Irish College of General Practitioners

IT Security for Irish General Practice

January 2020

IT Security for Irish General Practice

Introduction and Overview

Having a functioning computer network system has become a requirement for modern General Practice to operate efficiently. The purpose of this document is to assist you (the GP) in ensuring that any needed steps are taken to maximize the safety and productivity of your network.

Following the introduction of GDPR, there is much more of a responsibility on us to protect sensitive patient data. This work is becoming increasingly difficult with the rising realisation that small business data, especially GP data, is a tempting source of data for identity theft from hackers.

This document was prepared by the General Practice Information and Technology (GPIT) group to act as a guide to practices to keep their systems as safe as possible in today's IT climate.

The purpose of the document is to:

- Give an overview of security systems to consider for your practice.
- Provide an adaptable checklist for your practice.
- Outline the practice policies that should be embraced to improve IT security.

This document could be brought into the Practice as a working document, to allow the GP to make the checklists part of practice routine and refer to them in the likely situation when there are problems with your computer system in the future. The document is in three main sections, an overview, appendices to focus on some of the specifics and finally some use cases in practice.

In general, most GPs realise the importance of protecting their computer systems and having policies in place to ensure security is always maintained. But computer security for many is hard to embrace as there is a general perception that there is a need to understand the complexities of computer systems. The truth is sensible policies put into practice far outweigh any needed technological tweaks.

Start with appointing one (or two) people within the practice to act as the Practice IT lead. It would be wise to use the same person who serves as the data officer for the practice currently. The checklist on page 3, which if adhered to, will improve the IT security of your practice going forward.

This document was developed by a collaboration of the national GPIT group.

For more information, see: www.icgp.ie/gpit

Illustrations by Kevin Gallagher (www.kevingallagherdesign.com).

Category	Tasks	Has it been implemented/date	Useful contact numbers/notes
1.Practice IT lead	Appoint Practice IT lead. Define their role.	Name: ________ __/__ /__	
2.Policies and procedures	Are policies and procedures documented? Are staff trained on policies and procedures?	__/__ /__ __/__ /__	
3. Access control	Is there a policy on staff levels of access to information? Are individual passwords safe and secure?	__/__ /__ __/__ /__	
4. Computer and network maintenance	Physical security of server and network. Policy on screen security. Are all automatic updates running? Are UPS and surge protectors in place?	__/__ /__ __/__ /__ __/__ /__ __/__ /__	
5. Network Controls	Are perimeter controls installed? Are any intrusions or breaches being logged?	__/__ /__ __/__ /__	
6. Malware and viruses	Is antivirus and malware software installed on all computers? Are staff trained on malware procedures? Are automatic scans enabled?	__/__ /__ __/__ /__ __/__ /__	
7.Portable devices and remote access	Is there secure storing of backup data? Are wireless networks configured? Do you have a policy on the use of mobile devices?	__/__ /__ __/__ /__ __/__ /__	
8. Secure electronic communication	Use of Healthmail for patient info email. Do you have a policy on email and internet use in the practice?	__/__ /__ __/__ /__	
9. Backup/Recovery	Is there a daily back up with a periodic offsite stored backup?	__/__ /__	
10. Disaster recovery	Are disaster plans developed and tested?	__/__ /__	

Section 1: Practice IT lead

This job is a managerial/leadership role. Though not specifically technological, it is essential to understand the policies and procedures needed to keep the practice safe and how to get the critical information across to all staff in your practice.

The Practice IT lead needs to ensure all the recommendations are fulfilled and updated in the checklist. We would recommend an annual review of the list, periodic (quarterly) checks on hardware and software issues and daily backup of your data.

Ensure someone is shadowing the Practice IT lead's role in the unfortunate circumstance they are off on leave. The Practice IT lead may be one of the doctors, a nurse, a senior receptionist or the practice manager.

Role of Practice IT Lead

- Documenting and clarifying the computer security roles and responsibilities of all staff.
- Writing and updating the security policies for the practice, this could be based on this document, and if so, ensure it is kept up to date. These would include backups, access control, internet/email usage, malware/virus protection, wireless and mobile connection, perimeter controls, physical security of computer systems, disaster recovery plans, and business continuity plans.
- Training staff, focusing on ongoing security concerns.
- Maintenance of licencing registers; hardware, software, installation media, and digital certificates.
- Knowing who and when to call for technical support, by keeping phone numbers in the checklist. As well as the phone number of the technical support person consider including the software vendor helpline, phone provider, healthlink etc.
- Ensuring the practice is aware of any outstanding security issues and report at regular practice meetings

Section 2: Policies and Procedures

Consider developing a Practice IT security manual to document the security policies and procedures for the practice.

Policies and procedures include:

- This manual should describe the part of the Practice IT lead, as well as outline the procedures for backup and all the points in the checklist.
- Consider keeping a log of all hardware and software in the surgery. Make a note of the age and what operating system each computer station is using and maintaining dates for renewal and warranty on the equipment.
- Consider asking your IT technician to perform a risk assessment (penetration test) of the practice to identify apparent weaknesses.
- Have a business continuity plan for what should be done when no computers are operating for whatever reason. How can the practice return to a paper-based process to keep the practice running?
- With the rise of ransomware, it would be sensible to stop any personal email being received into the practice network. There should be one standard email account for the practice operated by the Practice Manager, to run regular business emails. If there are any unexpected emails with attachments to this account (even by known sources), then the sender should be phoned to check if they sent the email before opening the attachment.
- It is wise to have an email, and internet policy that has been understood and signed off by all members of staff.
- You should have a practice policy on what types of information is shared with patients using SMS or email messaging.

Section 3: Access Control

A cornerstone of data security in General Practice ensures that only those people that should be allowed access, are granted access to particular types of information. It is wise to consider a policy of allowing only authorised employees get access to specific information and systems.

In general, there are four levels of access to consider.

1. Systems administrator- Usually, the IT support person who will have access to the server and network environment.
2. Practice manager- Has access to financial, clerical and network systems.
3. Receptionists- Has patient administration access.
4. Clinical staff- For the clinical programs, these roles can be further subdivided between the doctors, nurses and other allied healthcare professional.

Policies regarding access control include:

- Everyone should use a password or some other unique authentication method, (other methods could include key fobs, fingerprint verification and, swipe-card).
- Consider staff that no longer work in the practice. Ensure their access will be turned off when leaving the practice.
- Under Data Sharing and Governance Act 2019 you will be required to have a data sharing policy in place for outside agencies who can access your data. That would include the practice IT technician, the Practice software company, Healthlink, pharmaceutical companies (running audits of your patient data) and companies you use to destroy old files.
- Don’t forget to have signed confidentiality agreements for your trainees, interns, and visiting medical students.
- Most Irish practices will use passwords for access control. It is worth considering drawing up a policy document on password security for staff. For most practices, there are multiple passwords required, usually one for the operating system and another for the practice management software.
- Everyone must have a unique password. Ideally, that is at least eight characters long with both upper- and lower-case letters and one or more numbers or symbols. Consider using phrases as passwords rather than words, as these are more easily remembered giving added security. Staff should be encouraged to change passwords periodically and not leave them written down around their workstations.
- As employees can be working in the practice on different days, using different terminals, it would be wise for the Practice IT lead to keep a list of all network passwords, to let others use the computers. But keep the list stored securely in a safe.
- Consider getting the IT technician to set up audit logs through Windows Active Directory. This will provide details of who is accessing, downloading, changing and deleting information. The audit logs should be reviewed periodically and retained in case information is required following an information security breach incident.

Section 4: Computer and Network Maintenance

Computer maintenance is an essential role for the Practice IT lead and should be logged and dated regularly. There are hardware and software maintenance tasks that need to be carried out periodically on all stations. This is above the role of the outside IT technicians that the practice may use. External IT technicians may well perform some of these functions, but the Practice IT lead should still be aware of these tasks.

Computer and hardware maintenance can be further broken down into the following:

a) Hardware maintenance

- The setup of the practice's network is vital as workstations and servers can be physically lifted and stolen. Consider tethering the server to the wall and be aware of increased theft risk with laptops. Ensure all computers and servers get a regular clean, particularly around the air vents, as they can build up with dust and overheat.
- If the servers are stored in a separate communications room, ensure there is no direct sunlight on the server, and the room is always locked.
- When computers have reached the end of their life and are being replaced. Ensure that the hard drives are removed and destroyed or recycled by a reputable organisation. When using a company to destroy old drives/computers, consider drawing up a confidentiality agreement with them and request a certificate of destruction.

b) Software maintenance

- Understanding that a lot of malware targets the automatic updates in operating systems and the antiviral software. It is always good practice to periodically go through all terminals in the practice to ensure ‘Windows’ (or another operating system) updates are running automatically. Ensure automatic updates are always left turned on.
- Consequently, it is vital that the practice is not running any old operating systems that are not getting any more future updates.
- Finally, when checking the windows updates, it is good to check that antiviral software is automatically updating and sweeping your data.

c) Screen confidentiality

- It is vital that computer screens are not visible to unwanted eyes, both beside a window or in the shared reception areas. Therefore, it is important to ensure that screen savers activate shortly after someone leaves a workstation. Consideration should be given to password protect the screensaver, as non-authorised practice workers could be viewing sensitive data when everyone else has gone home.
- A good tip, when leaving a computer unattended with a patient in the room, would be to “lock the screen” by pressing the Windows key and L. This will close any open session onscreen and will require authentication to reopen.
- For the reception area consider installing a glass sneeze guard to prevent anyone leaning over and viewing the computer screen. It also protects the front of office staff from non-software viruses. As well as some physical protection, a sneeze guard can also provide soundproofing, protecting patient privacy when staff are discussing patient’s details behind the reception area.

d) Other Hardware Considerations

- It is important to have a UPS (uninterruptible power supply) in place. A UPS is effectively a battery connected to the server, which will power the server and monitor for a short time, in the event of a break in electricity supply.
- If the electric power goes off, then someone should shut the server down to prevent the loss or corruption of data. It is wise to periodically check the battery life of the UPS and order a new battery when it's getting low.
- Consider installing surge protectors at all computer terminals and the server. Include your internet modem to be covered by the surge protector as these devices are vulnerable to damage in electrical storms.

Section 5: Network Controls

Network perimeter controls are the hardware and software tools used to protect the network. These systems analyse data flow. They are often referred to as firewalls or intrusion detection systems.

- There needs to be a balance in security and obtaining outside connection for the practice, such as remote access. If your practice system allows external network linking, like a peripheral surgery laptop, then extra protection such as VPN (a virtual private network) needs to be considered.
- For any computer networks, it is advisable to invest in a hardware firewall and have it configured so only authorised information is permissible to enter and leave the practice.
- Consider investing in a software IDS (Intrusion Detection System). The IDS will create an alert when there has been unauthorised access to the network, allowing necessary action to be taken.
- Antiviral software should be a part of the network controls and should be installed and operating on all machines.

Section 6: Malware and Viruses

Malware is a type of software program created by hackers which, when inadvertently activated on a computer networked system, will search for private information or can corrupt the data. Malware viruses are generally introduced to the network through the internet and especially via emails. They can also be transmitted through media like USB flash drives and CDs.

Care should be taken when opening any attachments, even from trusted senders. It would be advisable not to click any hyperlink from pop-ups recommending an update to specific programs. Hover over a hyperlink (to view the URL of the site) before clicking it, this will ensure it is a reputable site.

1. Malware can take on different forms, including:

- Viruses and worms- code that attaches to files and spreads from one computer to another.
- Trojans- Malware disguised as a real program.
- Phishing- Fake emails/websites attempting to get usernames/passwords and credit card details.
- Spam- Unwanted junk email.
- Spyware/adware-Advertising supported tracking software. These can collect keyboard keystrokes (for obtaining passwords), and the details of sites visited on the internet.
- Ransomware- This type of virus corrupts files making them unusable and then demands a ransom to reverse its effects. The common advice is, don’t pay the ransom as can give further access for the hacker to corrupt even more of your files.

2. Reducing the threat of viruses

The threat of malware can be limited by investing in appropriate antiviral software. Remembering, that it is not safe to use free antiviral software for your practice data. Practice process around the use of the internet and email are critical, as it is through human actions that many of these malicious programs get activated. Consider limiting access to the practice email to one or two individuals who are trained to recognise suspicious emails. Also, because spyware can be tracking keystrokes and collecting passwords it is wise to update passwords frequently.

It would be sensible for the Practice IT lead to log checks on all terminals to ensure that antiviral software is installed and running. Make sure automatic updates and scans are turned on. Keep in mind that a lot of malware will try to turn off automatic antiviral uploads and sweeps.

Section 7: Portable Devices and Remote Access Security

Mobile devices include laptops, USB flash drives, removable hard disks, smartphones and backup tapes. All these hardware devices have an increased risk of getting lost or stolen and because of this, require increased security consideration.

- Storage of the backup tapes both on and offsite should be in a locked device. Bear in mind fireproof cases will not prevent backup tapes from melting. All of these backups have patient data on them, so the storage of tapes must be secure.
- For all portable devices, ensure proper password protection and consider encryption technology.
- Remote wireless access to the network may be beneficial for peripheral surgeries or house calls, but this increases the chance of unsolicited hacking into the practice data. If remote access is to be used in a practice management system, it is worth getting technical advice on how best to protect the network. It would be advisable to consider installing Virtual Private Networks (VPNs) for this functionality.
- Many surgeries run wireless internet, and some advertise free Wi-Fi for patients in the waiting room. If the wireless system runs on the same network as the practice management software, this data could be open to attack. If the practice wants to offer patients or staff free Wi-Fi, then a separate network may need to co-exist alongside the practice management system.
- It may also be advisable to configure the wireless network, in such a way that it would be difficult for someone to access it. Change the SSID (how the network appears on a device), so it's not recognisable as belonging to a health centre and ensure the default modem passwords are changed at setup. Ensure the modem connection protocol is set to WPA2 (Wi-Fi Protected Access II) rather than older less secure WEP (Wired Equivalent Privacy). This may need the assistance of the hardware provider or appropriate technician to achieve.
- If any outside parties legitimately access the practice network through remote access, then there will need to be security agreements in place. This would involve the practice IT technician; any GP software companies and Healthlink.
- Consider the risks when any files are taken home to be worked on in the evenings and eventually returned to the network. Ensure the files are not carrying malware before being loaded back into the practice.
- In the last few years, there has been increased use of smart devices for gathering health data, from implantable glucose monitoring devices for diabetic patients to smartwatches collecting ECG data. Bear in mind that these devices have their own security limitations. These can be hacked and can be the cause of computer virus infection. In the future, more of this data will be brought into the patient's medical notes which could increase malware risk. Also, take into consideration that some of these devices may store patient data outside the EU, which will require separate security considerations.

Section 8: Secure Electric Communication

Practices transferring sensitive patient information should use Healthmail where possible and never use standard email unless the patient information is encrypted or with explicit and informed patient consent.

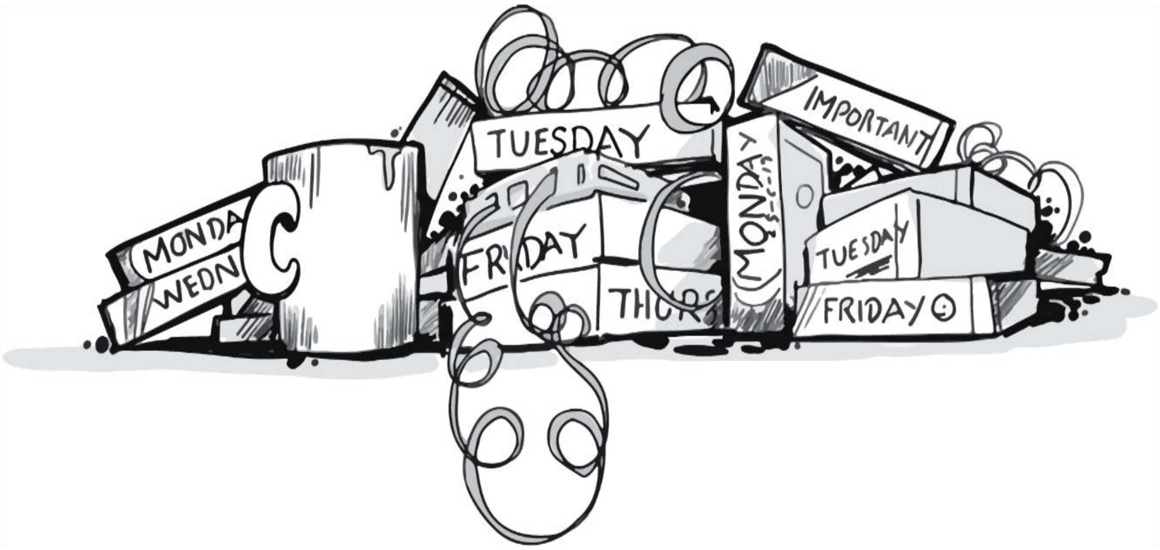
Patients may sometimes communicate with GPs by email, but Healthmail cannot be used for this purpose. These patients should be informed that communicating by standard email is not secure, and consent should be obtained before doing so.

- Health messages are sent to and from GP practices every day using HL7 messages through Healthlink. These messages are secure as they are encrypted, and they will only pass through authentic computers that have data certificates installed.

Section 9: Backup

When considering a backup model for the practice, the first question that must be asked is, how much historical data can the practice afford to lose and how far back can that data be lost?

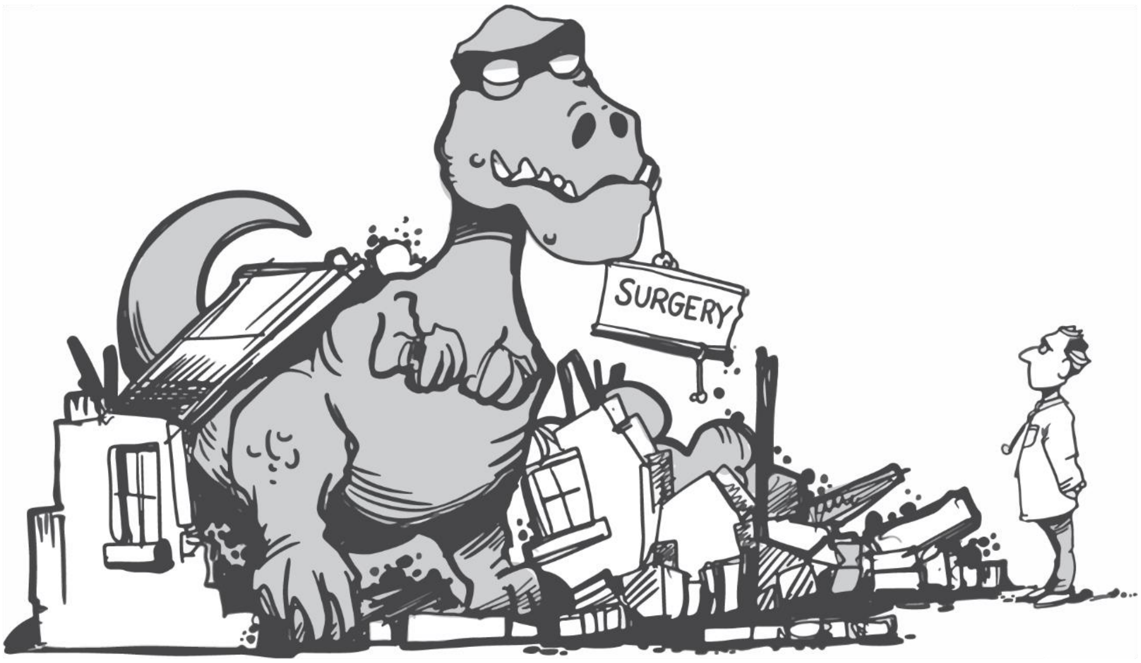
- It is advisable to use both hardware and a cloud system to back up practice data. There are many companies offering cloud data backup with data recovery. If not currently in place, consider investing in cloud backup with the hardware provider.
- Some practices using tape backup will use five tapes circulated every day. This process can be unsafe as it could take a few weeks for ransomware infection to become apparent, by which time, the system has already been compromised, and the backups infected. It is also advisable to store a tape or two offsite, in the event of a practice fire or flood, where all inhouse media could be destroyed.
- A valuable task for the Practice IT lead is to ensure not only that patient data is backed up, but a consideration is also needed for the accounting files, or other practice administration data. Ensure these files are getting backed up on the server, on a regular basis.
- Backup installation will require the assistance of the IT technician, and it would be advisable to get them to periodically check that the backups are working correctly, and these can be used to restore/recover the patient data.
- Consider drawing up a backup register, where the backups are logged with date and signature of those performing the backups.
- It is good practice when installing a new server to ensure it is a RAID (redundant array of independent disks) server. These servers run with multiple mirrored hard drives so if one hard disk fails the next will take over the disk function automatically with no interruption to the network.
- Caution should be used when working with online backup systems. Be mindful that the footprint of the company's servers should lie within the EEA (European Economic Area) to satisfy GDPR. There should be a data sharing agreement in place outlying the duties and responsibilities of both parties in ensuring patients information is protected.



Section 10: Disaster Recovery

This section describes procedures when there are disruptions in the computer systems' operations. These disruptions may be internal, localised (to one terminal) or external (involving power or telecommunication failures). In extreme cases, the surgery could be destroyed.

- Develop a plan that will outline steps that will get the business operating as efficiently and quickly as possible.
- Consider who to call for help and at what stage they should be called. Having the phone numbers on a checklist becomes useful, and remember, the checklist must be available from outside the failed system.
- Take time to consider what steps would be needed if the practice had to revert to a paper-based system, as the users have come to rely on computer-based systems over the last few years.
- The threat of Ransomware is on the increase and can easily cause the locking down of a computer network. Therefore, it is very important that all practice staff have a clear understanding of safe email and internet policies. If a practice is subjected to a ransomware attack, the IT technician will have to revert to the backup system before the primary system got infected. As it is difficult to get insurance for ransomware attacks, financial fines from the Data commissioner and compensation to affected patients, will have to be borne by the practice.



Appendices

Appendix 1

Practice Internet and email policy

Introduction

Policy Objective

To ensure internet facilities provided in general practices are used correctly in connection with official duties. The use of personal email is restricted to the practice network. Personal emails should only be viewed on non-network devices such as smartphones.

If using an email account that is not a Healthmail account for practice business, ensure policies are in place to maximise security to your network using that email account.

Scope

This policy applies to all internet services provided in general practice, which includes all users and uses of practice internet services.

Monitoring of Internet Usage by the practice

Internet Monitoring

Internet services are provided to authorised employees, authorised trainee general practitioners and interns in general practice, permitted students, work placement staff and in some cases authorised third parties, for use in connection with official duties only. All internet activities are tracked and logged automatically.

The internet usage records of each user shall be accessible by the Practice IT lead or general practitioners. The practice IT lead will not routinely monitor individual users use of the internet but will have the right to access the internet history logs of the individual users to deal with routine work-related matters, for example during periods of an employee's leave.

The Practice IT lead or General Practitioners will respect the privacy of users when accessing internet history logs and will not access items of a personal nature unless there are compelling conditions that warrant doing so. (An example of a persuasive situation would be the detection and prevention of fraud.)

While the practice does not routinely inspect user's internet history logs, it does reserve the right to do so:

a. For technical reasons associated with tracing and remedying technical faults and improving performance
b. When required by and consistent with law
c. When there is a reason to believe that violations of the law or practice policy may have taken place

Internet Usage

Acceptable Usage

Internet facilities provided by the practice may only be used for official purposes in connection with work. This includes using it for training, educational, or research purposes if this is associated with work-related activities or tasks.

While the practice does not routinely provide internet facilities for third parties, for example, medical students or students on work placements, if it does, then such services must only be under this policy.

Unacceptable Usage

The practice's internet facilities may not be used

a. For unofficial or personal purposes, even outside regular working hours.
b. To transmit private or confidential information outside the practice, unless it is appropriate to do so with the necessary facilities are in place to protect such information, for example by using Healthmail.
c. To knowingly misrepresent the general practitioners or the practice.
d. To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of contract is required).
e. To retrieve, create, host or transmit offensive or obscene material, which would cause offense to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs, or would bring the practice into disrepute.
f. To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others.
g. To recover, produce, host or send defamatory material.
h. For any activity that would infringe intellectual property rights (for example software piracy).
i. For any action that would compromise the privacy of others.
j. For any action that would waste the practice's resources (e.g. staff time and I.T. equipment and networks).
k. For any activity that would compromise the security of the practice's I.T. facilities, including confidentiality and integrity of the patient information and availability of I.T. services (for example by carelessly causing computer virus infection).
l. For any illegal activity.

Only internet facilities provided by the practice may be used in connection with private and or confidential information.

Internet facilities may only be used by users to whom the practice has directly provided these facilities. Users may not use other users' internet facilities.

Internet Security

Internet Privacy and Confidentiality

Confidential information must not be transmitted via the public internet. Transmission of patient information must be done using secure communication such as Healthmail. It is acceptable to exchange information with services such as Healthlink and PCRS. These sites are designed to authenticate users and exchange information securely.

Roles and Responsibilities

Internet Users' Responsibilities

Each user of the practice's internet facilities is responsible for

a. Complying with the policy contained herein this document.
b. Complying with instructions issued by the IT practice lead or general practitioners.
c. Attending appropriate training courses, as provided or arranged by the practice, so that he/she is aware of the proper use of the internet.
d. The data downloaded or uploaded via their use of the internet.
e. The privacy of his/her password(s) and other similar confidential authentication information.

Breach of this Policy

The general practitioner reserves the right to take such action as he or she deems appropriate against users who violate the conditions of this policy. Such violations will be regarded as a disciplinary matter for staff. For non-practice staff, action will be taken in conjunction with their educational institution, employer or relevant authority.

The practice may withdraw computer systems facilities from any computer user who it believes is not complying with this policy or who misuses computer systems in any manner.

The use of computer systems for illegal activities by any computer user is a breach of this policy and may result in prosecution. The practice will not afford any protection to employees or others who engage in such activities and will co-operate fully with, and provide whatever information may be required, to facilitate investigations into such activities.

Staff Acceptance

Signatures

I confirm I have read and understood this practice internet usage policy and accept its terms and conditions.

Print Name	Signature	Date

Appendix 2

IT Dos and Don’ts for New Staff

Do

- Read and sign the acceptable internet and email policy document (Appendix 1).
- Change passwords frequently.
- At the end of the day leave workstations turned on. Close applications down on the desktop, allowing configured updates to be installed outside of surgery hours.
- Consider a screensaver password which activates when the user leaves the workstation.
- Report any known data breaches/virus infection and ransomware notifications to the practice IT lead immediately.
- Understand what information can be shared to patients through SMS texts and email messages.
- Be mindful of unauthorised people being able to see computer screen over the shoulders of practice staff or through glass panels or windows.
- Consider backing up important nonclinical files on terminal desktops to the server.

Don’t

- Give passwords to anyone else or leave passwords written down at workstations.
- Leave identifiable patient information on open files on computer desktops.
- Open pop-ups on websites when browsing the internet.
- Open any unexpected attachments in emails especially unanticipated receipts.
- Look at email on the practice network or open attachments on the practice network. Users should use their smartphones for this.
- Use the practice internet for purchasing products.
- Open files from external sources from home or USB sticks without screening with antiviral software first.

Appendix 3

A Checklist to run by your Hardware Technician

For those who find this document too technical, this is a checklist to show the IT technician. This checklist is to ensure the practice network meets a minimal security level to operate in the current computerised climate.

a) Check Windows (or other operating system) and, anti-virus software is adequate, and updates are running automatically.
b) Check Audit logs are operating through Windows Active Directory.
c) Ensure personal internet access is separate from the LAN – for email, google etc. – Consider using a guest Wi-Fi network, which is- WPA2 and that WEP is disabled, normal portal and not captive portal, internet access only and no LAN access.
d) Passwords for Windows and practice management software should be in place with timeouts.
e) UPS and surge protector should be used– check the UPS battery life.
f) Check hardware firewall is in place and operating.
g) Check software Intrusion detection is in place and operating.
h) Malware and Virus. Establish what software is adequate – how to and how often to physically check that they are running automatically.
i) For peripheral clinics it is wise to use VPNs and may be a need to consider Encryption".
j) Guest Wi-Fi – security issues – do you need a separate network and what this entails.
k) Changing SSIDs and network passwords and disabling WEP.
l) Setting up backups (test recovery of data – how often and how expensive).
m) Consider laptop encryption – Bitlocker in Windows 10 pro.
n) Check need for encrypting external hard drives, memory sticks.
o) Check is there a possibility of performing a penetration test on the network.

Appendix 4

Wireless and Mobile Device Policy

If the practice is running Wi-Fi internet access through the practice network, it is wise to configure the router correctly to improve security.

Never use the default router password to access the network as this can be read off a sticker attached to the router. Change the WI-FI name, so it is not apparent to anyone looking for a wireless network that a GP practice is accessible. Use WPA2 for Wi-Fi passwords.

Mobile data devices like backup tapes and laptops have increased security concerns as they can be easily stolen, so take extra care in the safe storage of these mobile data devices.

If using laptops for remote surgeries, ensure they are protected with virtual private network (VPN) technology.

Appendix 5

Password Policy for Practice

Consider adopting a system in practice for passwords and passphrases.

On most terminals, there are 2 stages of password entry, one to get into the operating system and the other to access the Practice management software. It is advisable to get staff to change their passwords regularly, lessening the risk of a data breach by spyware hacking.

Never leave passwords written down beside computer terminals.

For Practice management software, the passwords are only going to be used by one individual, and they should remain private to those individuals.

If computers are used by different people throughout the week, it is sensible for the Practice IT lead to keep a record of the operating system login passwords for all terminals. These passwords must be entered after any updates and restarts. This password list should be stored securely. Remember that it will give open access to an individual computer terminal, but not directly access the sensitive practice management software data.

Appendix 6

Policy on Data Backup with External Media

As mentioned in the main text, it is wise to backup practice data, ideally with cloud backup with data recovery. If some practices still use tapes or mobile hard drives for backup, it is worth ensuring the practice uses a robust method to ensure security.

A backup method to consider for external media is the grandfather father-son method, where there is a backup media for each day of the week with a different media for each Friday in the month and a separate media for each month of the year.

Weeks	Usage of Backup Media
Week 1	Monday Tuesday Wednesday Thursday Friday1
Week 2	Monday Tuesday Wednesday Thursday Friday 2
Week 3	Monday Tuesday Wednesday Thursday Friday 3
Week 4	Monday Tuesday Wednesday Thursday Month 1
Week 5	Monday Tuesday Wednesday Thursday Friday 1
Week 6	Monday Tuesday Wednesday Thursday Friday 2
Week 7	Monday Tuesday Wednesday Thursday Friday 3
Week 8	Monday Tuesday Wednesday Thursday Month 2

The table above shows how this system works for over eight weeks. Every Monday you use the same backup media. On the first Friday of every month you use the Friday 1 media etc. It should be noted that 9 tapes are used over eight weeks. Approximately 20 tapes would be required for one year's backup schedule. The media is typically a tape or zip disc but can be DVDs, portable hard drives, etc.

Backup installation will require the assistance of the IT technician, and it would be advisable to get them to periodically check the backups are working correctly. Also ensure the backup can be used to restore the practice management data. As not only the patient data should be backed up, consider backing up the accounting files or other practice business data that are used, and ensure it is getting backed up on the server.

Date	Tape number	Person Responsible	Signature

Appendix 7

Performing and Automating Software Updates

Depending on whatever operating system is used in the practice, ensure software security updates are automated and turned on. To tell what operating system a computer is running on, right click on the "my computer" icon and check the properties.

For Microsoft Windows Computers

For Windows 8

Open the **Control Panel (icons view)** and click on the **Windows Update** icon. In the left pane, click on the **Change settings** link. **To Turn on Automatic Updating:**

A) In the drop-down menu under **Important updates**, select **Install updates automatically**.

B) Click on the **maintenance window** link to set the **automatic maintenance** window for what time you would like to have updates checked for and installed, and if you would like to wake up your computer to do so. *By default, the time is set to **2:00 AM***.

For Windows 10

Windows 10 uses its own software Windows Defender, and it automatically downloads and installs software updates as they become available both for the Windows operating system and any Office products.

Windows 7 and Windows XP

These operating systems are no longer being supplied with updates from Windows. Therefore, they are highly prone to cyber-attack. If the practice is using either of these operating systems, please consider upgrading them ASAP.

Apple Mac

For Apple Mac computers, ensure Automatic security updates are turned on. This can be checked from **System Preferences**> **App Store icon**> then ensure all these are turned on:

- Automatically check for updates
- Download newly available updates in the background
- Install system data files and security updates

User Cases

1. Risks of opening attachments on practice email that is not Healthmail
2. How to respond to Kidnappers when hit by ransomware
3. Helping with password retention and password apps
4. Risks with increased use of smart devices
5. Communicating with patients using email
6. What to do when the surgery becomes inoperable

1. Risks of opening attachments on practice email that is not Healthmail

The most common method for hackers to get into a computer network is by getting a user to open email attachments. These may be disguised as harmless, commonly used documents, for example 'iTunes' receipts. When the attachment is opened, it may look like a genuine receipt, usually something for a free app, which is not assumed as a threat. When the receipt is opened, a malicious program starts to run in the background, which gives the hacker remote access to the computer and network.

The same process can take place if unexpected pop-ups are opened when web browsing. The pop-ups will tempt the users to open them with familiar desired upgrades like 'Adobe Reader'. Check these pop-ups for authenticity before clicking to open. To do this hover the mouse over the file, and check if the destination address is legitimate.

2. How to respond to kidnappers when hit with ransomware?

Ransomware attacks are a specific type of internet virus. When they infect a computer network, they will corrupt the data files, making them unusable. The ransom comes into play when trying to open a file, the user is led to a release page, where the hacker will offer to release files for a fee. The most famous ransomware attack was aptly named 'Wannacry' which affected computers worldwide in May 2017.

When a ransomware email is opened and the virus activated, the network can become infected, which may not be apparent for a couple of days after the attack. During this incubation period, the virus can replicate itself and infect more computers on the network before detonating. For example, the ransomware virus 'Wannacry' specifically locked, renamed and password protected all the Microsoft office files on the affected systems.

Even though paying the fee is a reasonable response to release the files and get up and running again, it is worth noting that much more damage can be done to the network by paying the ransom. This can inadvertently give the hacker access to all the computer files, which would potentially allow them to encrypt more of the network and invariably a higher ransom for release will be demanded. The message is simple - don't pay the kidnappers!

If there is a good backup (in house and online), identify when and where the virus initially entered the system. If the practice is unfortunate enough to become infected, having rigid security allows backing up the system to a moment in time prior to the infection point, and allow for a destroy/wiping of the hard drive of the initially infected machine. It should be noted that data breaches like ransomware attacks must be reported to the Data Commissioner within 72 hours of infection, or the practice could face fines under GDPR as well as a review of practice systems by the Data Commissioner.

If this risk has not been considered up to now, it is worth the time and effort to take all steps needed to minimise the risk of attack to the business, as the consequences of a ransomware attack can be catastrophic.

What to do in event of ransomware attack

The first thing to do is to stop all e-mail communication in and out of the practice (other than Healthmail). This must be communicated to all practice staff, doctors, trainees.

Make sure there is good antivirus software installed and ensure Microsoft software updates are running on all computers. Consider investing in online backup and data-recovery as it will prove to be money well spent in the event of an attack.

3. Helping password retention and password apps

Everything needs usernames and passwords nowadays. With a lot of systems requiring upper and lowercase letters with numbers and symbols, it is getting increasingly difficult to remember all the passwords needed for life and not just in the practice. Avoid choosing common, easily guessed passwords like “12345678” or “password”.

It is dangerous to use the same password for everything. If one password is hacked at the weakest interface, identity theft could allow access to all sites using the same password.

Passwords need frequent updating to avoid malicious keystroke software capturing your passwords.

Consider investing in a password manager as these are relatively inexpensive applications. A good password manager is a one-stop for all system passwords. Popular password manager applications include ‘Keeper Password’ or ‘Dashlane’. Which use two-factor authentication to improve security.

Be careful with using inbuilt password retention on practice computers. This will remember all the passwords and even credit card information that has been input within the system, but all this information will then be accessible if someone else is using the same terminal. Or someone hacks into the system.

4. Risks with increased use of smart devices

Case 1: Doctor A takes a photo of a patient’s rash to send to a consultant dermatologist. The picture is taken using the doctor’s smartphone. Before they have a chance to upload the photo to the practice computer and delete the original from the smartphone, the phone itself is stolen. The phone is not password protected and as such, the thief has easy access to this patient data.

Points to consider: Consider protecting smartphones by installing an app like ‘Phlue’, that will delete the photo when it has been transferred to the patient’s notes. Smart devices such as smartphones, smartwatches, tablets, digital cameras have become more prevalent in recent years and are likely to be an ever-increasing presence in general practices soon. Security for these devices, both in terms of IT security and physical security is of paramount importance. Consider the use of such methods to record ECG tracings to your smartphone or to take clinically relevant photos. If the software on your phone is insecure, then the data is certainly not secure. Devices, in particular those that are connected to a network, are vulnerable to infection with viruses and malware similar to computers. Ensuring these devices are properly protected is essential. However, users of such devices including practice staff and patients, need to be aware that such data can never be considered 100% secure. The use of these devices does carry some risk, so be aware of whether data on a smart device is being backed up elsewhere such as on a cloud or stored in another jurisdiction. Make sure to read the terms and conditions of such storage and who has access to it, as these are easy targets for unauthorised access.

Where possible, smart devices should be password-protected and covered with anti-virus software. Where feasible, patient information should be anonymised (for example, for ECG tracings use patient initials rather than a full name when saving). Patients should be asked for consent before such devices can be used to store their private data. Such devices should also be kept in physically secure locations, preferably in locked cabinets or a safe when not in use and sensitive data should always be deleted from these devices as soon as possible.

5. Communicating with patients using email

Case 1: Patient A has been communicating with the practice regarding a recent consultation he attended the Practice for. He states that the medication he was prescribed has only partially alleviated his symptoms. A secondary plan was discussed at the initial consultation so the GP emails back to confirm a prescription has been left out for the patient to collect at the surgery. On Monday morning, the GP returns to find an email waiting in their inbox. This email was sent by the patient late on Friday evening and concerned some worrying side-effects the patient was experiencing. The patient was looking for urgent advice and sends a further email on Saturday morning stating the symptoms have worsened and they are requesting immediate medical attention.

Case 2: Patient B has consented to be contacted via email and her email address is kept in her file. Doctor A has tried contacting the patient by phone on several occasions with regards to some urgent abnormal blood results. Doctor A tries to contact the patient using the email address on file and advises in the email on what to do over the weekend with regards to the blood results. It subsequently transpires that a typo was made in the listed email address and confidential medical information was sent to an unknown person.

In Case 1, the patient was not aware that emergency advice could not be obtained via email and that the email would remain unopened over the weekend. This should have been made clear when obtaining consent to contact via email. Alternatively, the emails sent to the patient should have included information within the email signature outlying this.

In case 2, it is very easy to list an incorrect email address. Ideally, patients should send an email to the practice initially so that the email address can be obtained directly, rather than inputting and email address that has been written on a registration form.

The above cases highlight some of the possible pitfalls when using email to communicate with patients. Patients should fully consent to the use of email to communicate with the practice. It should be agreed from the start what is appropriate and what is not appropriate to use email for. For example, it should not be used for urgent or emergency issues. Emails sent from the practice should include a disclaimer reminding patients of this and they should also be made aware of the timeframe they might expect a response within. Out of office responses should be set during out of hours times, outside of using Healthmail between medical professionals.

Patients should be advised that email is not a secure method of communication. Therefore, items that a patient may wish to keep confidential should not be included in emails. Patients should also consider what information they are happy to receive before corresponding by email and practice staff should be aware that confidential medical information should not be sent by email.

6. What to do when the surgery becomes inoperable

Apart from hardware failure and software corruption (including, viruses, Malware and Ransomware) natural events like fire, lightning, flooding and power cuts/failure are just some examples. The following is a GP's story.

"This is what we thought until 24/10/2011 when a flood hit us. There was no history of flooding in our area. Our premises were uninhabitable, and we were out of them for approximately three weeks. Our insurers were very helpful; they had an assessor out the next day. They have experience insuring healthcare facilities so were clear on what had to be done. Everything the floodwater came into contact with had to be disposed of for infection control reasons. All of the carpet and plasterboard had to be removed. The underlying floors had to be professionally hygienically steam cleaned. All of our furniture and equipment had to be replaced. Several workstations had to be replaced as they were on the floor but thankfully, our server was in a rack in a comms room so was safe from water damage. Our landlord had some rooms which he gave us to run a skeleton service and we gradually got back to business. We no longer had flood insurance but since then have found an alternate insurer who does cover us, albeit with an excess. This underlines the importance of having a plan that all staff can easily put their hands on in the event of one of the above, or another disaster".

Top Tips when the surgery becomes inoperable:

1. Have a brainstorming/Role Play session with all staff to rehearse what could happen.
2. Produce a one-page plan with all relevant contacts to include:
   a. Software/Backup IT provider to restore the data, when necessary. Contact details for phone provider including instructions on how to divert the phone lines to a temporary number/mobile. Keep an emergency mobile in the practice; make sure it is charged/has credit.
   b. Hardware Provider – in case new machines are needed
   c. Consultation Template with Date/Name/DOB/Phone/Hx/Exam/Dx/Plan on A4 page. Have 50-100 available and be able to revert to a temporary paper-based system when necessary. The Consultation Template forms can be scanned when the practice gets back up and running. Note "See emergencies, defer routines".
   d. Instructions how the website/telephone message can be changed according to disaster. Need logins/passwords.
   e. Contact details for local Pharmacy that can facilitate patients temporarily with emergency supplies. Contact number for the neighbouring practices that may be able to offer some support. The plan outlines each person's role and responsibility in disaster management.
3. Review plan annually.
4. Always have at least two, preferably three forms of backup, one of which must be on-line. Remember, you can replace all physical items, but not data. NO DATA= NO BUSINESS.
5. Backup 'My documents', desktops, email, and any other important files, not just PMS data.
6. Review with your software/backup provider what will happen in the event of needing to restore data.
7. Never place essential electrical equipment (workstations/servers) on the floor.
8. Ensure the practice is adequately insured and
9. Ensure the service agreement with IT providers allows for an immediate response.
10. Contact the local ICGP GPIT Advisor for advice and help.
11. Remember "It could happen to you. Fail to prepare, prepare to fail!"

Consultation Template

Date: Name: Date of Birth:

Address:

Contact Phone No:

Presenting Complaint:

Medications:

Allergies:

Examination:

Diagnosis:

Plan: