Australian Government

Department of Health and Ageing

BROADBAND FOR HEALTH

General Practice Security Awareness and Conformance Report

OBJECTIVE

The Australian Government Department of Health and Ageing (DoHA) is seeking to raise awareness of secure computer management in general practice. In order to attract the Broadband for Health incentive, practices are asked to complete and submit a Security Awareness and Conformance Report (SACR). The report requires responses to the levels of implementation, and as such, awareness of computer security requirements based on those listed in the checklist developed by the General Practice Computing Group (GPCG).

Practices who submit a completed report are eligible for an additional security incentive. The SACR responses will provide a situational analysis of the level of conformance to the GPCG security guidelines. Each of the checklist items requests a response in the categories of either 'Met', 'Partially Met', or 'Not Met'. Practices are also asked to comment on and/or qualify their responses. This will enable the network of divisions of general practice and e-health implementation teams to gauge levels of awareness, understanding, and acceptance or practical resistance to IT security. The information gathered may be used to target support on key issues or areas of deficiency.

The report is accompanied by an Action Guide which provides additional information and possible measures for each item. This will assist practices in further understanding the requirements.

DISTRIBUTION/REVIEW

The Security Awareness and Conformance Report is available online as a PDF downloadable from the Broadband for Health website www.health.gov.au/ehealth/broadband. The Report should be returned to Medicare Australia prior to or accompanying lodgement of the Broadband for Health incentive application form. A managed online form will be developed in the future to simplify the process and improve the efficiency of collating the data received.

Responses will be reviewed and collated to create a 'State of Play' of secure computer management in general practice. To assist in planning future activities surrounding practice security, DoHA will make the information gathered from this report available to the network of divisions of general practice and, where applicable, e-health implementation teams. While the sharing of information is optional, practices are encouraged to participate in order to benefit from additional support that may be available through these networks.

IMPORTANT INFORMATION

Without specific IT knowledge or experience, it is likely to be difficult for someone to provide qualified answers and/or supporting information to various items in the report. DoHA encourages practices to seek specialist assistance in completing the report. The information provided in the Action Guide is intended as an example only. In addition, technically competent IT assistance will improve the quality and accuracy of the report results collated. The information received will benefit the development of future work in the area of IT security practices for GPs.

To help achieve optimal results when completing the report DoHA would recommend that practices:

- Have a technically competent IT specialist complete the checklist on behalf of the practice. This service may be available through your practice manager, current IT support, your broadband supplier, or through your local division of general practice; and/or

- Refer to supporting education and guidance material developed by IT security and communications specialists. Examples include the GPCG Computer Security Self-Assessment Guideline, and GPCG Computer Security Firewall Guideline available at: www.gpcg.org/topics/security. These documents and other available material developed both nationally and internationally can assist in addressing areas of technology security which require further clarification.

SECURITY AWARENESS AND CONFORMANCE REPORT

Please insert your Broadband for Health Unique Identified Number (UIN): **BFH _ _ _ _ _**

IT Category	**Tasks**	**Implementation Status ☑**	**Comments on Status** *e.g. Date for review, activities in progress or planned, alternate strategy, assessment of risk, or countermeasure.*
Practice computer security coordinator	Practice IT security coordinator appointed	□ Met □ Partially Met □ Not Met	
	Practice IT security coordinator's role description written (for GP, existing staff member or practice manager)	□ Met □ Partially Met □ Not Met	
	IT security training for coordinator provided	□ Met □ Partially Met □ Not Met	
	Security Coordinator's role regularly reviewed Date of last review: …………………	□ Met □ Partially Met □ Not Met	Date for next review: ……………………
Practice IT security policies and procedures	Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual)	□ Met □ Partially Met □ Not Met	
	IT security policies and procedures documented	□ Met □ Partially Met □ Not Met	
	IT security policies and procedures documentation regularly reviewed Date of last review: ………………	□ Met □ Partially Met □ Not Met	Date for next review: ……………………
	Staff trained in IT security policies and procedures	□ Met □ Partially Met □ Not Met	
Access Control	Staff policy developed on levels of electronic access to data and systems	□ Met □ Partially Met □ Not Met	
	Staff have created personal passwords to access appropriate level	□ Met □ Partially Met □ Not Met	
	Passwords are kept secure	□ Met □ Partially Met □ Not Met	
	Consideration given to changing passwords periodically	□ Met □ Partially Met □ Not Met	
Disaster Recovery Plan	Disaster recovery plan developed	□ Met □ Partially Met □ Not Met	
	Disaster recovery plan tested	□ Met □ Partially Met □ Not Met	
	Recovery plan regularly updated Date of last update: ……………..…	□ Met □ Partially Met □ Not Met	Date for next review: ……………………

PLEASE FAX TO MEDICARE AUSTRALIA WITH YOUR INCENTIVE CLAIM FORM ON: (03) 6215 5448

SECURITY AWARENESS AND CONFORMANCE REPORT

Please insert your Broadband for Health Unique Identified Number (UIN): **BFH _ _ _ _ _**

Consulting room and 'front desk' security	Practice aware of need to maintain appropriate confidentiality of information on computer screens	□ Met □ Partially Met □ Not Met	
	Screensavers or other automated privacy protection device enabled	□ Met □ Partially Met □ Not Met	
Backups	Back-ups of data done daily	□ Met □ Partially Met □ Not Met	
	Back-ups of data stored offsite	□ Met □ Partially Met □ Not Met	
	Back-up procedure regularly tested (by performing a restoration of data) Date of last test: ………………….	□ Met □ Partially Met □ Not Met	Date for next test: ……………………
	Back-up procedure has been included in a documented disaster recovery plan	□ Met □ Partially Met □ Not Met	
Virus	Anti-viral software installed on all computers	□ Met □ Partially Met □ Not Met	
	Automatic updating of virus definitions enabled (daily if possible)	□ Met □ Partially Met □ Not Met	
	Staff trained in anti-virus measures as documented in policies and procedures manual	□ Met □ Partially Met □ Not Met	
Firewalls	Hardware and/or software firewalls installed	□ Met □ Partially Met □ Not Met	
	Hardware and/or software firewalls tested	□ Met □ Partially Met □ Not Met	
Network Maintenance	Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches)	□ Met □ Partially Met □ Not Met	
	Uninterruptible Power Supply (UPS) installed (to at least the server)	□ Met □ Partially Met □ Not Met	
Secure Electronic Communication	Encryption systems considered - Encryption used for the electronic transfer of confidential information	□ Met □ Partially Met □ Not Met	

To assist in planning future activities surrounding practice security, DoHA would like to make the information gathered from this report available to the Divisions of General Practice. Please indicate you preference:

□ Yes – you may share this information with the divisions of general practice network.

□ No – I do not want to share this information with the divisions of general practice network.

PLEASE FAX TO MEDICARE AUSTRALIA WITH YOUR INCENTIVE CLAIM FORM ON: (03) 6215 5448

ACTION GUIDE

The following table provides basic information and guidance for implementation of the Security Awareness and Conformance Report. Documents such as those developed by the General Practice Computing Group (GPCG) on security and firewalls will provide additional information. The Department of Health and Ageing (DoHA) encourages practices to seek specialist assistance in completing the report.

Tasks	Action Guide
Practice IT Security Coordinator appointed	□ Security management and operational responsibilities are to be allocated to individuals with the appropriate skills. It is critical that an individual is responsible for oversight of practice security.
Practice IT Security Coordinator's role description written (for GP, existing staff member or practice manager)	□ Security management and operational responsibilities are to be documented in a way that can be understood by all staff and can be allocated to individuals with the appropriate skills.
IT security training for coordinator provided	□ Individuals with IT Security responsibilities should possess the appropriate skills to fulfil the responsibility. This may include hands-on knowledge of IT security polices, risks and mitigators and/or formal IT security training courses. □ The responsibility of IT Security for practices may include the procurement of specialist skills for either selected or all IT security functions.
IT Security Coordinator's role regularly reviewed	□ The role is to be reviewed at least annually or more frequently in the event of significant technology change or in response to new IT security threats.
Person(s) (e.g. IT Security Coordinator) appointed to document (and revise) security policies and procedures (can be part of Practice Manual)	□ The role description of the IT Security Coordinator includes the function of documenting practice IT security policy and procedures. This is to be reviewed at least annually or in the event of significant technology change or in response to new IT security threats.
IT security policies and procedures documented	□ The practice shall have IT security policies and procedures documented in either a standalone manual or as part of its Practice Manual. The GPCG Security Guidelines provide a first step for developing a security policy. Specific practice standards and procedures will need to be developed.
IT security policies and procedures documentation regularly reviewed	□ The documentation is to be reviewed at least annually or more frequently in the event of significant technology change or in response to new IT security threats to ensure efficacy and adequacy.
Staff trained in IT security policies and procedures	□ All staff shall receive security awareness training including induction to the Practice IT Security Policy and Procedures. This should occur as an induction function for new staff and an annual refresher course for all staff. This should include a process of staff sign-off of an understanding of practice policy and procedures and of their individual responsibilities.
Staff policy developed on levels of electronic access to data and systems	□ An access control policy should be documented that details the access rules applicable to various staff functions and various information types (classifications). This should implement responsibilities in accordance with information privacy laws. In summary, this should restrict access to information on a business needs-to-know basis. For example, access to personal health records shall be limited to staff who need to access the material as a function of their role in the flow of patient care. □ Access control functions shall be implemented in computer systems consistent with the defined policy. This may include creation of server directories with differing access, logon and access restrictions to clinical applications. Most, but not all systems will have some security functionality to control access.
Staff have created personal passwords to access appropriate level	□ Access to information systems such as Local Area Network (LAN) servers, laptops and application systems shall be via unique User ID/password pairs (as a minimum) with each user's password being known *only* to the staff member to whom it is allocated. □ Administrator-set passwords shall be changed immediately upon allocation to Users who should select a password that can be memorized by the User.
Passwords are kept secure	□ Passwords should ideally be memorized and not stored in ways that could be easily obtained by other persons or programs, i.e. do not write on Post It Notes left on computer screens, desks in other areas where they could be uncovered. □ Passwords should not be shared between Users where accountability for system access or action is required.
Consideration given to changing passwords periodically	□ Passwords should ideally be changed based on the frequency of use, sensitivity of information that may be compromised, and the risk of compromise over time. This is a defense against a number of technical and non technical attacks on passwords, such as multiple access attempts over time (known as brute force password attacks), keystroke logging etc. □ Password frequency change options should be enabled on computer systems. The frequency of change of 30 days is considered ideal, however this may change depending upon the sensitivity of the information.
Disaster recovery plan developed	□ A strategy shall be developed and procedural details documented for the recovery of IT computer systems in the event of a disaster. This may be as simple as ensuring routine system backups are taken and kept offsite such that computer information is retrievable in the event of a disaster such as fire. The plan should include details of how computer systems will be restored, e.g. new servers procured and restored to a new or replacement practice environment. □ A strategy may involve the contracting of disaster recovery services or specialist skills if desirable.

Disaster recovery plan tested	□ The plan should be tested at least annually. This may involve the testing of server recovery procedures and the restoration of data and application systems. □ Testing may involve the contracting of disaster recovery services or specialist skills if desirable.
Disaster recovery plan regularly updated	□ The disaster recovery plan shall be reviewed and updated at least annually and in response to changes to computer systems impacting plan execution, i.e. server or other computer infrastructure changes.
Practice aware of need to maintain appropriate confidentiality of information on computer screens	□ Computer screens should be positioned so that contents are not easily viewable by the public.
Screensavers or other automated privacy protection device enabled	□ Secure screensaver options should be enabled for desktop/laptop systems (windows or other operating system functions) such that they blank any sensitive data and lock unattended systems after a period of inactivity. Sensitive information and restricted functionality should be automatically protected from unauthorised persons, ideally after no more than 15 minutes of inactivity. □ Session locking option at either LAN/server operating system or within application security should be enabled similar to the periods for screensaver. Additional third party security products for desktop and laptop security can be purchased that may apply greater protection in *locking down* these devices.
Back-ups of data done daily	□ Implement a backup procedure that backs-up data that has changed since the last backup. It is likely that a backup each night of server data or changes (incremental backup) is desirable for practices. The period between backups may be longer if the practice considers the risk of failure is lower, and its ability to recover or recreate data between backups is achievable (e.g. once a week backup). □ A procedure may implement an automated backup to a tape unit only when a manual procedure to eject the backup tape occurs. Backups may be done over a communications link to an alternate location or may be undertaken as a procured service offering via an ISP (Internet Service Provider) or ASP (Application Service Provider).
Back-ups of data stored offsite	□ A tape/disc backup or a tape/disc backup replica is to be securely stored offsite to be used for disaster recovery in the event of destruction of computer systems and local backup media.
Back-up procedure regularly tested (by performing a restoration of data)	□ Back-up restoration procedure is to be routinely tested to ensure the currency of the restore procedure and the efficacy of the backups. This may be accommodated within the testing process of the disaster recovery plan. Backup tape efficacy may also be proven on a more regular basis or on an ad hoc basis through restoration of corrupt or deleted data. Any failure in the backup process may result in an inability to recover system data.
Back-up procedure has been included in a documented disaster recovery plan	□ Back-up restoration procedure is to be included in Disaster Recovery Plan.
Anti-virus software installed on all computers	□ Anti virus product is installed on all personal computers, laptops and servers. □ Full system scans are conducted weekly on all devices.
Automatic updating of virus definitions enabled (daily if possible)	□ Licenses are current and virus signatures are downloaded as soon as there are available from software vendors. Ideally a *live* update facility should be employed and configured such that the updates are automatically downloaded when available
Staff trained in anti-virus measures as documented in policies and procedures manual	□ Staff awareness and procedures are in place for response to virus infections and limiting the likelihood of spreading a virus.
Hardware and/or software firewalls installed	□ Ensure firewall is installed between internal network and insecure public network such as the Internet. □ Ensure no other un-firewalled connections to insecure networks exist, i.e. creating an unprotected backdoor into your LAN. All communications traffic to and from the internal network must be routed through the firewall as the only route. □ All ports not required are turned off. Only required ports to be activated in rules. The default rule is to deny all connections to and from the internal network and authorise specific connection via firewall rules. Refine rules as desired to restrict inbound and outbound ports and restrict the use of services to authorised or identified network addresses. Refer configuration guidance on. The specific site (such as pathology reporting sites) may provide firewall configuration guidance.
Hardware and/or software firewalls tested	□ Check firewall rulebase each month to ensure it is current and applicable. Audit or engage an IT security specialist to confirm firewall is protecting against known computer hacking scenarios.
Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches)	□ Ensure hardware and software are kept up-to-date with patches as soon as possible after release. Processes will need to be put into place to monitor update releases. In some cases vendors may provide a notification or online update service. Focus on server and PC operating system security patches, and security products including anti-virus, network security and firewalls. □ Where possible ensure network equipment and in particular the firewall, is physically secured from unauthorised access. This may be in a lockable room.
Uninterruptible Power Supply (UPS) installed (to at least the server)	□ Implementation of standalone UPS device on critical server(s) for controlled shutdown period is advantageous in the event of a power outage. Assess practice requirement if this is cost/benefit-risk justifiable. If the impact on computer systems is not significant it may be justifiable to accept the risk of an outage. In same cases the building power supply may be UPS protected providing battery/generator power for a defined period.
Encryption systems considered - Encryption used for the electronic transfer of confidential information	□ Transmission of sensitive health information over the Internet (a public network) potentially exposes the information to unauthorised access. Encryption when emailing of health records over public networks should be implemented. This may require the exchange of cryptographic keys or certificates. □ Encryption of file transfer or other data exchanges of sensitive information over public networks should be implemented. This may require applications to implement security protocols such as SSL Secure Sockets Layer (SSL) or Internet Protocol Security (IPSec) and may require the exchange of cryptographic keys or certificates.