No Data
No Business

General Practice The National GPIT Group Information Technology

No Data No Business

It's unlikely that you will read these guidelines. Even if you do read them, it is unlikely that you will understand much of them. What we are asking of you is a leap of faith:

- Accept these Information Communication Technology (ICT) Security Guidelines as relevant to your practice;
- Make a decision to implement them;
- Identify an IT company, perhaps with the advice of your regional GPIT Facilitator; to carry out a security audit using these guidelines and checklist;
- Rectify any risks identified in the audit;

Let's be straight about it. The whole thing is going to cost you money, time and effort. It is much easier to do nothing. And you may get away with doing nothing. But the risk is great. The most important things in a practice are the staff, the patients and the information. How would you cope in the morning if your practice premises burned down? If your staff and patients were unharmed and you had an off site, up to date, backup of your data then you could be working again in 24 hours. If you have no data, you have no business!

These security guidelines were put together by John FitzGerald of Commnet. He is an IT expert who deals with security issues every day and is familiar with the needs of GPs and small businesses. The guidelines are written to make your IT support company aware of what needs to be checked and how your system should be configured to give you maximum protection. Risks change over time, so ensuring you are protected is not a one off task, it is an issue that you will need to revisit on a regular basis.

Here is a list of GPIT Facilitators, please contact them if you want some advice on these guidelines or in identifying an IT company to carry out the audit for you.

NAME	REGION	EMAIL	PHONE
Dr Donal Buckley	HSE Dublin/Mid Leinster	dbuckley@fitzmedical.com	01 6785100
Dr Fergus McKeagney	HSE Dublin/Mid Leinster	fmckeagneysurgery@eircom.net	05786 23183
Dr Martin White	HSE Dublin/North East	dr.martinwhite@gmail.com	046 9052109
Dr Anne Lynott	HSE Dublin / North East	drannelynott@eircom.net	01 8579397
Dr John Cox	HSE South	john.cox@drjohncox.ie	051 397111
Dr Frank Hill	HSE South	fghill@imagine.ie	021 4319087
Dr Kieran Murphy	HSE South	wmc@indigo.ie	068 42271
Dr Jack MacCarthy	HSE West	jackmaccarthy@mac.com	065 6844455
Dr Barry O'Donovan	HSE West	barry.odonovan@nuigalway.ie	091 797106
Dr John Sweeney	HSE West	johnnyhalflung@hotmail.com	074 9131344

General Practice Information Technology (GPIT) Group: www.icgp.ie/gpit

General Practice
Information Communication Technology
Security Guidelines and Checklist

Introduction

One of the goals of the General Practice Information Technology (GPIT) group is "to provide guidance and support to general practice on Information Communication Technology (ICT) infrastructure requirements" and a key area in ICT infrastructure is security.

Many practices now have a General Practice software system in place and the day to day operation of the practice has become reliant on its operation. General Practices have confidential patient information which must be protected.

To help practices deal with ICP security a security checklist has been developed which highlights key areas that should be addressed to prevent computer systems from being compromised. In addition to the checklist, security guidelines have been developed which give more detail on the key aspects of ICT security which need to be addressed and implemented.

General Practice Information Technology (GPIT) Group

The GPIT Group is made up of representatives from the Health Service Executive and the Irish College of General Practitioners. The members of the GPIT Group are: Mr Pat O'Dowd (Assistant National Director, PCCC), Mr Richard McMahon (Director of Information Systems, ICT Directorate), Mr Fionan O'Cuinneagain (CEO, ICGP), Dr Michael Boland (Director of Postgraduate Resources, ICGP), Dr Brian Meade (GPIT Co-ordinator) and Dr Brian O'Mahony (GPIT Project Manager).

The GPIT Group works in the following areas:

- Provision of education and training through the network of GPIT Facilitators;
- Publication of guideline documents on www.icgp.ie/gpit and articles in Forum;
- Maintaining a certification standard for GP software systems;
- Encouraging an integrated approach to IT in the health services;
- Promoting electronic messaging for efficient communication between primary and secondary care.

File name: Security Checklist and Guidelines rev4.doc
Date: 14/1/2008
Revision 4
Published by the GPIT Group, available at www.icgp.ie/gpit

GP ICT Security Guidelines

Policies Procedures

Some important user roles

One of the most important aspects of IT security, which aims to ensure that IT security issues are raised, addressed and resourced, is to appoint a security coordinator. It is this person's responsibility to ensure that any IT security issues are defined and addressed. One of the first tasks is to define the role of the security co-ordinator.

Computers break down and accidents happen. Being able to recover from such disasters is of the utmost importance and to this end the backup procedures and administration are crucial. It is necessary to assign someone with the responsibilities of backing up all the important electronic information in the practice and ensure that it can be restored.

Data Protection Commissioner

As a holder of personal health information you are legally required to register with the data protection commissioner. For more information connect to www.dataprivacy.ie. See also the Legal Aspects of Medical Computing handout on http://www.icgp.ie/index.cfm/loc/6-12-7.htm

Internet Usage Policy

Internet usage can be abused where inappropriate material can be accessed or the integrity of your computer system can be compromised. Hence, an internet usage policy is recommended. Please see the GPIT Internet Usage Policy document at http://www.icgp.ie/gpit.

Support agreements

It is a fact of life that computers can give trouble and you need to have support available when they do. Either have a maintenance contract or a 'pay as you use' support agreement in place for both hardware and software.

Firewall

A Firewall is a device or piece of software that acts as a barrier between your PC and the internet. On the internet there are continual scans and attempts to compromise machines. A firewall where all inbound traffic is blocked will stop these scans reaching your PCs and servers.

A hardware based firewall should be installed on broadband connections and a personal software firewall should be installed on PC with dial-up connections. Please note that most broadband routers have firewalling capabilities which may be sufficient for your network.

A specialised firewall or an upgrade of your broadband router may be required if you wish to implement other security features such as secure remote access. There are also firewalls available that will scan all inbound and outbound traffic for viruses and spam etc.

When implementing a firewall solution please ensure that the minimal amount of inbound traffic is allowed. Also ensure that the default password set on firewalls is changed and that a strong password is set. Disable the firewall management/configuration from the internet (usually the default setting).

If access is required into your network, for example remote support or you would like to work from home and require remote access, then make sure this is done in a secure manner. Use Virtual Private Network (VPN) technology where remote users should authenticate (logon) to the firewall and all traffic from the remote session would be encrypted. Web based tools such as WebEx (www.webex.com) or Citrix gotoassist (www.citrix.com) can be used for giving remote access to support companies. Using these solutions you connect to a secure web site and grant the support company access to your PC or server when they require it via your web browser.

Please ensure that your firewall policies/rules are documented and all access should be signed off. The company installing and configuring the firewall should provide you with the necessary documentation and only configure the policies that are signed off.

Malware

Viruses and spyware

Virus, Worms and Trojans are all software programs that run without your knowledge, are usually malicious and can damage your computer. A relatively new phenomenon is Spyware which is basically software that can monitor your activity, collect personal information such as passwords or credit card information. In some cases Spyware can take control or change the configuration of your computer and will often just slow it down.

Ensure you have anti-virus software installed on all your PCs and that it is set to update automatically. Virus definitions need to be updated on a regular basis to protect against new viruses that are being released every day.

Some antivirus software protects against viruses, worms and trojans but does not protect against spyware. Please check your antivirus software to determine if it protects against spyware and if not then either upgrade or change to a version that does. You may also wish to consider installing dedicated antispyware software.

Patches

Client and server operating systems may contain vulnerabilities that can be exploited to compromise or infect your PC. Service packs and security updates are regularly issued that fix these vulnerabilities. These patches should be applied to your machines to remove the vulnerabilities; the recommendation is to automatically install these patches. This is configured by clicking on the start button >Control Panel> Automatic updates and set the option to Automatically install.

Good practice

Some good practices that can protect against your PC being compromised is to

- Avoid opening suspicious emails or programs
- Never open an email attachment unless you are sure of the source
- Only download software from trusted sources
- Only use disks, CDs, DVDs, USB drives etc from trusted sources
- Check each PC on a regular basis to ensure the antivirus, antispyware and patches are up-to-date

Physical Security

Extra reliability and security can be gained by using a dedicated server. By not running applications or browsing the internet etc on a dedicated server, the chances of outages due to application corruption, memory leaks or getting infected by spyware or viruses is reduced. This server should run a network operating system such as Windows 2003 server which includes a centralised accounts database called Active Directory. This can simplify security administration in relation to user accounts and setting permissions.

A server should be stored in a secure location where only authorised people have access. There is less risk of either accidental or malicious damage when no physical access is available. The server should be connected to an Uninterruptible Power Supply to protect against power outages and spikes which could damage your server.

Hard disk failures can be difficult and time consuming to recover from. Recovery can involve reinstalling the operating system, reinstalling the backup software and restoring backups. Hence, consideration should be given to installing a RAID (Redundant Array of Independent Disks) controller on the server and RAID protecting the hard disks. This will protect you against a hard disk failure.

Access Control

Staff should only have access to the electronic information relevant to their role in the practice. This reduces the risk of accidental or malicious damage. Permissions should be set on shares, files and databases to only give the access that is required by each user.

Consideration should be given to running a directory service such as Windows Active Directory. This will give a centralised user accounts database, i.e. user accounts that can be used on any PC on the network. The alternative is a workgroup situation where users have local accounts on each PC. Administrative issues can arise when sharing out files and granting specific users permissions because your account on one PC is a different entity to your account on a second PC. Without the proper training this can be very confusing. In an Active Directory environment one account can be used on all PCs and permissions can be granted accordingly.

Staff should use their own individual accounts when logging onto Windows and when logging onto the GP system. In the event of accidental or malicious damage to data, with proper auditing enabled, it is possible to trace back to the account that caused the damage. Strong passwords should be setup on each account and the following table gives some guidelines in relation to using passwords.

Use of Passwords

PASSWORD DO'S

- DO use a password of at least eight characters
- DO use a random mixture of characters, uppercase, lowercase numbers and punctuation
- DO use a password with mixed-case letters. Do add uppercase letters throughout the password.
- DO change passwords regularly.
- DO use a password that can be typed quickly. This makes it harder for someone to steal your password.
- DO choose a password that you can remember
- DO use the first letter of each word from sentence or a line from a poem or song

PASSWORD DONT'S

- DO NOT share passwords with others
- DO NOT write a password on sticky notes, or writing pads where it can be accessed by others.
- DO NOT use your name or anyone else's name
- DO NOT use a word contained in English or foreign dictionaries
- DO NOT use a password of all numbers, or a password of all alphabet characters.
- DO NOT use pet names, license plate numbers, telephone numbers, car makes/ models, etc
- DO NOT use names or cartoon characters, Disney characters, etc

Laptop use

Laptops because of their portability present additional security threats. First of all they are more likely to be stolen.

Secondly, Laptops are often plugged into more than one network which can lead to more security attacks. For example, in the office the laptop may be behind a firewall but when taken home and plugged onto a home broadband or dialup connection it may not be protected by a firewall.

The following are some recommendations

- Install a personal firewall on the laptop as it may not always be protected by the office firewall.
- Keep the antivirus, antispyware and operating system patches up to date and check regularly.
- Do not store confidential information on laptops.
- If you have to store confidential information on laptops then encrypt the information. Products are available that will encrypt the entire hard disk, you are asked for a password when booting up the system and the system is unusable without the password.
- Do not leave unattended in non secure environments and do not leave the laptop visible in the car etc.
- Setup a secure BIOS (Basic Input/Output System) password. This will hopefully stop someone else accessing the information on you laptop. The strength of BIOS protection varies between manufacturers.

Wireless

Wireless access to your network brings additional security threats because you do not have to physically connect a cable to your network hub to gain access to your network. Wireless access could be available from your car park.

If you don't require wireless access then make sure the wireless is disabled on your broadband router or any desktops or laptops that may have wireless cards installed.

If you need to use wireless then you should perform the following tasks to make your wireless connections more secure.

- Change default SSID (Service Set Identifier) on wireless access point
- Don't broadcast the SSID
- Enable security features including Wired Equivalent Privacy (WEP) (use Wi-Fi Protected Access (WPA) encryption where available)
- Enter your own encryption keys
- Restrict wireless access based on MAC (Media Access Control) addresses

Backup Guidelines

What is backed up?

Make sure all your important data is backed up

- Ask yourself if I lost my computer what information do I want to get back?
- Along with your GP Software System are there any other documents, email that you would like to protect

Hold multiple copies

Sometimes problems can occur that are not noticed for a while, for example a file can be deleted or data can be corrupted. In these situations the most recent backups are backing up the corrupt file or not backing up the missing file. The only way to recover data is to hold multiple backups that go back over a period of time.

The recommended method is the grandfather father son method where you have backup media for each day of the week with a different media for each Friday in the month and a different media for each month of the year.

WEEKS	USAGE OF BACKUP MEDIA (TAPES OR ZIP DISKS ETC)
Week 1	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY1
Week 2	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY2
Week 3	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY3
Week 4	MONDAY TUESDAY WEDNESDAY THURSDAY MONTH1
Week 5	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAYI
Week 6	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY2
Week 7	MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY3
Week 8	MONDAY TUESDAY WEDNESDAY THURSDAY MONTH2

The table above shows how this system works over an 8 week period. Every Monday you use the same backup media. On the first Friday of every month you use the Friday1 media etc. Note 9 tapes used over an 8 week period. Approx 20 tapes required for one years backup schedule. The media is typically a tape or zip (Iomega) disk but can also be DVD disks, memory sticks etc.

Keep backups off site

Keep your backups off site.

- You need to protect against damage from fire, floods, theft etc.
- Ask yourself the question "If your premise burns down what data will you have left?"
- If you loose your server and backups what effect has it on your practice?
- Backup media stored in fireproof safes may not burn, but can melt and be unusable

Keep the backup media off site in a secure location (e.g. locked cabinet) as sensitive confidential information is stored on the media.

Test restore

The ONLY way to verify a backup is to restore it.

- Always assume you do not have a backup until you can restore it.
- Perform test restores regularly.

Software system backup procedures

Implement the backup procedures recommended by your GP System provider. If you don't follow these procedures then you may not have a good working backup !!

- E.g. Some software systems required you to stop SQL services or logout of the system prior to running a backup:

GP ICT Security Checklist

Policies Procedures

- Assign the role of IT Security coordinator
- Assign the role of IT Backup coordinator
- Register with data protection commissioner
- Software support in place
- Hardware support in place
- Implement an internet usage policy
- Develop and test a disaster recovery plan

Firewall

- Firewall protect your network
- Set a secure password on your firewall
- Minimise the traffic that is allowed into your network
- Use VPN for remote access
- Use secure remote support
- Document and sign off on your firewall policy

Malware

- Antivirus software installed and up-to-date
- Antispyware software installed and up-to-date
- Install operating system patches and service packs
- Avoid opening suspicious emails or programs
- Only download software from trusted sources

Physical security

- Use a dedicated server
- Keep server in a secure location
- Server should be connected to a Uninterruptible Power supply (UPS)
- RAID protection on server to protect against disk failure

Access Control

- Run a directory service such as Windows Active Directory to give centralised user accounts that can be used on all PCs
- Password access required on all PCs and servers
- Staff to use individual accounts in Windows and the GP system
- All accounts should have "strong" passwords
- Permissions set to only allow authorised staff access to data

Wireless

- Change default SSID on wireless access point
- Do not broadcast the SSID
- Enable security features including WEP (preferably use WPA encryption)
- Enter your own encryption keys
- Restrict wireless access based on MAC addresses

Laptop use

- If possible do not store confidential information on laptops
- Encrypt any confidential information on laptops
- Do not leave unattended in non secure environments
- Keep the antivirus, antispyware and patches up to date
- Install a personal firewall

Backups

- Back-up ALL important data, documents, email and GP system
- Backups - run and checked daily
- Implement any GP system backup requirements
- Backups stored off-site in a secure location
- Test restores on a regular basis