Guidelines for computer security in general practice

Peter Schattner MD MMed FRACGP
Clinical Associate Professor, Department of General Practice, School of Primary Health Care, Monash University, Victoria, Australia

Catherine Pletschner BEd GradDip EdAdmin
Research Fellow, Department of Rural Health, School of Medicine, Dentistry and Health Sciences, University of Melbourne, Victoria, Australia

Heinz Bhend MD
General Practitioner, and Member, WONCA Informatics Working Party, Swiss Society of General Medicine, Aarburg, Switzerland

Johan Brouns MD
General Practitioner and Specialist in Health Care Data Management, and Member, WONCA Informatics Working Party, Domus Medica IT, Belgium and Department of Pathology, Goormaghtigh Institute, University of Ghent, Ghent, Belgium

ABSTRACT

Background As general practice becomes increasingly computerised, data security becomes increasingly important for both patient health and the efficient operation of the practice.

Objective To develop guidelines for computer security in general practice based on a literature review, an analysis of available information on current practice and a series of key stakeholder interviews. While the guideline was produced in the context of Australian general practice, we have developed a template that is also relevant for other countries.

Method Current data on computer security measures was sought from Australian divisions of general practice. Semi-structured interviews were conducted with general practitioners (GPs), the medical software industry, senior managers within government responsible for health IT (information technology) initiatives, technical IT experts, divisions of general practice and a member of a health information consumer group. The respondents were asked to assess both the likelihood and the consequences of potential risks in computer security being breached.

Results The study suggested that the most important computer security issues in general practice were: the need for a nominated IT security coordinator; having written IT policies, including a practice disaster recovery plan; controlling access to different levels of electronic data; doing and testing backups; protecting against viruses and other malicious codes; installing firewalls; undertaking routine maintenance of hardware and software; and securing electronic communication, for example via encryption. This information led to the production of computer security guidelines, including a one-page summary checklist, which were subsequently distributed to all GPs in Australia.

Conclusions This paper maps out a process for developing computer security guidelines for general practice. The specific content will vary in different countries according to their levels of adoption of IT, and cultural, technical and other health service factors. Making these guidelines relevant to local contexts should help maximise their uptake.

Keywords: computer security, general practice, guidelines
Background

Information security has been defined as a process for ensuring the confidentiality, integrity and accessibility of electronic data.1–9 In general practice, data refer to clinical, demographic and financial information, and keeping these secure is important for both patient health and the efficient running of a practice.

Australian general practice is becoming increasingly computerised. By the year 2000, almost 90% of practices were using computers, particularly for administrative tasks.10 The proportion of practices using clinical software is not known exactly, but it is estimated that 80–90% of GPs use computers for generating prescriptions.11

This paper outlines the principles of developing computer security guidelines for family medicine/general practice. The authors recognise that GPs in other countries might choose to adapt these principles to accommodate local circumstances depending on cultural, technological and health service factors. However, our study could provide a useful template for the development of such guidelines in other countries.

Methods

Several strategies were used by Peter Schattner and Catherine Pleteshner to develop computer security guidelines for Australian general practice.

Reviewing the literature on computer security in the health industry

A literature review was undertaken with Medline, ProQuest and Google. Various keywords were employed including combinations of computer security, information security, general practice, information technology (and IT), computers, training doctors, health informatics and doctors and the internet. Non-research literature was also reviewed, particularly the guidelines produced by Standards Australia and the draft guidelines on computer security developed by the Australian General Practice Computing Group (GPCG) in 2001.1–9,12

Reviewing existing data from surveys in general practice

Australia has 118 divisions of general practice; these are regional organisations funded by the Australian Government to support general practice. In December 2003, all of these divisions were contacted to see if they had undertaken surveys on computer security among their GP members. Only three divisions were in a position to provide comprehensive survey information.

Interviewing key stakeholders

We conducted 14 key informant telephone interviews, which included GPs (4), a representative of the medical software industry association, government representatives (3), experts in IT (3), relevant staff from divisions of general practice (2) and one member of a health information consumer group. The consumer representative had experience with health IT, and the three government representatives included nominated senior managers responsible for the management and implementation of key Australian Government health IT initiatives.

The objectives of the interviews were to:

- conduct a risk assessment on the likelihood and consequences of breaches in computer security in general practice
- obtain risk management advice
- obtain suggestions for the implementation of security guidelines in Australian general practice and identify potential barriers to their uptake.

An interview schedule was developed to meet these objectives by reviewing the literature, with particular reference to publications by Standards Australia and the earlier GPCG draft IT security guidelines.1–9,12

The views of each key informant were transcribed and arranged according to the themes outlined in the original, semi-structured interview framework. The identities of the respondents have been kept confidential.

Computer security risks have been divided into organisational and technical ones. The interviewees were first asked to consider what would be the likely consequences to both the patient and the practice if a risk were realised. The following scale was used:

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

The interviewees were also asked to comment on the likelihood of nominated and other technical risks occurring. They were asked to make this assessment on the basis of not only their own experience but also on their observations when assisting colleagues, and through insight gained by other exchanges within
the profession. The following working definitions for likelihood were used:

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

Both patient and practice business risks were taken into account, and risk management included a consideration of the cost of preventing a breach in security.

Results

Literature review

A search of the peer-reviewed literature on computer security in general practice revealed virtually no articles based on original research. A few papers described overseas studies in nursing, specialist medicine or hospital settings, none of which necessarily applied to Australian general practice. The vast majority of the articles were reviews. Computer security guidelines to date have generally been based on ‘expert opinion’ rather than quantitative risk assessments. For example, information published on the reasons why GPs should encrypt electronic data before transmission elsewhere does not give any evidence on how often problems have arisen by not encrypting. Nevertheless, it is generally accepted that the security of patient information is important for the proper ethical, legal and professional functioning of the practice. Unfortunately, there are several threats to this security in general practice, including GP use of the internet. The relationship between confidentiality of personal health information and the use of computers and the internet was raised by the Australia National Health Information Management Advisory Council in 2001. The Privacy Commissioner reported that many Australians believe there is less privacy now than there has been in previous years and that computers make it easier for confidential information to fall into the wrong hands. As a consequence, policies are needed to guide processing, receiving, modifying, disseminating, sending, storing and disposing of patient-related healthcare data. The Australian Government has responded by passing the Privacy Amendment (Private Sector) Act 2000 which addresses the need to safeguard personal information in the private sector. This applies as much to paper records as it does to electronic ones in medical practice.

Information based on key informant interviews

The consensus from the interviewees was that the most important issue in computer security in general practice is the backing up of data. Other important issues raised included physical and internet security (firewalls, anti-virus solutions and encryption) and the confidentiality of patient records. Further, a number of GPs observed that most general practices were relatively small businesses, and many had limited in-house knowledge of, or expertise in, computer security, which was therefore considered somewhat beyond their reach.

Questions were asked on specific aspects of IT security as follows:

Organisational aspects (see Table 2)

IT POLICIES IN THE PRACTICE

The importance of a practice developing an IT policy was recognised:

‘In my experience, where there are no IT policies there is generally no IT focus ... there is no investment in
## Table 1  Australian general practice surveys on data security

<table>
<thead>
<tr>
<th>IT policies and procedures (% of practices)</th>
<th>Backup procedure</th>
<th>Anti-virus and firewall protection</th>
<th>Passwords</th>
<th>Awareness of computer risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>78% have an IT co-ordinator (a GP in 47%)</td>
<td>77% back up data daily</td>
<td>76% have anti-virus software</td>
<td>69% do not have passwords to login to computers</td>
<td>Majority are not confident about their knowledge of backup procedures</td>
</tr>
<tr>
<td>61% have written IT disaster plan</td>
<td>69% have tested their backups at some stage</td>
<td>60% do not have this software on every computer in the practice</td>
<td>51% do not have passwords to login to clinical software</td>
<td>Some practices that are confident do not have adequate data safety procedures</td>
</tr>
<tr>
<td>&lt;50% have formal written IT policies and procedures</td>
<td>47% were unsure if all important files on network were backed up</td>
<td>29% do not update anti-virus software regularly</td>
<td></td>
<td>Cost is a major factor preventing practices from obtaining expert advice from commercial IT services for data security</td>
</tr>
<tr>
<td></td>
<td>54% have an uninterruptible power supply (mainly for server)</td>
<td>69% of practices with internet connections did not have firewalls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Table 2  IT security risks in general practice – organisational aspects

<table>
<thead>
<tr>
<th>Risk analysis</th>
<th>Potential magnitude of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational risks</td>
<td>High</td>
</tr>
<tr>
<td>Practice IT policy</td>
<td></td>
</tr>
<tr>
<td>Risk to the patient</td>
<td>6</td>
</tr>
<tr>
<td>Risk to the business</td>
<td>7</td>
</tr>
<tr>
<td>IT practice co-ordinator</td>
<td></td>
</tr>
<tr>
<td>Risk to the patient</td>
<td>2</td>
</tr>
<tr>
<td>Risk to the business</td>
<td>8</td>
</tr>
<tr>
<td>Practice disaster plan</td>
<td></td>
</tr>
<tr>
<td>Risk to the patient</td>
<td>3</td>
</tr>
<tr>
<td>Risk to the business</td>
<td>6</td>
</tr>
<tr>
<td>Practice email and internet policies</td>
<td></td>
</tr>
<tr>
<td>Risk to the patient</td>
<td>7</td>
</tr>
<tr>
<td>Risk to the business</td>
<td>7</td>
</tr>
</tbody>
</table>

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

**PRACTICE IT CO-ORDINATOR**

Similarly, most respondents felt that having an IT co-ordinator was important, especially for the business aspects of general practice.

**PRACTICE DISASTER PLAN**

Disaster plans are required when the computer system ‘goes down’. Respondents indicated that they thought there was considerable risk in not having a practice disaster plan. They considered it vital to have an alternative system in place whereby they could keep booking and treating patients.

’Surn 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 ... it’s simple ... use a paper-based system.’ (GP, interview transcript: original emphasis)

**EMAIL AND INTERNET POLICIES**

Most respondents considered that there was a substantial risk to both patients and the practice from not having practice-wide email and internet policies. However, some thought that as there was currently limited use of email and the internet for clinical purposes, the actual risk is likely to be low for the time being.

‘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 ... it’s simple ... use a paper-based system.’ (GP, interview transcript: original emphasis)

**ACCESS RIGHTS TO DATA**

A clear protocol on who has access to which data is essential to reduce the risk of inappropriate access to information, both clinical and financial. However, most thought that compliance with national privacy legislation was cumbersome and costly.

**Technical aspects (see Table 3)**

**BACKUPS AND RESTORATIONS**

The respondents felt that there was a reasonable likelihood of backups failing. The risks to both patients and the business were considered to be of major significance although difficult to quantify. There were considerable monetary implications for GPs not having effective data backup strategies in place.

**SCREEN SAVERS**

Respondents considered the lack of screen savers to be a relatively low risk to both patients and the business. The main risk was in terms of litigation for breach of confidentiality.

**PASSWORDS**

A number of GP respondents explained that the widespread failure by GPs and their practice staff to use passwords was as a result of a high degree of mutual trust. One commented that although each individual GP in the practice had his/her own password, these were collected by one of the practice staff and then written on a piece of paper that was hung up in the back office area. It also appeared that as the size of practices increased, so did the risk of a breach in security associated with passwords.

**MALICIOUS CODE AND FIREWALLS**

Not protecting computers against malicious code (such as viruses) was generally thought to pose a high risk, particularly to the business. This was especially so where GPs and practice staff regularly accessed the internet. Rectifying the ensuing problems such as computer crashes was costly, time-consuming and disruptive to the day-to-day operations of the practice. One GP commented on one such 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.’ (GP, interview transcript)

Respondents varied in their assessment of the magnitude of risk to the patient, some considering this to be minimal.

**POWER SURGES**

Power surges were thought to be more likely in rural rather than metropolitan settings, and the magnitude of risk was considered greater for the business than for patients.

**ENCRYPTION OF DATA**

Respondents reiterated the generally-held view of the need to encrypt patient data for electronic transmission beyond the practice. The risk of not doing so was thought to be considerable, particularly for breaches of patient confidentiality; however, litigation was also a possible outcome of breaches to privacy. It was noted that only a minority of practices had adopted the Australian Government’s freely available encryption solution – Public Key Infrastructure (PKI).
"We don’t have, as a practice, any particular organised approach to encryption of things like specialists’ letters.”
(GP, interview transcript)

**OTHER TECHNICAL RISKS**

Two other areas of risk identified were:

- doctors trying to tinker with their computer systems beyond their levels of expertise
- not replacing ageing IT infrastructure until some part of it failed.

The risk analysis (summarised in Table 4) revealed the priority ratings for organisational and technical security risks for Australian general practice. Protection against malicious code and the use of firewalls were rated as high priorities, as were the need for IT policies and disaster recovery plans. The use of screen savers, protection against power surges and the use of encryption were considered low priority.

## Discussion

This paper reports on the development of a set of computer security guidelines in Australia. These
guidelines were based on information from other published guidelines, surveys which documented some of the shortcomings in the adoption of computer security measures, and the opinions of experts in the Australian context. Unfortunately, little research has previously been undertaken to justify how generic computer security guidelines should be modified to make them applicable to general practice. This study has attempted to make these guidelines relevant to GPs, and this should assist in their adoption.

The five surveys referred to provide some indication of the extent of the problem of computer security in Australian general practice, although the findings are likely to be of limited accuracy. Most of these studies had poor response rates (less than 50%) and did not use validated data collection instruments. Further, it is likely that considerable improvements have been made to computer security practices even within the few short years that have passed since these studies were done. It is interesting that the findings of these surveys are consistent with those that have been undertaken in Switzerland and Belgium in 2006 by two of the authors, Heinz Bhend and Johan Brouns. These also suggest that GPs are not taking adequate measures to ensure the security of data in their practices.

The information gathered in the context of Australian general practice was used to produce guidelines which can be accessed on www.gpcg.org. A summary checklist was derived (see Table 5), which provides a simple, one-page set of computer security items which GPs can use to see if appropriate procedures have been put in place. Ideally, the guidelines and summary checklist should be evaluated in the field to find out just how usable they are.

Nevertheless, as a place for others to start, this study illuminates a set of principles that have been selected and used to develop computer security guidelines for general practice. These principles can be summarised as follows:

- understand what has been developed to date within one’s country and elsewhere (a literature review)
- understand the local issues (i.e. gather information about current computer security problems and the socio-technical barriers to overcoming them)
- finally, ask experts (GPs, those in the IT industry, GP professional organisations, government and consumers) what needs to be done and how best to do it.

Following, whilst adapting, these steps should help other countries develop IT security guidelines which are relevant to their own requirements.

Once such guidelines are produced, how can we encourage GPs to adopt them? GPs will need incentives, training and support. Respondents in this study emphasised the importance of human factors over purely technical solutions, for example, the need for a practice to identify someone who co-ordinates security issues, including ensuring practice staff and GP training.

The Australian Government has provided financial incentives to encourage GPs to adopt computer security measures in their practices. It has also funded the nationwide distribution of the computer security guidelines referred to in this paper. These guidelines

<table>
<thead>
<tr>
<th>Risk to be addressed</th>
<th>Prioritisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT policies in the practice</td>
<td>High</td>
</tr>
<tr>
<td>Practice IT co-ordinator</td>
<td>7</td>
</tr>
<tr>
<td>Disaster plan</td>
<td>7</td>
</tr>
<tr>
<td>Email and internet policies</td>
<td>6</td>
</tr>
<tr>
<td>Backups (restorations)</td>
<td>7</td>
</tr>
<tr>
<td>Screen savers</td>
<td>1</td>
</tr>
<tr>
<td>Passwords</td>
<td>3</td>
</tr>
<tr>
<td>Malicious code (e.g. viruses)</td>
<td>8</td>
</tr>
<tr>
<td>Firewalls</td>
<td>8</td>
</tr>
<tr>
<td>Power surges</td>
<td>3</td>
</tr>
<tr>
<td>Encryption of transmitted data</td>
<td>3</td>
</tr>
</tbody>
</table>
Table 5 General Practice Computing Group computer security checklist

<table>
<thead>
<tr>
<th>IT category</th>
<th>Tasks</th>
<th>Has this been implemented? (tick if yes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice computer security co-ordinator</td>
<td>Practice IT security co-ordinator’s role description written</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Practice IT security co-ordinator appointed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT security training for co-ordinator provided</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security co-ordinator’s role reviewed (at specified intervals)</td>
<td></td>
</tr>
<tr>
<td>Practice IT security policies and procedures</td>
<td>Person(s) (e.g. IT security co-ordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT security policies and procedures documented</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT security policies and procedures documentation reviewed (at specified intervals)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff trained in IT security policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td>Staff policy developed on levels of electronic access to data and systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff have created personal passwords to access appropriate level</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passwords are kept secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consideration given to changing passwords periodically</td>
<td></td>
</tr>
<tr>
<td>Disaster recovery plan</td>
<td>Disaster recovery plan developed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disaster recovery plan tested (at specified intervals)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disaster recovery plan updated (at specified intervals)</td>
<td></td>
</tr>
<tr>
<td>Backups</td>
<td>Backups of data done daily</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backups of data stored offsite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup procedure tested (by performing a restoration of data) at specified intervals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup procedure has been included in a documented disaster recovery plan</td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td>Anti-viral software installed on all computers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic updating of viral definitions enabled (daily if possible)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff trained in anti-viral measures as documented in policies and procedures manual</td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>Hardware and/or software firewalls installed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware and/or software firewalls tested</td>
<td></td>
</tr>
<tr>
<td>Network maintenance</td>
<td>Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uninterruptible power supply installed (to at least the server)</td>
<td></td>
</tr>
<tr>
<td>Secure electronic communication</td>
<td>Encryption systems considered</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encryption used for the electronic transfer of confidential information</td>
<td></td>
</tr>
</tbody>
</table>

Source: GPCG computer security project ©GPCG February 2004 (This checklist should be used in conjunction with the GPCG computer security guidelines which describe each item in more detail. www.gpcg.org.au/images/stories/pdfs/publications/docs/2004Phase1Proj/SecurityGuidelines.pdf)
and accompanying templates are available at no charge on the internet (www.gpcg.org). Finally, the Royal Australian College of General Practitioners has taken up the majority of the suggestions described in the guidelines and incorporated them into its Standards for General Practice which form the basis for practice accreditation in Australia.27

Other countries will need to adapt guideline implementation strategies to suit their own healthcare systems, the extent of adoption of information technologies and other organisational and political factors. The guidelines themselves will not be the same in countries with advanced rather than basic IT systems in health. For example, countries which already use shared electronic health records will need to add another layer of security. However, the principles of how to develop guidelines are relevant to countries that currently exhibit a range of IT practices within the primary healthcare sector.

ACKNOWLEDGEMENTS

We are thankful for the support of the General Practice Computing Group, the Australian Government and those interviewed.

The contributions of Grant Schiller from the ACE Division of General Practice, Matthew Rose from the ACT Division and Karen Young from the Monash Division for survey data on computer security are gratefully acknowledged. Professor Shane Thomas from the School of Primary Care, Monash University and Ms Mary Mathews, from the Monash Division of General Practice, Melbourne, assisted with earlier drafts.

A discussion about this article held at a WONCA Informatics Working Party conference in Prato, Italy in August 2006, provided helpful insights. WONCA also provided limited funding to help bring the authors together in Prato.

REFERENCES

27 www.racgp.org.au/standards

CONFLICTS OF INTEREST
None.

ADDRESS FOR CORRESPONDENCE
A/Prof Peter Schattner
Department of General Practice
School of Primary Health Care
867 Centre Rd
Bentleigh East, Victoria, 3165
Australia
Email: peter.schattner@med.monash.edu.au

Accepted April 2007