a business] of not having [and implementing] practice wide email and Internet policies substantial. Those who did not consider it so, did so on the premise that there was a *relatively low use of email*

and the Internet for clinical purposes, and, therefore, compared to the other more *tangible* risks (such as backups/data restorations not working) this was, in that context, *relatively minor*. However, these same respondents did note that this risk was *on the horizon* and commented that *unfortunately someone's going to be sued before that issue becomes crystal clear to everyone*.

4.3.5(e) Other organizational risks

A number of additional risks associated with IT Security were suggested. These related directly to the development and promulgation of documented policies and procedures within the practice. Furthermore, respondents emphasized the need for the identification of *someone to do specific tasks...the who behind the what*.

Suggestions included: *mapping of IT infrastructure; regular system service reports; documenting how external (3rd Party) help/support is (or should be) managed; staff induction to include IT security matters, staff in-service; the articulation of a separate physical security policy; a computer system service record; access control; token management; password management; QA systems; access rights/control; standard protocols for all staff in the practice; and a systematic education and training program*.

General reference was also made by a number of GPs to risks to *the organisation* associated with engaging in *electronic communication with patients*. However, this was generally not considered to be a high priority (given the others) at present, although it was *looming on the horizon*.

Community health centres were mentioned by a number of informants as potentially *places where access and IT security problems were compounded*. Suggested reasons why this may be the case included being seen as a wider range of clinicians, and others, working in this health care setting; an individual's personal healthcare record, seen as a *shared record...within a shared [computer] system* was not clearly identified with one particular clinician; and the existence of *lots of terminals with lots of people having access across, in many cases, lots of sites*. The computers used in these settings were also perceived to be *old and often unreliable*.

4.3.5(f) Access rights: vulnerability

A clear protocol on who has access to what is essential to reduce the potential risk of inappropriate access to information. This may have a high cost to the business as one GP reflects: *if a practice doesn't have some clarity about who has access then ... ad hoc decisions are made on any particular day about who should have access to information or not ... In that situation the practice exposes itself*. It may release or provide access to *information to people who shouldn't have it*. Furthermore, it was noted by a number of experts from all sectors that moving general practice to *compliance with privacy legislation will cost big money*. In the context of State and Commonwealth privacy legislation, although *larger practices may find it easier and more cost effective to generate consent forms and access [to patient information] forms, developing similar procedures by smaller practices with fewer resources for their own use should also be encouraged*.

A *sharing with the consumer some of the safeguards that were being put in place* was also recommended.

4.3.6 General Practice IT Security Risks: from a practice-based Information and Communication Technologies (ICT) infrastructure management perspective

It really depends on what's gone wrong ...(GP, interview transcript)

In addition to being asked to make a considered judgement in terms of the potential magnitude of risk to both the patient and the business (as described in the previous section), experts with a strong technical background in GP computing were asked to also consider *the likelihood* of nominated and

other technical risks occurring in the wider GP community. Respondents were asked to make this assessment on the basis of not only their own experience [with computer systems in their own practice], but also on their experience and observations when assisting colleagues and through insight gained through other exchanges with professional colleagues and peers. The following working definitions for likelihood were used for the telephone interviews:

Likelihood	
High	very likely to occur within the next 12 months
Medium	might occur within 12 months
Low	not very likely to occur within 12 months

Refer to **Table 4: Technical framework: summary of experts' GP IT security risk analysis** for a summary of what experts in GP computing considered the greater (and lesser) potential IT Security risks. The experts' view regarding the likelihood and potential magnitude of nominated and other risks is then discussed in detail (see below).

Table 4: Technical framework: summary of experts' GP IT security risk analysis

RISK ANALYSIS	LIKELIHOOD and POTENTIAL MAGNITUDE OF RISK			
	High	Medium	Low	No direct answer given*
Technical Risks				
Backups (restorations) **				
<i>Likelihood of failure</i>	6 (2)	1	3(1)	4
Risk to the Patient	4 (3)	1	4(1)	5
Risk to the Business	6 (3)	1	1	6
Screen Savers				
<i>Likelihood of failure</i>	3	0	5	6
Risk to the Patient	0	2	3	9
Risk to the Business	0	1	5	8
Passwords				
<i>Likelihood of failure</i>	4	2	2	6
Risk to the Patient	4	0	2	8
Risk to the Business	4	2	1	7
Malicious code (eg. viruses)				
<i>Likelihood of failure</i>	8	0	2	4
Risk to the Patient	3	2	4	5

RISK ANALYSIS	LIKELIHOOD and POTENTIAL MAGNITUDE OF RISK			
	High	Medium	Low	No direct answer given*
Risk to the Business	7	1	1	5
Firewalls				
<i>Likelihood of failure</i>	7	0	0	7
Risk to the Patient	5	2	0	7
Risk to the Business	6	1	1	6
Power Surges				
<i>Likelihood of failure</i>	3	2	2	7
Risk to the Patient	2	0	3	9
Risk to the Business	5	1	1	7
Encryption of Data Transmission				
<i>Likelihood of failure</i>	1	4	3	6
Risk to the Patient	7	0	1	6
Risk to the Business	5	4	0	5

* Respondents from the government sector indicated that they were not in a position to make an *informed* comment.

** The decision to differentiate data collection between backups and restorations was made after the third interview. The two datasets have been presented together in order to indicate the logical association being reiterated by the respondents, irrespective of which ‘cut’ of the risk assessment the analysis of the data was adopting.

4.3.6(a) Back-ups and restorations

It's not immediately clear what's where...(GP, interview transcript)

Experts in GP computing, when considering general practice as a whole, suggested that there was a reasonable likelihood of backups failing. The reliability of software in such a situation is identified as a key enabler here. One GP explains that *there have been occasions when I've got a [clinical software] backup disc, that I've tried to load up on my machine at home and I've had relatively little success. I've been able to do it once or twice but ... more often than not, it's not successful.*

Furthermore, the potential magnitude of the risk to both patients and the business was considered to be of major significance although difficult to discretely quantify. Here a GP makes this point *patient risk is probably more difficult to gauge... because of the fact that we do have paper records and partly because of the variability of the amount of [patient] information in the machine. Nonetheless it would be an anguishing time.* While this GP consider an unsuccessful restoration as *anguishing*

others have indicated that they considered the potential risk associated with a backup failing as more of an inconvenience rather than of critical importance.

Another GP pointed out that he considered the currently available technology [for backups] inadequate. Although *many different backup solutions have been trialled ...the results are very disappointing... none of them are 100% reliable*. This GP estimated *that up to around 10% of backups aren't working* thereby the practice having to *carry a 10% risk with restorations*. This GP and his team were *currently looking at a range of hardware and ...writer solutions to try and solve the problem*.

Finally, the potentially negative financial implications of GPs not have effective data backup strategies in place are considerable. One expert referred to previous work done by *Dr John North and the GP Practice Management National Committee who did a survey in the 1990s that showed that the average General Practice was owed, at any one time, about \$20K per doctor, as money owed to the practice*. So, *if your electronic accounting system at the front desk dies, walks out, melts, whatever ... you've basically lost \$20 grand per doctor unless you have a backup of the people that owe you money. And there is almost no way that you could be able to reconstruct it. So the risk is huge, to say nothing of the clinical information and all the other stuff*.

4.3.6(b) Screen savers

All our rooms are set out in a way that patients sit next to the doctor so they can see what's on the screen. I have very little difficulty with patients seeing information that relates to them on the screen. It's nonetheless possible between patients to have some confusion as to what's on the screen, and that's where you run into problems. I would much prefer to have a regular screen saver that clicked in ...I don't have any idea what the appropriate time should be. (GP, interview transcript)

In terms of the nominated and other technical risks referred to in the study, respondents considered the potential magnitude or risk to both patients and the business as relatively low; that is, more on an inconvenience than of critical importance. The likelihood of failure was also considered to be low; albeit due to the fact that screens savers were perceived to be rarely used in most practices.

Where screen savers were noted by respondents as a potential risk, this was done in the context of *litigation for breach of confidentiality*, and therefore a potential risk to the business, or *breach of patient privacy*, and therefore a potential risk to the patient. GPs also commented that while adopting the use of screensavers might alleviate these risks it would present other IT practice use issues. They were unsure of how to ensure an appropriate time interval for screen saver activation: one that would reduce these risks without unduly restricting or irritating the GP computer user.

4.3.6(c) Passwords

*I don't think you can justify not having passwords... however, you could certainly depend on there **not being a consistent approach within the practice**.* (GP, interview transcript, emphasis in original)

In terms of the wider GP community, there was a reasonable likelihood of GPs and their staff not using passwords, or multiple *levels of access* protocols. This was the case in reference to both clinical and general practice management information. However, user access in the wider GP community to practice financial data was, in the opinion of experts, likely to have been implemented, and implemented well, thus reducing the potential risk of failure in terms of enabling unauthorised access.

A number of practicing GPs presented the wide-spread (non)use of passwords by GPs and their practice staff with the context of *the trust between GPs and their practice staff*. While trust between clinicians and their staff is essential, passwords which provide little security may well be of little

practical value. This point is illustrated by this comment by a GP interviewed: *Although each individual GP has their own password, it is collected by one of the practice staff and then written on a piece of paper that hangs up in the back office area.* Such practices need to be taken into consideration if the adoption and implementation of passwords is considered integral to the establishment of IT Security standards in general practice. From discussions with experts, one of the reasons screen savers were used was *to prevent members of the public coming in and looking at [practice] computer[s].* Practice size was considered to be a determinant of how great the potential for password use (or lack thereof) posed. As the size of practices increases, so does the potential breach of security associated with passwords.

4.3.6(d) Malicious code and firewalls

...better to just put on a condom... (GP, interview transcript: original emphasis)

Where GPs and practice staff were accessing the Internet, experts in GP computing considered the likelihood of failing to put into place appropriate measures designed to mitigate, or at least minimize, the potential risk caused by malicious codes (such as viruses) by the wider general practice community as high. The practical consequences of such an event can be considerable. One GP comments on such an experience: *the system was down for some time ...it took quite a lot of time to eradicate the viruses ... some of them are very difficult to get rid of.*

Furthermore, not doing so was generally thought to pose a high risk particularly to the business. Rectifying the problem *would cost* in terms of *both money and people time*, as well as *disrupt the day-to-day operating of the practice*. Respondents varied in their assessment in terms of the magnitude of risk to the patient.

Expert opinion suggests that Linux users are at a lesser risk in relation to the potential magnitude of risk posed by malicious codes such as viruses.

4.3.6(e) Power surges

Experts considered the likelihood for power surges and *brown-outs* to be more likely in rural rather than metropolitan settings, and the potential magnitude of risk greater for the business, than for patients. However, a number of GPs refer to the nuisance a disruption can cause to both the business and the patients, particularly when some medical procedures are unable to be undertaken due to a disruption in the mains power supply. This GP commented on the impact of a power failure on his practice: *We had the whole power go off the other day ... quite a number of the [individual computers] just shut down and we [GPs] simply couldn't do anything with them. It was only individual machines though. It wasn't the whole system. You could still do things such as make patient bookings.*

4.3.6(f) Encryption of data transmission

We don't have, as a practice, any particular organised approach to encryption of things like specialists' letters. (GP, interview transcript)

Respondents noted the *in-principle requirement* for the encryption of all patient data if transmitting it electronically *outside of the actual practice*, or data collection *node*. Furthermore, the potential magnitude of not doing so was high, particularly for the patients (*breach of confidentiality*) as well as for the business (*litigation as the result of breach in security and privacy*). The increased risk to the practice of not using e-signatures was also noted.

(i) *Pathology results*

A number of experts made reference to using *an encrypted service with the pathologists ... that's a dial-in system rather than being Internet-based*. In terms of access security, *there's a certain level of protection that's already built in [because the practice] has to actually dial in to get the information*.

(ii) *Emails between GPs and specialists*

Experts working in different parts of the health system referred to the *anticipated* online transmission of patient information between general practice and specialists. As one GP in the study commented, *I have yet to receive my first specialist's letter ... it's not a huge issue at present. But one of the reasons why it doesn't happen is because of concerns that many of us [GPs] have that there is no effective system for encryption of information that would guarantee the safe passage of ... patient information*. As another GP in the study suggested, *GPs don't want to spend any money [on encryption] ... it's not worth the time and effort to expend our time and energy... The government is doing this ... or the providers, they do actually pay for it. The GPs are lucky*. However, it is still unclear how the process of encryption of transmission will materialise in the online exchange of confidential patient information between GPs and specialists.

(iii) *General Practice and PKI Use and Digital Certification*

A Commonwealth Government expert in GP computing who was interviewed indicated that *approximately, 20% of practices across Australia have a location certificate. On current estimates we think about 11% of GPs have an individual certificates. As of today, we have about 7,000 certificates in the [general practice] sector. There's a 75/25 split, so about 75% of them are individual certificates with a personalised certificate and about 25% location or practice certificate*. However, although certificates has been issues, this same respondent expressed concern about the certificates not actually being used.

4.3.6(g) Other technical risks

*One of the most prevalent risks that I see to general practice security is **doctors tinkering with the so-called system computer guru**.* (Medical Software Vendor, interview transcript: original emphasis)

The actual age of the [ICT] equipment [in practices] itself is a risk... a lot of them are running six or seven year old machines on a mission critical system (Government, interview transcript)

A number of additional key technical risks were noted by the study participants. The first set of these relates to *software characteristics*. These include: *spy-ware management, MicroSoft (MS) product obsolescence, MS product upgrades, vulnerability of email software and levels of access to the system controls*. In terms of risk mitigation, sensitizing the wider GP community to these risks through documentation, education or other means may prove worthwhile. We recognize that addressing such risks is peripheral to the Commonwealth's current approach.

The second series of additional risks relate to the *maintenance and configuration of hardware*. UPS, systems maintenance, e-signatures and encryption, the technical aspects of data storage, *audit logging and privacy auditing*.

Whilst these additional technical risks have been grouped into the conventional *software and hardware* dichotomy, it is important to recognize and to emphasise that changes to software may well impact on hardware requirements and visa versa. Furthermore, the importance of the

organizational aspects of any such modifications, particularly in relation to implementation and monitoring, must also be considered.

GPs in the study emphasized the need to *be particularly cautious when installing upgrades* and others referred to hardware and software *obsolescence* as risks to general practice security.

It is important to note here that a small number of technical experts in the study encouraged the further detailed articulation of the existing GPCG Draft Security Guidelines as they did not consider it, *specific enough...especially in relation to* [security risks associated with] *email and the Internet*. Adopting another approach, one highly regarded technical expert in the study proposed that *by getting rid of one email software program [that]... three quarters of the security risks seen now would be solved*. This expert suggested that, *there are many other readily available and suitable commercial as well as free alternatives*.

However, for the majority of experts participating in the study, once having completed the risk analysis, the focus for them was on the *who and how* rather than the *technical specifications of the what*.

4.3.7 Evaluating security risks in general practice: setting the priorities

Although not all of the study participants were guided through the comprehensive risk analysis by the field officer (the details of which have been presented in the previous section) all experts in GP computing recruited for the study were given the opportunity to, in the first instance, nominate what they considered to be high (medium and low) priority organizational and technical security risks for Australian general practice at the present time (see **Table 5: Experts' prioritization of IT security risks needing to be addressed**).

The field officer suggested to respondents that they take into account the following factors: (i) firstly, the significance to the welfare of the patient or the functioning of the business; and (ii) the potential cost to address the potential risk versus the cost of dealing with the breach in security.

Table 5: Experts' prioritization of IT security risks needing to be addressed

RISK TO BE ADDRESSED	PRIORITISATION		
	High	Medium	Low
IT Policies in the Practice	7	3	0
Practice IT Co-Ordinator	6	3	0
Disaster Plan	7	3	0
Email & Internet Policies	6	1	2
Backups (restorations)	7	0	1
Screen Savers	1	3	4
Passwords	3	5	0
Malicious code (eg., viruses)	8	1	0
Firewalls	8	1	0
Power Surges	3	2	2
Encryption of Data Transmission	3	3	2

Malicious code (such as worms and viruses) and the implementation of firewalls were equally considered by the experts participating in the study the most important IT Security issues facing general practice presently. The management of these two factors was considered to have a significant effect on the integrity of IT systems and so naturally patient data stored in these systems.

Backups (and restorations) which were considered (in the *initial* stages of the interviews) as the most important IT Security issue still rate highly. The absence of reliable and effective backup and restoration systems can have detrimental effects on the integrity and dependability of data structures.

The development of policies and plans for managing IT in practices rated next highly. IT Policies in the Practice and Disaster Plans were not considered low risk by any interviewees.

4.3.8 Other risks

GPs using the Internet to communicate with patients was raised. As one GP in the study argues, ... *what we can do with the technology is significantly ahead of what we have thought through are the issues ... [in relation to the] information we provide to patients and the context in which we do it. Its not just a question of charging although that's inevitably an element of it, but I think the problem that I see is that there is not yet a clear understanding of how a GP should respond to comments from a patient in a way that [ref to online] ... the information might be accurate but the context in which the information is provided [by the GP] and in particular the interpretation that's place on that information by the recipient of it, might be quite different to what was intended. It's not like when you've got someone sitting there in front of you, then you've got an opportunity to actually adjust the content depending on the response you get from the individual, but you can't do that with a piece of written information.*

The field officer then asked the respondents to prioritise the risks that they individually nominated as high priority in the order in which a national program addressing IT Security risk in General practice should be ‘rolled out’ (see **Table 6** for experts’ individual prioritisation of which IT Security risks in general practice should be addressed first). This additional stratification process on behalf of the respondent was undertaken so that the expressed needs of which risks individual experts considered to be most important in their ‘IT Security’ setting was made explicit.

Table 6: Experts’ individual prioritisation of which IT Security risks in general practice should be addressed first

KEY INFORMANT EXPERTS IN GP COMPUTING	HEALTHCARE SYSTEM NODE	FIT	1 ST PRIORITY	2 ND PRIORITY	3 RD PRIORITY
01	Consumer representative	Commonwealth and State Government privacy legislation	Education and training – sensitization to privacy and security	Greater use of screen savers and quality assurance systems associated with the management of patient information	Formalisation and clarification of GP-based population health data collection processes
02	General practice	Financial incentive model Functioning of the business	Backups/ restorations	Viruses, Firewalls, Power surges	Screensavers Passwords
02		Phase 2 Implementation strategy	Concerted, and co-ordinated	Resources: 30-50 Million over 3 years.	
03	General practice	Functioning of the business	System ‘reliability’	‘allocated /identify accountabilities (practice staff & service providers)	
03		Financial incentive model Practice accreditation	Backups/ restorations	Viruses/Firewalls/ Hardware, Spyware	
04	General Practice	Financial incentive model Functioning of the business	Articulation of (i) IT policies (ii) disaster recovery plan; and (iii) email and Internet at the individual practice level		

KEY INFORMANT EXPERTS IN GP COMPUTING	HEALTHCARE SYSTEM NODE	FIT	1 ST PRIORITY	2 ND PRIORITY	3 RD PRIORITY
05	General Practice	Financial incentive model Practice accreditation Privacy legislation	Practice-specific IT Policies (incl passwords and screensavers)	backups	Viruses, firewalls
06	General practice/ research	Financial incentive model	backup	Practice IT coordinator	Viruses, firewalls
07	General Practice accreditation	RACGP	Viruses, spyware, firewalls	Disaster plan	Backups, restoration
08	GP Medical Software Industry	synergy	Functioning (i) backups; (ii) screen savers; and (iii) passwords	Viruses, firewalls, power surges	Practice-based organizational documentation: IT Policies (inc disaster plan) and practice IT coordinator role
09	Medical Software Industry	synergy	Backups, viruses, firewalls	IT policies and Practice IT coordinator	Power surges
10	Commonwealth Government	Towards national privacy standards	Privacy		
11	Commonwealth Government	Towards national security standards	Archiving of patient data, use of e-signatures, viruses and firewalls	security policy developed for/by each practice	
12	Commonwealth Government	Towards national security standards	Security processes in place in all practices (incl framework for responsibility) Access rights (password management) – role based controls	Robust IT systems in place	Consumer Record authentication for use by provider
13	Commonwealth Government	Towards national security standards	Comprehensive IT security policy in place (incl privacy, email, disaster recovery) for each practice	In-house quality assurance processes documented for (i) data storage (archiving); and (ii) access to archived data for each practice	

KEY INFORMANT EXPERTS IN GP COMPUTING	HEALTHCARE SYSTEM NODE	FIT	1 ST PRIORITY	2 ND PRIORITY	3 RD PRIORITY
14	Divisions of GP	GP change management support infrastructure privacy	Upskilling practice staff	Backups, screen savers, passwords	Viruses, firewalls,
15*	State Government	Synergy: Commonwealth – state systems interface	Quality assurance accreditation/authorisation of IT security service providers to general practice	Education and training: user ‘competency-based’ framework (GP and practice staff) and service provider (technical and support)	

* It was thought to be valuable to note what one state government expert (who participated in a less comprehensive interview) considered to be the priorities summarised in this matrix along with the views of the main study participants.

4.3.9 Managing security risks in general practice: identifying ‘cost effective’ strategies and solutions

*I think the biggest technical risk is that all **these things cost time and money, and so won’t be done.** (GP, interview transcript: original emphasis)*

Experts in the study were asked to suggest what they considered to be *cost effective* strategies for improving IT Security in general practice. (Please note that there was no discussion as to the meaning of ‘cost effective’ between any of the study participants and the field officer.)

Commonwealth Government experts generally promoted the use of more education and training as well as large scale and generic technical solutions referred to as *pipes* and *channels*. On the other hand, experts who either worked directly with, or currently practiced as GPs, generally re-iterated the need for *practice-based, micro* implementation strategies and *on the ground ... change management* solutions. These differences in approach highlight the need to consider the context within which practice occurs as central to the implementation of guidelines. Previous social science research claims that practice is not identical to theory, rather that one of the most significant differences is that clinical practice occurs in particular situated contexts (Suchman, 1987; Berg & Mol, 1998; Mol, 2002).

Experts in GP computing were then asked to offer suggestions as to ‘the best and most cost effective way’ the nominated organizational and technical as well as the other interviewee-nominated potential security risks could be mitigated. The interviewer encouraged respondents to consider their responses, (i) in terms of how much their solution would cost particularly in terms of GP or practice staff time; or (ii) perhaps in dollar terms, if they were able to do so.

From the GPs’ perspective, the most cost effective way to address security risks in the practice was to get *everyone in the practice sharing information and talking about it*. As one GP stated, *The most cost-effective solution is to have everyone communicating and operating together as a team and understanding about IT stuff. That’s where you get your real break-throughs in the process. Then coffee isn’t spilt, operating systems aren’t degraded by people doing the wrong things ... promote a*

culture of acceptance of the need to integrate IT usage in General Practice at all levels of the organisation. Not just the bookkeeper, not just the front desk, but the doctors on their desktops have all got to be convinced that there's a benefit in having IT.

The details of what experts in the study considered to be 'cost effective' strategies for managing nominated and other risks are listed (column one) in the following series of tables. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. This migratory approach has been initiated in order to present the experts' proposed strategies in as useful a way as possible should their suggestions be drawn on during future discussions between the Commonwealth, GPCG and other stakeholders when negotiating a national framework for the implementation phase (column 4).

4.3.9(a) Managing the risk: IT Policies in the Practice

It seems to me that it's meaningless to talk about implementation of IT Security until you've actually got a policy that outlines what it is that you're trying to do. (GP, interview transcript)

Work with the practice as a whole... not just the doctors ...to identify IT Security procedures and sustainable solutions (GP expert practice accreditation, interview transcript)

Enshrine it as a College standard and make sure its built into practice accreditation (Government expert, interview transcript)

There is a call for a nationwide, unified policy published by a body such as the GPCG...devising such a policy may cost the value of two face to face meetings of possibly five or so qualified people...in terms of implementing the policy...it's the cost of teaching your own practice staff, and that depends very much on their own background and knowledge. (GP expert, interview transcript)

Table 7: Managing the risk (IT policies in the practice): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
A standards approach which can be customized to every practice	GPCG/RACGP	College Standards & Practice Accreditation Model	
National IT Security Policy for General Practice	GPCG/Monash University	Practice Accreditation Model	
IT Policies (what needs to be done) template with a responsibilities framework (who) adapted for <i>typical GP</i>	GPCG	Financial incentive model Practice Accreditation Model	

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
<i>circumstances</i>			
'cultural change' in the practice	GPCG/ Divisions of General Practice IM Officers and other service providers	Incorporation into the IT Standards and the College's Standards documents so it becomes part of practice accreditation for the next cycle Built into a three year GPCG strategic implementation framework	
Upskill your own current staff	Practice principal/s	Practice-based approach	
Provide training for practice admin staff	Divisions		
Write a sub-policy on minimizing the risk of theft on and off site of portable equipment (eg laptops)	GPCG & experts		
Tie practice staff development in IT security to performance review and employment contracts	Practice-based		
Make compliance with a separate security policy a condition of employment (for the practice)	Practice-based		
Using Division of GP IT Officers as 'Commercial Contractors'	Commonwealth Divisions		
Articulation of an IT Policy template (var technical implementations incl web-based)	Standards Australia (technical writer)		Anticipated cost: \$30K Turnaround time: 4 months Implemented & disseminated by GPCG/Divisions Network HIC State Business Development Officers (4-5 per State)
Dissemination of an IT	GPCG/Divisions		

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Policy template	Commonwealth HIC		
Specify access controls for the system (who can “do” what)	Practice-based		
Specify access controls for the system (who can “see” what)	Practice-based		
Specify system access controls and protocols for when non-practice technical support visit the practice to work on the system	Practice-based		
Specify access to patient data controls and protocols for when non-practice support and other service providers visit the practice.	Practice-based		
To raise awareness, incorporate PKI individual token management into the practice Policy and Procedures Manual	Practice based	HIC Divisions	
Facilitate the promotion of the National Health Privacy Code in general practice ‘to satisfy the demands of the Privacy Act’.	Commonwealth Govt	Commonwealth sections & GPCG	
Document procedures for ‘handing over’ and ‘recording’ informed consent	Practice-based	Commonwealth sections & GPCG	
Education campaign (component of a wider implementation strategy) targeted at general practitioners as well as patients to facilitate the cross-	Commonwealth sections & GPCG		

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
sector adoption of a generic 'privacy regime' (National Health Privacy Code)			
Web-based and targetted education/training interventions 'to convince' GPs (particularly small practices) that adopting privacy, security and patient consent protocols is 'sound practice'.	GPCG Divisions Commonwealth privacy and other sections		
Establishment of a national steering committee to oversee the coordinated development of privacy-related 'educational tools'	Commonwealth & GPCG		
Wider distribution of Commonwealth privacy guidelines and pamphlets (available in electronic and hard copy)	GPCG to oversee Divisions to promulgate		
Workshops for GP on 'IT: the interplay between consent, confidentiality and patient access rights'	Commonwealth sections & Divisions		
Patient Information Leaflet as an Appendix to an IT Security Handbook for GPs, for GP to distribute to their patients detailing the 'security' of their computer work practices and compliance of these with privacy principles (Commonwealth Legislation)	Practice-based	Commonwealth sections & GPCG Divisions	
Carry out research into GP attitudes related to the introduction and adoption of IT Security	GPCG & Higher education sector & Divisions		

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Guidelines **			
Preparation of breaches of privacy-related case studies for dissemination is association with IT Security education and training materials ***	GPCG & contractors		
Review of software accreditation systems in the context of privacy	GPCG, Commonwealth, MSI		
Articulate and disseminate guidelines for how to go about the process of developing an IT Policy for the practice 'a guideline for how to prepare the guidelines'	GPCG & Divisions	Financial incentive model	Change facilitation, information dissemination role through Divisions
Convening of an 'industry-based' IT Security working group Build IT Standards into College Standards	RACGP, GPCG, other GP representn organizations & the AMA	synergy	
Adopt a GP-GP professional peer approach for education and training	Practice accreditation peer surveyors Divisions		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

** Recommended by a Government expert in GP computing, not the research team.

*** We recognize the inter-dependancy of IT security and patient privacy and confidentiality. However, for the purposes of this report, strategies associated privacy are included on the basis that the expert expressly recommended were incorporated into GP education and training materials around IT security.

GP non-adherence to any proposed IT Security Guidelines was noted by a number of experts in the study as a major risk in itself, and hence the need to incorporate the adoption and use of IT Security guidelines in general practice in a broader change management framework such as *industry standards, financial incentives and practice accreditation*.

4.3.9(b) Managing the risk: Practice IT Coordinator

... However, just having a policy sitting on a shelf, isn't having a policy (Government expert, interview transcript)

Reward the culture of wanting to be interested in IT within the practice (GP, interview transcript)

The cheapest way is to upskill your current staff ... if certain key staff have got aptitude ... pick them out for training ... we all need to be upskilled...If you can target one person to take on the role of practice IT person and give them more advanced training then that's fantastic... whether it be a practice manager or a nurse or an administration person or even a doctor. (GP-5 doctor practice, interview transcript)

A number of experts raised the issue of the increased cost to the business of appointing an additional member of staff (the Practice IT Coordinator) to the practice, and suggested that it was more *workable*, where possible, *to review what current staff do and to upskill one of them if you think they show potential*. However, such a suggestion does not take into account the *need for the doctors to know where they're going with this...and what needs to be done*. Furthermore, GPs, have also in the past been able to draw on Divisional IT support and expertise. However, as one informant suggests, *in the absence of [such] Division support, most GPs simply aren't prepared to pay the going hourly rate to bring in a commercial provider*.

For most experts in this study, facilitating the initial appointment of someone who took on the role of Practice IT Coordinator was the most difficult potential risk and general practice organizational development conundrum for which to find solutions. Moreover, the reality is that any auspicing of such an appointment, or task re-allocation, is essentially at the discretion of the business owners (the principals) of each practice.

Table 8: Managing the risk (Practice IT Coordinator): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Support practice - based decision making at to whether to (i) upskill inhouse; or (ii) out-source the role	Divisions/ practice accreditation agencies	Practice Incentive Program	
Explore 'groups of GPs (multiple practices) setting their own standards and sharing an IT Coordinator'	GPCG/DoHA IT security best practice light housing	Practice Incentive Program	

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
	Division/state government funded equivalents		
Upskill current practice staff (GPs & other staff)	Practice principal	Practice-based	
Rewarding current practice staff (GPs & others) who 'take on learning about IT by financially looking at salary packages, modest salary increments	Practice principal	Practice-based	
Provide training for practice admin staff	Divisions, other service providers	Practice-based	
Component of implementation of IT Security Policy	Divisions of General Practice and other service providers	Practice-based	Dependency: articulation of a GP IT Policy
Skills assessment proforma (a structure-pre-employment interview) to access baseline knowledge	GPCG/Divisions/HI C IT-savvy practice GP	Practice-based	

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

Some solo practitioners are early adopters and capable users of ICTs. However, previous Divisional and other surveys indicate that many are not. Solo practitioners (who currently make up around 20-25% of practitioners in Australia) were identified by a number of experts in the study as needing targeted support in how to address the issue of nominating someone within the practice who's role it was to be the Practice IT Coordinator, and conducting the IT Security tasks associated with that role. Experts put forward a number of possible solutions. These included Divisions have a backup system or advise on the backup process in place; and solo practices forming *IT Security Practice Networks* where one person is employed to look after a number of practices.

4.3.9(c) Managing the risk: Practice Disaster Plan

*A lot of people **wouldn't even think about** half of the potential disasters in an IT sense that could happen in a practice, because **they just don't know** what they are.* (medical software expert, interview transcript: original emphasis)

...start somewhere...and build it up **one bit at a time** (Government expert, interview transcript: original emphasis)

...standards, accreditation, proformas... (Government expert, interview transcript)

Linking having a practice disaster plan to practice accreditation was seen by a number of experts to be instrumental in stimulating not only the articulation of such documents, but the practices that go with it. Furthermore, the *decay rates* of specific elements incorporated into such a document should be considered from the outset. Whilst the technology itself may change, the principles behind the use of the technologies are unlikely to change at the same rate. In this context, a number of experts suggested that for a practice to develop a comprehensive disaster plan from scratch, of which IT Security is a sub-set, may involve a 2-3 year in-house process.

Table 9: Managing the risk (Practice Disaster Plan): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Writing of a generic principles document	GPCG& contractors	Practice Incentive Program	GP IT Security Program funding to facilitate PIP targets Available through GPCG online ClearingHouse Role for Divisions of General Practice.
Compile a series of template scenarios for dissemination associated with the risk of commonly used email software impacting negatively on the practice's computer system	GPCG experts & contractors	Practice Incentive Program	GP IT Security Program funding to facilitate PIP targets Available through GPCG online ClearingHouse
Development of a generic Disaster Plan template (var technical implementations suggested)	GPCG/Standard s Australia/HIC (technical writer)	Practice Incentive Program Practice accreditation	GP IT Security Program funding to facilitate PIP targets Available through GPCG online ClearingHouse
Facilitate the uptake of a generic Disaster Plan template	Divisions of General Practice	Practice Incentive Program	GP IT Security Program funding to facilitate PIP targets
Articulate a series of commonplace lesser IT disasters scenarios (e.g. spilled coffee on keyboard, stolen laptop, server not starting) along with some	GPCG experts & members	GP IT Security Program funding to facilitate PIP targets	GP IT Security Program funding to facilitate PIP targets Develop collaboratively online (e-list) Proposed dissemination however, primarily paper-

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
general suggestions as to how the rectification of these should be approached			based (not email, and not mail out) and in person ('on the GP's lap') Available through GPCG online ClearingHouse Dissemination and facilitating practice-based change management role for Divisions of General Practice.
Divisional support case studies/success stories	GPCG/ADGP	GP IT Security Program funding to facilitate PIP targets	Available through GPCG online ClearingHouse and ADGP information channels
Clarifying the legal issues re. 'locus of responsibility' (owned, shared or transferred) and the 'locus of control'	Insuring and litigation agencies & GPCG, RACGP & Divisions		
Incorporation of IT security into accreditation database		Practice accreditation	
Expert panel to create a template with different scenarios, practice sizes, network types	GPCG experts & contractors		<i>Divisions to promulgate</i>
Practice 'disaster plan' drills	Practice-based		
Open and non-moderated discussion of such on both expert and other mailing lists	GPCG e-list Divisions e-lists		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicings organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

The point was raised that disaster plans are quite specific to a practice and their circumstances. Just handing out a generic disaster plan won't work because people haven't thought it through and realised what the issues are. Therefore it was argued that the articulation of disaster plans occur within the context of the practice accreditation model. To illustrate the pragmatic approach adopted by one GP who facilitated the change within their own practice: As you move towards establishing the protocols within your practice, or adapting the generic protocols to your practice, then you address the specific

issues around disaster plans. But you see again, the real thing with disaster planning is not so much the plan but the thinking that's gone into it. So, people need to be helped to recognise what are the issues they need to think about.

Experts referred to the *principles of disaster planning*. One GP drew a parallel with the planning around managing and downloading pathology reports within the practice: *There's a whole series of questions that start with the result being in the pathology laboratory and how do you get it into the practice record. And where is it possible for mistakes to occur; how is it possible to know that mistakes that have occurred, what can you do to notify people that mistakes have occurred, what can you do to reconstruct the pathology record and what can you do to make sure that there aren't any gaps in the system.*

In terms of IT security, one GP suggested that a bottom line disaster plan is knowing how to immediately deal with the front desk issues such as when patients come in and computers aren't up... I mean the disaster is when the computers aren't working. Hopefully [the patient and other records are] retrievable but the immediate problem is to get patients seen to, get bookings made ... have money taken and invoiced and receipted etc.

4.3.9(d) Managing the risk: Email and Internet policies

*Although it seems like such a low priority to most GPs at present, **you do need something** to protect yourself and the organisation from liability or other issues... you do need a policy and it has to go in your standard Policies and Procedures Manual... that's **to protect you** if your employees are in the habit of, say, downloading child pornography and yet its stated in the Manual that you're not allowed to download anything offensive, then the employer and the site of employment are better covered from issues that arise from that. (GP, original transcript: original emphasis)*

Table 10: Managing the risk (Email and Internet Policies): summary of experts' proposed strategies

STRATEGIES	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Adopt a <i>common sense approach</i> of what you actually put in' the e-communiqué.	Individual locus of control	GP organisations	
Restricting GPs to only providing certain sorts of information over the Internet.	Commonwealth	Legislation	
Circulate a short discussion paper for GPs [and other clinicians] related to the intrinsic question about whether you can have a patient consultation within the context of an Internet interview.	GP organisations: peer to peer discussions		
A policy to go in the practice's standard Policies and Procedures Manual	Practice-based	Divisional support	
Security policy around exchange of patient prescription b/w health care providers	GPCG & DoHA & RACGP, AMA, HIC		
Education re doctors talking to patients over the Internet	GPCG experts & contractors		Divisions of General Practice
Raise awareness of potential breaches of confidentiality as the result of remote access by 3 rd party IT service providers	GPCG experts & contractors		Divisions of General Practice
Develop an individual PKI token management strategy for each practice	Divisions HIC		
Develop and regularly review progress being made towards the introduction of PKI/other encryption within the	Practice-based Division-based HIC-based		

STRATEGIES	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
practice			
Provide a managed service with Broadband connections (built in firewall)	Commonwealth & major service providers		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicings organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

Experts generally agreed that both email and Internet use policies...*to start with, would need to be customized for each practice and the staff who worked there and that for the majority of practices, would require a lot of hand holding.*

4.3.10 Managing technical risks

Acts of God... the blame someone else factor (GP, interview transcript: emphasis in original)

The best long-term cost-effective way to deal with IT management ... is to have one supplier ... I strongly advise people to have one supplier for as many of the IT needs as possible. That means hardware and software. So that then, if a problem occurs you have one person to go to and point the finger at. Otherwise, if you're buying your hardware from one person, software from somebody else, consultancy services from somebody else then the finger-pointing and blaming will go around and around ...and you will not get your problem solved. No-one will take the responsibility.' (GP, interview transcript: original emphasis)

4.3.10(a) Managing the risk: Back-ups (restorations)

Ensuring appropriate backup routines and checks...is bread and butter stuff for Divisions wanting to go down the 'looking after the IT security needs of practices' line (Medical software expert, interview transcript)

Table 11: Managing the risk (backups and restorations): summary of experts' proposed strategies

STRATEGIES	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
General information leaflet for GP about the efficacy (reliability) and cost of various backup	GPCG/medical software industry experts		

STRATEGIES	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	<i>GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES</i>
strategies			
A written practice policy and tools	Practice-based		
The articulation and promulgation of a specific document addressing the privacy and security issues and recommended procedures around doing, archiving and restoring backups	Commonwealth Government 'sections' and GPCG experts		
Re/allocation of additional resources within Divisions to enable this support role	Commonwealth/ ADGP		
Provision of a managed service (Broadband)	Commonwealth & private sector		
Divisions as Application Service Providers (with thin clients in the practice	DoHA & Divisions		
5 point backup plan Information brochure containing (i) which devices should be used; (ii) how often they should be used; (iii) which data format should be used; (iv) how backups should be secured; (v) how often backups should be refreshed	GPCG & experts		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicings organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

4.3.10(b) Managing the risk: Screen savers

Table 12: Managing the risk (screen savers): summary of experts' proposed strateg

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Cultural change within the practice	Practice-based	Divisions Practice accreditation Medical and other software providers	
Raise awareness - generally	Practice-based	Gpcg Divisions Commonwealth (privacy section) Medical and other software providers	
Incorporate the articulation of the appropriate use of screen savers into practice (and related) quality assurance processes and standards	Practice-based	Practice accreditation Divisions	
Education and training	Practice-based	Gpcg Medical and other software providers Divisions Commonwealth (privacy section)	
Raise awareness amongst users of any software functions that initiate screen savers engaging	Practice-based	Medical and other software providers Divisions Commonwealth (privacy section)	

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicings organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

And, and the micro-level in the context of the adjusting the computer-user interface *these just have to be set up...in such a way as they don't disrupt you all the time...they just kick in after a certain time....so people have to find out what their own time span is so that they don't get annoyed by the screen saver and simply switch it off.*

4.3.10(c) Managing the risk: Passwords

Passwords are cheap...but they're not going to be used (GP, interview transcript)

Although passwords are easy to issue, encouraging GPs and staff working in Australian general practice to use this form of access control may prove more difficult to achieve. As one GP expert in the study suggested, in general practice, *it may be easier to manage authorised access to patient and other information in terms of something you own, something you have, or something you are.*

Table 13: Managing the risk (passwords): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Nominate one person in the practice as 'holder of the passwords' - the practice management software, the accounting software, the clinical practice software, email software.	GP principal Practice-based strategy		
email software: a general policy that collates and stipulates that the generation of additional passwords must be authorized by the practice manager	Practice-based approach		
Raise awareness using case studies involving breaches of confidentiality	Practice-based approach	GPCG Clearing House GPCG/ Commonwealth & MSIA	Dissemination role for Divisions
Signing off on the practice security policy	Practice owners (principals)	PIP	
Raising awareness of what a good password is	Practice-based		
Raising awareness of what NOT to do (eg yellow post it stuck on monitor	Practice-based		

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Promote fun strategies within the practice for coming up with non-alpha-numeric and (which tend to be easily forgotten) other language passwords (which tend to be miss pelt)	Practice-based		
Promote fun strategies to encourage memorization of passwords by individuals (although centrally recorded somewhere else)	Practice-based		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

4.3.10(d) Managing the risk: Malicious code and firewalls

Firewalls are cheap. There is no excuse for not having one. Get one or perish. They're cheap. \$400 or \$500... there's absolutely no excuse for not having one. (GP, interview transcript: original emphasis)

Firewalls and viruses are high maintenance...once installed...they're an ongoing support issue (Government, interview transcript)

We don't see the case studies of the failures, we [only] see the case studies of the positives and I just wonder if sometimes seeing the disaster story might just help people to stop and take notice that it might happen to me? Some horror stories need to be told... (GP, interview transcript)

You also need someone with the knowledge...someone qualified that also has their own professional indemnity insurance (Government expert, interview transcript)

Table 14: Managing the risk (malicious code and firewalls): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Demystification (through simple description of component parts) of what a hardware firewall actually is	Divisions		
Every practice workstation connected to the Internet, and even workstations that aren't connected to the Internet, should have virus checkers that are updated at least twice a week	Practice-based	Practice Incentive Program	
Dissemination of virus disaster case studies	GPCG/HIC & contractors		
Adapting the standards-based security handbook (17799) to the health sector	Commonwealth/ Standards Australia (technical writer)		Anticipated cost: \$30K Turnaround time: 4 months Implemented & disseminated by GPCG/Divisions Network HIC State Business Development Officers (4-5 per State) [note: overlap with content of IT Policy]
Facilitate out-sourcing of online communications to a managed service	Not nominated		
Dissemination of information about spyware freeware websites	Not nominated		
Recommend to general practice a range of hardware firewall products	GPCG & contractors Divisions		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected

from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

Mitigating the risk posed by lack of firewall may have different solutions in the rural setting as compared with metropolitan areas. Furthermore, the appropriacy and efficacy of the technical solutions may vary depending on the size of the practice, the extent to which the internet is used by the practice, as well as its geographic location and the provision of services (such as dial-up and Broadband connections) therein.

A number of experts noted the reluctance on the part of Divisions to *support or empathise with one particular large scale ICT service enterprise over another*. It was felt they were looking for guidance from the Commonwealth in this regard. Furthermore, the hardware and other costs associated with introducing and maintaining a range of different solutions also need to be considered. The preparedness of general practice to invest in such things varies considerably.

4.3.10(e) Managing the risk: Power surges

There are no real cost-effective solution for power surges (GP, interview transcript)

Table 15: Managing the risk (power surges): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Installation of server UPS	Practice-based	Practice Accreditation Practice Incentive Program	
Clear strategies in place for how to manage patients	Practice-based	Practice accreditation	
Write up real life scenarios (e.g 'My router got cooked by a thunderstorm.'	GPCG & contractors		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

Experts considered installing a UPS *a must-have in every Australian practice ...whether you're in a metropolitan or rural area*. A more significant issue for practices in rural settings, however, was that *of longer power outages and whether [a rural practice] needs a higher powered UPS with some sort of generator is a separate issue*. Cost-sharing with the *power providers or the [particular] government that's providing services to patients* was suggested by GPs in rural practice. They argue that, *power runs more than just our information systems, it also runs our monitors and life-saving equipment... it's a bigger issue than just IT*.

4.3.10(f) Managing the risk: Encryption of data transmission

The debate in relation to managing this risk predominantly revolves around two core issues. Firstly, the technical specifications of the most appropriate messaging and encryptions systems (on which the authors of this study are unable to provide expert comment, and which is also the subject of another GPCG report to be released shortly). The GPCG, in collaboration with other GP representative bodies, is currently reviewing current options such as the HIC PKI system (currently free to general practice) and alternative solutions, some of which are based on open source encryptions. It is important to note that there was a preference expressed by a number of GPs in this study for, *a non-proprietary solution that they then won't have to pay for and lock into*.

The second debate revolves around who will be responsible for promulgating the actual use of digital certificates associated with the Commonwealth's current Public Key Infrastructure (PKI). This issue is raised on the reasonable assumption that the implementation of PKI and the digital certification implementation process that goes along with it is likely to continue in its attempt to work towards adopting *industry standards*.

Although it has been estimated that over 6,000 digital certificates have been generated for and hence now exist in the general practice sector, as one Government expert infers, *the problem is that very few people in general practice are actually using them*. The development of education resources and protocols was suggested. However, a number of experts in the study referred to *a general reluctance on the part of many GPs to accept IT Security and other advice from the Health Insurance Commission*. Moreover, although the HIC has employed a number of state-based field officers, there still appears to be lack of clarity or *a demarcation* as to which agencies are to be primarily responsible for facilitating the actual use of certificates in general practice. This is likely to be due to the lack of funding targeted at facilitating *on the ground* support. Divisions and their IT personnel were once again raised as possible facilitators and *whose advice may be more welcome*. Understandably, government experts interviewed for the study were very clear about their position on this matter: *The main thing is that the Government has chosen PKI and we've just got to get out there and do it...the more that are on [the infrastructure] the more will use it*.

Table 16 Managing the risk (encryption of data transmission): summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Education and Training in PKI for GPs re (i) individual (hard) token and (ii) practice token (floppy disk) access, management and storage	HIC Divisions of GP		
Articulation of a PKI-related protocol to be included in the Practice Policies and Procedures Manual	HIC Divisions of GP		

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI- STAKEHOLDER APPROACH.	<i>GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES</i>
Articulation of a practice policy for the storage of encrypted data	HIC Divisions		
Articulation of a practice policy for the storage of unencrypted emails intended for transmission, including the storage of digitally signed messages	HIC Divisions		
Each practice carrying out of 'routine audit logs to ensure adherence to documented security protocols are being adhered to and any breaches detected'	Practice-based		
Increase the GP use of HIC online	HIC Divisions		
Lessons to be learnt from demonstration project such as ADGP's HealthLink	ADGP		
GP peer visits to PKI demonstration practices	HIC Divisions		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicings organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

4.3.10(g) Managing other technical risks

Table 17: Managing other technical risk: summary of experts' proposed strategies

STRATEGIES *	AUSPICE	FIT INTO A NATIONWIDE COORDINATED MULTI-STAKEHOLDER APPROACH.	GPCG PHASE TWO IT SECURITY PROJECT IMPLEMENTATION MAPPING: SEQUENTIAL, PARALLEL DEVELOPMENT AND/OR DEPENDENCIES
Ensuring practice 'intra-operating system consistency	Practice-based		
Supporting GPs with developing an IT budgetary process	Authorized service providers		
Education re. spy-ware management	Divisions of GP and other service providers		
Occasional expert articles in IT sections of Medical Observer (e.g. how to fix up firewalls, fix up viruses, backups, DVDs	GPCG & members		
Occasional expert articles 'pros and cons' of doing things in a particular way	GPCG & HIC & contractors\	GPCG online Clearing House	Co-ordinated dissemination approach by Divisions of GP and HIC field support personnel
Development of case scenarios and best practice guidelines	GPCG & RACP & contractors		

* The details of what experts in the study considered cost effective strategies for managing nominated and other risks are listed in column one. The auspicing organisation/s listed in column two have been nominated by the experts. Where data collected from experts clearly suggested 'a fit' of the proposed strategy into a coordinated multi-stakeholder approach, an entry has been made by us in column three. However, where this is less apparent, or where we considered that the proposed strategy required further consultation with the nominated stakeholders no entry has been made. Completion of entries in column four is the subject of negotiations between the Commonwealth, the GPCG and other stakeholders.

(i) *IT Assets Register*

For a range of reasons, as a precursor to any IT Security change management approach, practices will, in the first instance, need to collate (and periodically review) an IT assets register if they have not already done so. Experts in the study recommended that, as a minimum, that the register documents *what you have, where it is located or stored, and how its integrated* and then is reviewed once or twice a year. Such templates are readily available. However, to date they have not been made generally available to general practice. On expert suggested that the College would be the appropriate conduit for reviewing existing templates and adapting them, in the context of standards, for general practice.

(ii) *Systems Service Report*

The need to attend to the maintenance of the practice computer system/s on a regular basis was suggested by a number of experts, with a simple document titled *Practice Systems Service Report* being the means by which this process is documented and monitored. Along with this, it was suggested that, *all the telephone numbers of who you should ring when something goes wrong* should also be inserted into the front of this document for easy access and reference by practice staff.

(iii) *Upgrades*

GPs in the study generally agreed that, *upgrades should be taken with the utmost care and there should be a culture of wait and observe deciding (i) whether they're necessary and (ii), if they are necessary, are they safe?*

(iv) *Physical security: corporate culture and the little things*

GPs also supported the notion that practices, *must increasingly adopt a corporate culture where everybody, that includes the most junior reception staff, understand a little bit about computers. They realise you shouldn't be drinking coffee over the monitor, and that you must turn the monitors off at night because then they can catch on fire, you must not accidentally kick the on button and off button on the server, you mustn't touch things that are operating... lots of little things like that.*

(v) *Access security: initiation and termination of access rights*

As one GP in the study suggests, *the whole issue of how you lock down your database that a disaffected doctor or staff member can't distribute it, is an important issue. And that's largely an access issue, so, yes, there's stuff around access rights but there's also a need to be policy around when you terminate those access rights. How you do it in a way that it stops people getting into it. You don't want anyone external coming in without permission to fiddle with your system...and you want to keep your confidential information confidential...be it your own financial records or be it patient records.*

(vi) *Clinical Software*

The technical implement of a *privacy auditing function* in clinical software was suggested by one expert in the study. However, they were not one of the medical software experts recruited for the study. It was proposed that software could be developed to *embody privacy upgrades and periodic prompts could alert GPs and their staff that it was time to re-view their in-house privacy protocols and procedures.* Furthermore, it was mooted by another GP that *clinical software vendors may well develop and offer general practice security solutions which compliment other GPCG/DoHA organisational change management initiatives*

4.3.11 Other barriers

One expert suggested that one important barrier was the current *lack of capacity* on the part of Divisions of General Practice to take on a practice support role in relation to improving IT Security in general practice: *They just lack the manpower [sic], ... but most importantly, they see their role as being education providers around how to use [name of clinical software] rather than organisations that are assisting people in a generic sense to manage the IT systems of the practice.*

4.3.11(a) Translating privacy legislation for general practice

According to one Commonwealth Government expert, duplication of privacy legislation in some states is *leading to confusion for some GPs, especially those who [are employed] by the public sector*

...they have to [subscribe] to one set of privacy rules in their own organization and another when they go and do locum work... in a hospital, or an Aboriginal medical service. Trying to translate privacy [legislation] into IT Policies, and actual practice, especially if the uptake of IT has only been recent [as in Australian general practice] was considered by GPs in the study to be quite difficult, as the following quote illustrates: Obviously you want your [practice's front desk] staff to be able to do all the billing for patients. So how do you ensure that your practice's [paper-based and electronic] patient clinical notes are kept separate from admin data?

4.3.11(b) PKI

On the ground problems [with computer systems in general practices] associated with driver installation are common ...computer system configurations... lack of patching... not using the latest version software were identified, by experts from the government sector as barriers to the use of a public key infrastructure by general practice. However, some non-government experts in the study suggested that there is *a[n alternative and] better technical solution for doing this.*

4.3.12 Other enablers

4.3.12(a) Patient rights and confidentiality: towards a policy-based approach?

Interviews with experts suggest that GPs are getting advice from *medico-legal units which is really very legally-based rather than policy-based, and rather than being based on the reasonable expectations of the ordinary consumer...* [the current focus] is on *what if this had to stand up in court?*

4.3.12(b) Barrier or enabler?

One consumer rights advocate interviewed for the study suggested that *some consumers are very aware of privacy and security and consent protocols. They understand the language and how it impacts on them far better than the wider general practice community at present.*

4.3.13 Change management implementation models

*There's a big difference between policy and implementation...educating GPs about the policy will be crucial...accreditation standards are a bit of a stick...but what we really need to do is to get people to **understand the reason why they need to do it...and a bit more about the how.*** (Rural GP, interview transcript: original emphasis)

The following series of change management models is a summary of the recommended change management approaches to improving general practice IT Security proposed and expressed by experts in this study. The further integration of these and any other relevant models into a 'GP IT Security Program' delivery framework is beyond the scope of this study.

4.3.13(a) The incremental model

One expert suggested that the most likely intervention model to work was one build on principles to, *the National Prescribing Services' medication management model which in essence says that individual Divisions of General Practice will be funded by a national coordination body [such as the GPCG] as the fund holders. ... in order to undertake certain activities, such as [engaging] and a [nominated] proportion of practices within the Division to upgrade their security systems [within a specified timeframe].. Typically with the NPS, it's over twelve months and the sort of percentages they're talking about are accessing 50% of practices... we do need to be clear [from the outset] about what is expected in terms of actual performance indicators (outcome measures) ... 'cause I think it's unrealistic to expect all Divisions to have 50% of [their] practices in any particular period of time, with ... [all having] secure arrangements at the end of 12 months. An incremental model that says*

something like, "that 50% of practices have been contacted in a 12 month period moving over a period of three years to significant uptake" ... however you define significant ... but you know say looking at say 75% adoption over three years, would strike me as being a practical and sensible way. And it's achievable way of going forward with it. But the cost for [Divisions] to do something like that is probably between \$30 and \$50 million over a three year period.

4.3.13(b) The financial incentive model

This was raised by experts as a *pertinent issue for the Commonwealth Government particularly in relation to the Practice Incentive Payments* [such as those used previously to encourage the uptake of IT by GPs for clinical and practice management purposes]. A number of experts who were interviewed suggested that the possibility of such a financial incentive would help *move things along*. However, one GPs in the study referred to such a *one off* incentive as only having *limited impact*: *After all these years, I'm unimpressed with single [incentive] payment models. I don't think it fits normative human behaviour for most people, and that includes GPs ... most of us ... are much more likely to be more impressed with payments that go on over three or four years so that our behavior becomes more efficient ... gradually towards working in the way that's being promoted.*

Experts in the study agreed that addressing IT Security in the practice is a significant business cost. And although, *the overall dollar cost to practices would increase* with financial incentives such as the Commonwealth Government's practice incentive payments, GP would be more likely *to bare the additional cost in order to get other benefits such as improved efficient and better patient health outcomes.*

4.3.13(c) The General Practice Accreditation Model

Practice accreditation was seen as one of the 'major drivers' for improved IT security. As one informant suggested, *GPs get dragged kicking and screaming into [practice] accreditation but only see the value afterwards. The risks become clearer to them as they actually go through the process.*

4.3.13(d) The Divisions of General Practice (practice-based) support model

References were made by all experts to the pivotal role played by Divisions [albeit to a greater or lesser degree in the case of individual divisions] in facilitating the introduction and use of information and communication technologies in general practice. As one GP expert summarised, *most general practices wouldn't be where they are today without Divisional involvement and support*. Furthermore, it is likely, as another expert suggests, *that of the 15 or so organizations that represent GPs interests ... that only a few are likely [to get involved] with promoting IT Security in general practice in a meaningful way*. One expert suggested that the urgent need to address IT Security in General Practice was *very good justification for bringing Divisional IT Officers back*. He goes on to suggest that *they could be funded as a separate part of the Divisional movement*. Furthermore, *not leaving it to each Division to do from scratch* was reiterated by a number of experts, along with the notion of *some national co-ordination from someone like the GPCG... so everybody's not reinventing the wheel like they've done in the past, and like they're doing now*.

4.3.13(e) The 'push – pull' HIC Online Model

Packages such as MedicarePlus exists and has *HIC Online built into it*. As one expert in the study speculated, the role of facilitating change (with a view to improving IT Security in general practice) may well be increasingly *taken up by HIC online*. This expert further argues that, *if you're going to force a practice to go online, you should really send someone around to make sure that when they do it, it's all safe and secure*. One expert suggested that *the Commonwealth HIC set up a unit to support general practice directly* [in the context of Medicare rebates for GP services] *and try out some GP [computer] systems directly*. However, the current perceived GP *lack of trust* [of the HIC] *might be very low*. As another GP expert suggests, *GPs might not want anybody who works for the*

Commonwealth coming out into their practice...it's a question of who the GP currently has confidence in...it might be better having the Division IT Officers or commercial contractors come in.

4.3.13(f) The (education and training) information dissemination model

Based on feedback received from experts in the study, the development of an *effective and coordinated information dissemination strategy* is integral to the success of an implementation strategy intended to improve IT security in general practice. As one expert put it, *there's plenty of neat stuff that's already been done that has never made it into the GP's brain because the [information] distribution mechanism wasn't thought through enough at the beginning.* Divisions were considered *ideally placed* to do this. Publications such as Australian Family Physician along with GP magazines were also considered appropriate and effective vehicles for the dissemination of information about IT Security. Experts emphasized the need for dissemination not to adopt a *one off* approach, but rather for there to be a series of articles intended to repeatedly expose GPs to the issues, and for them to, at some point, start thinking about IT Security in relation to their own practice.

4.3.13(g) The once bitten ...twice shy model

Experts, at various points in their interviews acknowledged that, for many GPs, just as it had been for themselves, it would take an *IT disaster of one kind* [either of their own or of one of their colleagues] *to prompt GPs to actually take some preventative measures.* As one GP recounts, *If the system crashes and you've got to spend 20 or 30 hours and a significant amount of staff time in returning the system and yourself back into a reasonable state, you become much more diligent the second time 'round...Look at HIV Aids, and what happened with the contaminated hypodermic syringes in a small number of practices ... the risk of it happening in individual practices was probably fairly low ... but the consequences were extremely high ...It managed to change the [practice] culture of sterilisation and change management.*

This implementation model requires the preparation of a series of real case *IT Security disaster case studies*. However, issues such as practice anonymity will need to be addressed in their preparation. Notwithstanding, the dissemination of scenarios such as these would play a useful role in a coordinated strategy.

4.3.13(h) The Software Implementation Model

A number of experts proposed the embodiment of IT Security standards in clinical software. Such technical implementations, although varying in complexity, were considered desirable in terms of addressing both security and privacy issues. Some experts even considered this solution as quite likely with the prospect of clinical software vendors offering an IT Security solution package to their customers.

4.3.13(i) The IT Security service provider quality assurance model

A number of experts raised the need to have some way of assessing the quality of...not only the [IT Security] advice being given to GPs, but the quality of the IT services being provided. This seems particularly relevant to GPs with relatively little computer systems expertise and to practices which, out-sourced to external contractors. The issue of service quality arose not only in reference to commercial service providers, but also in relation to potential service provision by Divisions of General Practice.

Although Divisions have well-established IT support service delivery models, the *comprehensiveness of what they currently offer* varies considerably. Whereas a number of Divisions *are direct IT services providers to their constituencies*, and have established credibility in this regard, other Divisions, for a number of reasons including lack of adequate human resourcing, have chosen to put a greater emphasis on other general practice change management agendas.

However, the main issue under discussion here, as one GP expert working closely with his Divisions puts it, is that *of the **reliability, availability, cost of the contractor and ensuring that they understand ...confidentiality**, and that we've [the Division] somehow measured the suitability of that person for that sort of work... It's a very difficult thing for a GP to understand and be able to assess, these professionals or quasi professionals.* This GP goes on to describe how his rural Division has attempted to address this issue: *We looked at the idea of Division-accredited IT providers... we actually put ads into the paper to ask for interested people to register for an assessment by our IT Support Officer in the Division... but didn't get very far ... only two or three [other service providers] in our whole Division registered their interest...and as they were already providing support to a large number of practices anyway, they didn't have any difficulty getting approval [from the Division], but it didn't become certified or anything ... but we need **some form of minimum accreditation standards for IT [staff] supporting practices** ... but it comes down to why would anybody bother if they can get the work anyway?*

5. Security guideline and check-list

The security guidelines are based on the content of the original (2001) GPCG interim security guideline, and significantly modified by suggestions obtained from the key informant interviews. At this stage we regard the guidelines as the intellectual property of this project; they should therefore not be used or modified by others. The guidelines are a first edition version, and although they have had significant input from people who are located in a variety of professional, government and consumer organisations, it is important to obtain formal input from their representatives. This will enable the organisations to consider the guidelines using their usual review processes. It will also be necessary to 'field test' the guidelines and check-list, this being a component of phase 2 of the GPCG computer security project and therefore beyond our brief.

We have tried to keep the guideline brief, partly because it is not the only aspect of computing that GPs have to come to terms with. GPs also have to develop skills in the use of operating systems, clinical software, email and the Internet, at the very least.

Although the guideline is not a technical manual, it does state in reasonably didactic terms the minimum standards which are required to keep electronic data secure.

The introduction to the guideline explains why computer security is important. It also explains that the emphasis which we place on security items is based on expert advice, i.e. it is based on the risk assessment we have undertaken. Then follows a list of the risk categories, what they mean and how practices should manage them. Finally, we also present a summary check-list which GPs can use to review their standard of computer security. A copy of this check-list has been included in the appendix to this report.

6. Implementation strategies

6.1 Introduction

The adoption of information technology by GPs in the late 1990s and the early part of this decade provides us with a lesson about the way change occurs in general practice. In the case of IT, adoption occurred because the products themselves (computers, clinical software, and electronic prescribing rules) were sufficiently 'mature' that GPs could use them within a small business environment. It is, however, a matter of record that the use of practice computing systems is suboptimal. Several strategies were used to bring about change, including financial incentives through the Practice Incentives Program, and training and support from the GPCG IT officer program conducted by divisions of general practice.

Encouraging GPs to follow a set of guidelines on computer security will similarly require a range of strategies. GPs will need incentives, training and support. Using the frameworks of Cabana (1999) and Grol (1997) referred to in the literature review section of this report, the strategies described below might help overcome some of the common barriers to the uptake of guidelines by GPs.

The key informant interviews provided very detailed comments on how GPs and practices can be encouraged to take up the guidelines, and highlight some of the difficulties that can be anticipated. We suggest that the earlier section of this report (4.3), which richly describes some of the perceived barriers and enablers to implementation, be read in conjunction with the recommendations presented below. In particular, several tables in Section 4.3 provide micro level suggestions for computer security implementation; many of these suggestions should be taken up by the GPCG phase 2 implementation project.

A range of organisations can provide various components of support for IT security guideline implementation, with our recommendations on how this might be achieved being presented here. However, we are conscious of not having had an opportunity to allow other organisations time to formally review what we have produced, and this is an essential requirement if they are to be involved in implementation. Also, many of these organisations will have to adapt the guidelines and check-list to suit their own purposes. The principles should remain the same, but the format will have to be made relevant to the requirements of the organisation. For example, the RACGP will need to consider how the guidelines can be incorporated into its Standards for General Practice.

Finally, we have produced guidelines and a check-list based on expert input. However, this and the versions produced by other organisations, will need pilot testing. The GPCG version of the guidelines should be tested in phase two of the GPCG computer security project (the implementation phase) which is described in the GPCG Phase 2 Work Program.

Caveat

The following list of strategies is our recommendations and is partly based on information from the key informants. They are suggestions at this stage. They can only be 'operationalised' by further discussions with and the active involvement of the organisations themselves. This collaborative effort should see a significant role for the GPCG in the immediate future.

6.2 Commonwealth government strategies

The Commonwealth Department of Health and Aging can provide support in the following ways:

Incentives directly to GPs

We acknowledge that the one-off PIP payment to be made in November 2004 to May 2005 includes an incentive for GPs to comply with most of the items on the GPCG security checklist (possibly with the exception of the recommendation for encryption). In the longer term, we recommend that the IT component of PIP can include the same requirement until new practice standards are implemented in practice accreditation.

Targeted funding to divisions of general practice

Targeted funding for divisions of general practice is essential to enable them to educate, train and support GPs to adopt computer security guidelines. This is the case as many no longer have IT training capability. An important element of this would be to support the uptake of encryption which, quite rightly, is an important issue at the Commonwealth level. GPs have so far been slow to adopt encryption because of confusion about competing systems, and difficulties associated with application and set-up processes. Strong divisional support to general practices in implementing encryption would be a prime facilitator to its successful adoption.

A similar case can be made for divisions supporting the Commonwealth's *HIC-Online* program.

Other aspects of the role of divisions are described below.

Publicity

The computer security guidelines should be formally launched by the Minister of Health.

Collaboration with GPCG

The Commonwealth has acquired valuable experience in and developed many resources for computer privacy and security matters through its *HealthConnect*, *MediConnect* and PKI initiatives. The HIC and HeSA should work with GPCG to provide information to general practice, indicate PKI support strategies and help disseminate guidelines on computer security.

6.3 GPCG strategies

There are several roles that the GPCG can play:

Publishing the guidelines and check-list

GPCG should publicise the guidelines and check-list so that GPs at least know of their existence. The guidelines should be published in an attractive format, the check-list should also be well presented and templates on policy and procedures documents, practice computer security coordinator role descriptions, and disaster recovery plans, among others, should be easily downloadable from the GPCG website.

The phase 2 (implementation) security project might have funding available to distribute the templates on CD-ROMs. Sponsorship could be found to help with dissemination.

Engaging with other key stakeholders

The GPCG, as the peak body of general practice computing, should engage with other stakeholders in a broader dissemination strategy. Most of these stakeholders are referred to below, and most if not all have representation on the GPCG Management Committee. The GPCG can provide ongoing expert advice to professional bodies and the Commonwealth on strategies to increase the uptake of the guidelines. For example, it is working with the RACGP to help the latter incorporate computer security into its revised Standards for General Practice.

The GPCG should also collaborate closely with ADGP and State Based Organisations (SBOs) as many divisions do not currently have adequately trained resource people available to provide the service and training required to support general practices for computer security.

Commissioning the phase 2 implementation project on computer security

The 2nd phase of the GPCG computer security project will field test the guidelines and check-list, oversee publication of the guidelines and actively collaborate with key stakeholders to establish a dissemination strategy. This will be supported by strategies developed by the Commonwealth as part of the Red Tape incentive payment in November 2004 to May 2005.

The Evaluation and Monitory Committee of the GPCG will track the uptake and effectiveness of the GPCG implementation strategies.

6.4 Other key professional organisations

6.4.1 Divisions of general practice

Divisions should be provided with *targeted funding* by the Commonwealth to support computer security in general practice. This approach has been used before with success and was acceptable to GPs, for example, Enhanced Primary Care and immunisation. In some cases, GP education was provided by organisations such as university departments and SBOs (of divisions). The SBOs have an

important coordination role and should run training workshops for division staff with the GPCG providing input to the educational content.

The ADGP, in collaboration with GPCG and ACRRM, would have a major role in overseeing a national, divisional computer security program.

The Commonwealth targeted funding to divisions would be used to provide the following:

Education and training

Divisions should be funded to provide education and training in computer security on the basis of the GPCG guidelines. This is best done through continuing professional development (CPD) activities such workshops and practice visits by program officers. Practice staff will also require training.

Practice support

Divisions can provide direct assistance to GPs and practices to implement the guidelines (through 'academic outreach'). This does not mean technical advice but rather seeing that the principles outlined in the security guidelines are understood and implemented by practices using a 'whole of practice' approach. Many divisions have developed expertise in supporting this type of 'change management'.

Divisions should also provide guidance to practices which seek technical advice from private industry. Computer security requires technical assistance from systems administrators and other IT technicians, and divisions can facilitate communication between them and GPs and their staff. Divisions can also give independent advice on service contracts and help practices share information on which are the most cost effective technical services in a region.

Case scenarios, 'lead practice' exemplars and GP experiences

Divisions can publicise the problems associated with ignoring computer security and inform GPs what lead practices (including 'early adopters') are doing. Divisions can also encourage GPs and facilitate meetings so that they can inform each other about their experiences with computer security issues in their practices.

Support for encryption

Divisions should support the use of encryption in general practice and train GPs and practice staff in its use. This element of computer security has been highlighted as it seems to represent a problematic area at this point in time. This is partly due to confusion about competing systems. However, it also concerns perceptions about shortcomings in the application and set-up processes associated with PKI. Another difficulty is the apparent lack of interest in and awareness of the electronic communication needs of GPs by medical specialists.

6.4.2 RACGP

Incorporate security guidelines into Standards for General Practice

The computer security guidelines and check-list will form a part of the Standards for General Practice which are currently undergoing review. Clearly they would need to be incorporated in a manner which is consistent with the other standards. This in our view is a high priority action item as the RACGP standards provide the basis for general practice accreditation. Funding has been set aside in the GPCG Standards workplan to support this work.

Support the uptake of computer security standards by accreditation providers

The College Standards forms the basis for accreditation of general practice by other providers (AGPAL and GPA). The GPCG could assist the College to see how computer security principles can be adopted by accreditation providers and their surveyors.

Publicity

The RACGP could highlight computer security issues by presentations at its conferences and publications in *Australian Family Physician*.

6.4.3 ACRRM, RDAA

These rural organisations can also help disseminate the security guidelines and provide education, training and support to their members to encourage the uptake of the guidelines.

6.4.4 Accreditation bodies

AGPAL and GPA can use a modified version of the computer security check-list to determine whether practices are adhering to security guidelines. The GPCG (and the College) can assist these accreditation providers to revise the check-list in keeping with their organisational requirements.

6.4.5 The AMA and other professional bodies

The AMA should be involved in disseminating the guidelines and check-list. The published information provided to GPs on the national privacy principles is an example of successful collaboration between peak GP bodies and the AMA. The AMA, in collaboration with GPCG, has indicated its interest in working with specialist organisations to adapt the GP computer security guidelines for other medical settings.

Other organisations such as State governments should also participate in a dissemination strategy.

6.5 *Publicity through the media*

The check-list should be published in 'trade magazines' such as *Australian Doctor* and *Medical Observer*.

In addition, the check-list can be disseminated via the previously mentioned peak bodies through their usual communication mechanisms (newspapers, emails, etc.).

Other professional organisations could be involved in computer security workshops at their conferences. This also applies to various educational meetings which are sponsored by the pharmaceutical industry and others.

These strategies are summarised in the following table (but please read the caveat in the box at the end of Section 6.1).

Table 18: Strategy Summary

ORGANISATION	ROLE	POSSIBLE STRATEGIES	COMMENTS
Commonwealth Government (DoHA)	<ol style="list-style-type: none"> 1. Incentives 2. Funding 3. Publicity 	<ol style="list-style-type: none"> 1. PIP 2. Targeted funding for divisions 3. Launch by Minister 	<p>One-off November PIP plus ongoing PIP incentives.</p> <p>2 year targeted funding for divisions suggested.</p>
GPCG	<ol style="list-style-type: none"> 1. Publication of guidelines and dissemination 2. Collaboration with stakeholders 3. Phase 2 implementation project 	<ol style="list-style-type: none"> 1. Phase 2 project will lead to publication 2. GPCG (through project) to liaise with other groups 3. Dissemination via website, conference presentations, etc. 	<p>The main activity will occur while the phase 2 project is active. Longer term involvement via website, the GPCG executive and GP representatives.</p>
ADGP, SBOs and divisions of general practice	<ol style="list-style-type: none"> 1. Education and training 2. Practice support 3. Case scenarios 4. Encryption 	<ol style="list-style-type: none"> 1. Workshops 2. Practice visits 3. Newsletters 4. Phone advice 	<p>Success will depend on targeted Commonwealth funding. ADGP has a key role in pushing this agenda.</p>
RACGP	<ol style="list-style-type: none"> 1. Standards 2. Role with accreditation 3. Dissemination 	<ol style="list-style-type: none"> 1. Incorporate into standards 2. Involvement with accreditation providers 3. Newsletters 	<p>RACGP adoption of guidelines is essential if it is to become a part of accreditation.</p>
ACCRM, RDAA , AMA, others	<ol style="list-style-type: none"> 1. Education, training and support 2. Dissemination 3. Collaboration with specialist colleges 	<ol style="list-style-type: none"> 1. Workshops 2. Newsletters 3. Phone advice Publicise check-list in its media 4. Inform specialists 	<p>Funding source uncertain, but could use materials produced by GPCG. Important roles in dissemination of guidelines, including beyond general practice.</p>
AGPAL, GPA	<ol style="list-style-type: none"> 1. Accreditation 	<ol style="list-style-type: none"> 1. Incorporate standards into accreditation survey visits 2. Security included into surveying 	<p>Important for GPs claiming PIP.</p>

ORGANISATION	ROLE	POSSIBLE STRATEGIES	COMMENTS
Medical media	1. Dissemination	1. Publish check-list	Important publicity.

6.6 Conclusions on an implementation framework

One of the key features of our implementation plan will be that this cannot be a one-off process. This is really a quality improvement exercise in which GPs will not make all the changes at once. It is essential that a framework be established that includes periodic reminders and incentives for GPs and practices to attend to computer security. This will require a commitment from general practice and other peak bodies to ongoing resourcing.

Bearing in mind that a successful implementation of a series of strategies as outlined above depends on effective cooperation between people and organisations, money, competing interests and other factors, we suggest the following sequence of events:

6.6.1 Immediate

- GPCG continue to 'manage' computer security guidelines through its phase 2 project. This will lead to publication, dissemination and the engagement of other stakeholders.

6.6.2 Short term (2004)

- Commonwealth Government commits to funding (PIP and divisions)
- RACGP incorporates guidelines into its Standards.

6.6.3 Medium term (2005 – 2006)

- Guidelines become a part of accreditation in general practice
- AMA, ADGP, ACRRM, RDAA and other professional organisations participate in guidelines uptake (with dissemination, education, training and support strategies) in collaboration with GPCG.

6.6.4 Long term

- Computer security becomes accepted by GPs as an essential part of managing their practices, with ongoing improvements in security standards.

7. Project outcomes

The *Phase One GPCG Computer Security Project* has produced the following ‘deliverables’:

- A review of the literature on computer security in general practice
- Information from divisions of general practice on the extent to which GPs currently adhere to security guidelines
- Interviews with key informants to gain a better understanding of the following:
 - An assessment of the IT security risks in general practice (i.e. a ‘risk assessment’)
 - Advice on how to best manage these risks at the national and practice level
 - Suggestions on how to encourage the profession to improve its IT security practices and performance.
- Preliminary discussions with the RACGP and other potential stakeholders (in informal rather than official capacities), to see how best to include IT security as an important standards issue in general practice and how it can be incorporated into practice accreditation.
- A ‘plain English’ computer security guideline written for general practice
- A summarised one page computer security check-list for easy reference
- A series of proformas for GPs and their practice staff on varying aspects of IT security
- An electronic template which can be downloaded and used by GPs and staff as a basis for their computer security practice policies and procedures manual
- An implementation strategy to support the dissemination and uptake of the security guideline and check-list by general practice
- A comprehensive final report that describes all of the above in detail.

We believe that the *Phase One GPCG Security Project* has achieved what it set out to do and that the way is now prepared, through the detailing of a number of inter-related strategies, for the *Phase Two* implementation.

8. References

- ACNielsen Research. (1998). *A study into levels of, and attitudes towards information technology in general practice*. Commonwealth Department of Health and Family Services.
- Allender, M. (2002). HIPAA compliance in the OR. *AORN Online*, 75, 121-25.
- Anderson, R. (1996). Clinical system security: interim guidelines. *Br Med J*, 312, 109-11.
- Berg, M. and Mol, A. (1998). *Differences in Medicine: Unraveling Practices, Techniques, and Bodies*. Durham: Duke University Press.
- Cabana, M., Rand, C., Powe, N., Wu, A., Wilson, M., and Abboud, P., et al. (1999). Why don't physicians follow clinical practice guidelines? A framework for improvement. *JAMA*, 282, 1458-65.
- Caruso, R. D. (2003). Personal computer security: Part 1. Firewalls, antivirus software and Internet security suites. *Radiographics*, 23, 1329 – 37.
- Commonwealth. (2000). Privacy Amendment (Private Sector) Act 2000.
- Effective health care bulletin. (1999). Getting evidence into practice (systematic review). *NHS Centre for Reviews and Dissemination*, 5:1-16
- Georgiadis, C. K., Mavridis, I. K., and Pangalos, I. (2003). Healthcare teams over the Internet: Programming a certificate-based approach. *Internal Journal of Medical Informatics*, 70, 161-71.
- GPCG. (2001). *Interim IT security guidelines*. Canberra: General Practice Computing Group.
- Grimshaw, J.M., Thomas, R.E., MacLennan, G., Fraser, C., Ramsay, C., Vale, L., et al. (2004). Effectiveness and efficiency of guideline dissemination and implementation strategies. *Health Technology Assessment*, 8, 1-84.
- Grol R. (1997). Beliefs and evidence in changing clinical practice. *Br Med J*, 315, 418-21.

- Headland TN, Pike KL and Harris M. (1990) *Emics and Etics: the insider/outsider debate*. Thousand Oaks, CA: Sage.
- Holstein J and Gubrium J (1995). *The active interview*. Thousand Oaks CA: Sage.
- Millman, A., Lee, N., and Brooke, A. (1995) ABC of medical computing: computers in general practice II. *BMJ*, 311, 864-67.
- Milstein, B., and Tongo, J. (2001). *Legal issues in general practice computerisation*. Canberra: Department of Health and Aged Care and The General Practice Computing Group.
- Mol, A. (2002). *the body multiple: ontology in medical practice*. Durham: Duke University Press.
- National Health Information Management Advisory Council. (2001). *Health Online: A Health Information Action Plan for Australia* (2nd ed.). Canberra: Commonwealth Department of Health and Aged Care.
- Privacy Commissioner. (1995). Community attitudes to privacy. Information Paper no 3. Sydney: Human Rights and Equal Opportunity Commission.
- Rice PL and Ezzy D. (1995) *Qualitative Research Methods: a health focus*. Melbourne: Oxford University Press. pp43-6
- Rogers, E.M. (1995). Diffusion of innovations (4th ed.) New York: The Free Press.
- Rose, M. (2003). A survey of computer security in the ACT Division. Canberra: ACT Division.
- Sardinas J and Muldoon J (1998). Securing the transmission and storage of medical information. *Computers in Nursing*, 16, 162-8.
- Shiller, G. (2003). *Informatics survey of general practice*. Adelaide: Adelaide Central and Eastern Division of General Practice.
- Suchman, L. (1987). *Plans and Situated Actions: the problem of human machine communications*. Cambridge: Cambridge University Press.
- Trost J. (1986) 'Statistically Non-representative Stratified Sampling: a sampling technique for qualitative studies' *Qualitative Sociology*, 9:1 pp54-7
- Western, M., Dwan, K., Makkai, T., Del Mar, C., and Western, J. (2001). *Measuring IT use in Australian general practice 2001*. Canberra: Department of Health and Aged Care.

Winner L. (1989). *The Whale and the Reactor: a search for limits in an age of high technology*. Chicago, USA: University of Chicago.

Young, K., and Schattner, P. (2002). *Survey of computer security in the Monash Division*. Melbourne: Monash Division of General Practice.

9. Appendix

9.1 *Key informant semi-structured interview schedule (short version)*

The schedule which follows represents a slightly abbreviated form of the telephone interview questions.

9.1.1 Context

First of all, could you please tell me what you think is the **MOST important IT Security issue** facing Australian **general practice at present**?

In what way might this General Practice IT security issue be **different to those experienced by other kinds of small businesses**?

In what way might this General Practice IT security issue be **different from those experienced in other parts of the healthcare system**?

Please keep in mind that, as we move into the next stage of the interview, when we talk about IT security, I am broadly referring to:

- keeping electronic patient data confidential
- maintaining its integrity; and
- allowing patient data to be accessible when required.

However, in this interview we are not going to deal specifically with privacy matters.

9.1.2 Risk categories

Security risk in general practice generally falls into the list already provided to you in **Task A**.

- Are there any other major organisational risk categories that you think are really important?
- Are there any other major technical risk categories that you think are really important?

ORGANISATIONAL RISKS
IT policies in the practice (includes access rights, patient confidentiality, as well as all the technical protocols)
Practice IT Coordinator
Disaster plan (= a sub-set of IT policy)
Email and Internet policies (= a sub-set of IT policy)
[insert additional <i>organisational</i> risk categories proposed by key informant]

TECHNICAL RISKS
Back-ups
Screen-savers
Passwords
Viruses
Firewalls
Power surges
Encryption of data transmission.
[insert additional <i>technical</i> risk categories proposed by key informant]

9.1.3 Risk analysis

I wonder if we can now **look at each of these items** in turn (starting at the top of the list) and decide on two things with each of them: **how likely** are they to occur, and what is the *magnitude* of the **consequences (for the practice or the patient)** if they do occur.

9.1.4 Working definitions:

9.1.4(a) Likelihood

High very likely to occur within the next 12 months

Medium might occur within 12 months

Low not very likely to occur within 12 months

9.1.5 Consequences (magnitude)

High of major significance to the business or to the patient

Medium important to either, but not of critical importance

Low a nuisance, but can cope with this without too much difficulty

ORGANISATIONAL RISKS	CONSEQUENCES		
IT policies in the practice (includes access rights, patient confidentiality, as well as all the technical protocols)	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L

ORGANISATIONAL RISKS	CONSEQUENCES		
Practice IT Coordinator	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L
Disaster plan (= a sub-set of IT policy)	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L
Email and Internet policies (= a sub-set of IT policy)	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L
<i>Additional organisational risk category 1</i>	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L
<i>Additional organisational risk category 2</i>	H	M	L
• Consequences would be in terms of patient risk	H	M	L
• Consequences would be in terms of cost to the business	H	M	L

TECHNICAL RISKS	LIKELIHOOD			CONSEQUENCES		
Back-ups						
<i>e.g. How likely is it for a back-up to fail in general practice? If it does fail, what are the consequences?</i>	H	M	L	H	M	L
• Consequences would be in terms of patient risk				H	M	L
• Consequences would be in terms of cost to the business				H	M	L

TECHNICAL RISKS	LIKELIHOOD			CONSEQUENCES		
Screen-savers <i>Eg if a GP does not have a screensaver, how likely is there to be a breach in security by either staff or, more usually, by patients</i>	H	M	L	H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of patient risk 				H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of cost to the business 				H	M	L
Passwords <i>Eg if GPs do not use passwords, how likely is there to be a breach in security by either staff or by patients</i>	H	M	L	H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of patient risk 				H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of cost to the business 				H	M	L
Viruses <i>Eg if anti-virus software is not kept up to date, how likely is there to be a breach in security?</i>	H	M	L	H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of patient risk 				H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of cost to the business 				H	M	L
Firewalls <i>Eg if firewalls are not in place, how likely is there to be a breach in security?</i>	H	M	L	H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of patient risk 				H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of cost to the business 				H	M	L
Power surges <i>Eg if power surge protection is not in place, how likely is there to be a breach in security?</i>	H	M	L	H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of patient risk 				H	M	L
<ul style="list-style-type: none"> • Consequences would be in terms of cost to the business 				H	M	L

TECHNICAL RISKS	LIKELIHOOD			CONSEQUENCES		
Encryption of data transmission <i>Eg if emails are not encrypted, how likely is there to be a breach in security?</i>	H	M	L	H	M	L
• Consequences would be in terms of patient risk				H	M	L
• Consequences would be in terms of cost to the business				H	M	L
insert additional <i>technical risk 1</i>	H	M	L	H	M	L
• Consequences would be in terms of patient risk				H	M	L
• Consequences would be in terms of cost to the business				H	M	L
insert additional <i>technical risk 2</i>	H	M	L	H	M	L
• Consequences would be in terms of patient risk				H	M	L
• Consequences would be in terms of cost to the business				H	M	L

9.1.6 Risk evaluation

Based on what you have told me of the **likelihood and consequences** of each of the risks, I wonder if you could tell me what you think are currently **high priority** risks, which are **medium** and which are **low priority** for general practice in the current climate.

Your prioritisation could take into account a number of factors:

- the significance to either the welfare of the patient or the functioning of the business
- how much it costs to address the risk versus the cost of dealing with the breach in security

RISK ITEMS	PRIORITY		
	HIGH	MEDIUM	LOW
Organisational			
IT policies in the practice (includes access rights, patient confidentiality, as well as all the technical protocols)			
Practice IT Coordinator			
Disaster plan (= a sub-set of IT policy)			
Email and Internet policies (= a sub-set of IT policy)			

RISK ITEMS	PRIORITY		
	HIGH	MEDIUM	LOW
<i>Additional organisational risks noted by the expert informant</i>			
Technical			
Back-ups			
Screen-savers			
Passwords			
Viruses			
Firewalls			
Power surges			
Encryption of data transmission			
<i>Other technical risks noted by the expert informant</i>			

9.1.7 Risk management

Now for each of these risks, what do you think is the **best way of preventing each from becoming a reality?**

Can you also indicate how **much it will cost:**

- in terms of GP or staff time
- perhaps dollar terms

to implement a solution for a given risk

RISKS	SUGGESTED COST EFFECTIVE RISK MANAGEMENT SOLUTIONS AND STRATEGIES (IE WHAT NEEDS TO BE DONE AND WHAT WILL THE 'COST' BE?)
Organisational	
Not having IT policies in the practice (includes access rights, patient confidentiality, as well as all the technical protocols)	
Absence of a Practice IT Coordinator	

RISKS	SUGGESTED <i>COST EFFECTIVE</i> RISK MANAGEMENT SOLUTIONS AND STRATEGIES (IE WHAT NEEDS TO BE DONE AND WHAT WILL THE 'COST' BE?)
Lack of a Disaster plan (= a sub-set of IT policy)	
No documented Email and Internet policies (= a sub-set of IT policy)	
<i>Other technical risks noted by the expert informant</i>	
Technical	
Inadequate Back-ups	
Inadequate use of Screen-savers in the practice	
Lack of Passwords	
Lack of protection from Viruses	
Lack of Firewalls	
Inadequate protection from Power surges	
Inadequate Encryption of data transmitted	
<i>Other technical risks noted by the expert informant</i>	

9.1.8 Barriers and enablers

We intend to write a **security guideline** for general practice based on the kind of information you have just given us.

What are some of the (other) **barriers** to **doctors** (or **practice staff**) carrying out some of these **security protocols**? Why don't GPs seem to be doing what they should?

More importantly, what might be some of the **enablers**?

What can **we do to encourage GP adherence to a security guideline?**

9.1.9 Further comments

Is there anything else you wish to add that we have not yet covered?

9.1.10 Finally:

- whose views is this key ‘expert’ informant representing in this interview?
- Have you spoken with anyone else in preparation for this interview?
- Has there been a FORMAL or INFORMAL ‘in-house’ consultation process that has occurred prior to this interview being conducted

9.2 Acronyms and definition of terms

9.2.1 Acronyms and definition of terms

ACRRM	Australian College of Rural and Remote Medicine
ADGP	Australian Divisions of General Practice
AMA	Australian Medical Association
CHF	Consumer Health Forum
DGPs	Divisions of General Practice
DoHA	Commonwealth Department of Health & Ageing
GPCG	General Practice Computer Group
GPPAC	General Practice Partnership Advisory Council
HESA	Health E-Signature Authority
HIC	Health Insurance Commission
MDAV	Medical Defence Association (Victoria)
MDGP	Monash Division of General Practice
MSIA	Medical Software Industry Association
NSCS	National Standing Committee on Standards, RACGP
RACGP	Royal Australian College of General Practitioners
MoDGP	Monash University Department of General Practice
RDAA	Rural Doctors Association of Australia
UoMDRH	University of Melbourne Department of Rural Health

9.2.2 Risk management terms

Taken from AS/MZS 4360:1999 'Risk Management'

Consequence

The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Event

An incident or situation, which occurs in a particular place during a particular interval of time

Likelihood

Used as a qualitative description of probability or frequency

Loss

Any negative consequence, financial or otherwise

Risk

The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood

Risk analysis

A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences

Risk assessment

The overall process of risk analysis and risk evaluation. In this document, risk analysis and risk assessment are used interchangeably.

Risk control

That part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimize adverse risks

Risk evaluation

The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria

9.3 The GPCG computer security check-list

This check-list should be used in conjunction with the GPCG computer security guidelines which describe each item in more detail. The list is designed to help practices check whether they have put in place a number of computer security processes or systems. Please note that the list is restricted to security aspects of IT.

IT CATEGORY	TASKS	HAS THIS BEEN IMPLEMENTED? (TICK IF YES)
1. Practice computer security coordinator	<ul style="list-style-type: none"> Practice IT security coordinator's role description written Practice IT security coordinator appointed IT security training for coordinator provided Security coordinator's role reviewed (at specified intervals) 	<input type="checkbox"/> <input type="checkbox"/>
2. Practice IT security policies and procedures	<ul style="list-style-type: none"> Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual) IT security policies and procedures documented IT security policies and procedures documentation reviewed (at specified intervals) Staff trained in IT security policies and procedures 	<input type="checkbox"/> <input type="checkbox"/>
3. Access control	<ul style="list-style-type: none"> Staff policy developed on levels of electronic access to data and systems Staff have created personal passwords to access appropriate level Passwords are kept secure Consideration given to changing passwords periodically 	<input type="checkbox"/> <input type="checkbox"/>
4. Disaster recovery plan	<ul style="list-style-type: none"> Disaster recovery plan developed Disaster recovery plan tested (at specified intervals) Disaster recovery plan updated (at specified intervals) 	<input type="checkbox"/> <input type="checkbox"/>
5. Consulting room and 'front desk' security	<ul style="list-style-type: none"> Practice aware of need to maintain appropriate confidentiality of information on computer screens Screensavers or other automated privacy protection device enabled 	<input type="checkbox"/> <input type="checkbox"/>
6. Back-ups	<ul style="list-style-type: none"> Back-ups of data done daily 	<input type="checkbox"/>

IT CATEGORY	TASKS	HAS THIS BEEN IMPLEMENTED? (TICK IF YES)
	<ul style="list-style-type: none"> Back-ups of data stored offsite Back-up procedure tested (by performing a restoration of data) at specified intervals Back-up procedure has been included in a documented disaster recovery plan 	<input type="checkbox"/> <input type="checkbox"/>
7. Viruses	<ul style="list-style-type: none"> Anti-viral software installed on all computers Automatic updating of viral definitions enabled (daily if possible) Staff trained in anti-viral measures as documented in policies and procedures manual 	<input type="checkbox"/> <input type="checkbox"/>
8. Firewalls	<ul style="list-style-type: none"> Hardware and/or software firewalls installed Hardware and/or software firewalls tested 	<input type="checkbox"/> <input type="checkbox"/>
9. Network maintenance	<ul style="list-style-type: none"> Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches) Uninterruptible Power Supply installed (to at least the server) 	<input type="checkbox"/> <input type="checkbox"/>
10. Secure electronic communication	<ul style="list-style-type: none"> Encryption systems considered Encryption used for the electronic transfer of confidential information 	<input type="checkbox"/> <input type="checkbox"/>

Source: GPCG computer security project ©February 2004

End of doc.