
# BASELINE GENERAL PRACTICE SECURITY CHECKLIST Guide

Last Updated 8 March 2016

# Contents



# INTRODUCTION

This document is intended to accompany the "Baseline General Practice Security Checklist". It is intended to provide additional background and explanation for each item on the checklist. The items in the checklist have been drawn from the *Health Information Security Framework,* and represent the most relevant issues applicable to general practice.

This document is not intended to be a comprehensive guide to properly securing your general practice and its health information. It is intended to provide you with support to work through the checklist.

## Use

Use this workbook to provide additional explanation and clarification of the purpose and interpretation for each checklist item.

# 1 KEY POINT OF CONTACT

*Do you have a single staff member who is the key point of contact and co-ordination for all IT work within the practice?*

## 1.1 Rationale

Having a key resource within a practice that has oversight over all IT related work can aide in the co-ordination of that work. It may be possible for many different organisations and individuals to work on a practice' information systems over time. These may include contract IT support providers, PMS vendors, third party software providers, such as HealthLink and PHO staff. It is likely that none of these people who complete work on your systems are aware of what work has or is about to be carried out by the others.

By providing a single point of contact within the practices, all those working on related information systems have a single point of coordination and can avoid completing unrelated work at the same time. It also provides a single reference for what work has been carried out in the event of issues.

# 2 THIRD PARTY IT SPECIALISTS

*Do you use a paid third party IT specialist to undertake or have oversight of your IT?*

## 2.1 Rationale

General Practice systems are complex. They have many points of interconnection with other systems. They are responsible for transmitting health information. It is important that they are maintained in such a way as that they are available most of the time and the way in which they operate does not compromise the security of the information that they hold.

There may be a temptation for practices to undertake the majority of this work themselves, but this is ill-advised. Having a specialist IT provider with knowledge of the systems and industry and help with



maintenance of the systems and ensure that they are not configured in a way as to compromise the security of your system.

## 2.2 Clarifications

In order to answer yes to this question your third party IT specialist should be paid by you to perform the work. This excludes family or friends that complete IT work for you as a favour or in-lieu of other non-cash payments. While not a guarantee, ensuring that you are paying for your IT services ensures that it is clear to those providing such services that they are providing a professional service.

You should have a contract with your third-party IT provide that covers all standard aspects of engaging a professional service. The contract may be on a time-and-materials basis, or have some retainer type component to it.

# 3 ACCEPTABLE USE OF INFORMATION

*Do your practice policies cover acceptable use of information and systems by staff?*

## 3.1 Rationale

Written policies act to document the policies and procedures within an organisation. This provides staff with a resource to help them learn what is acceptable and not in an organisation. This is useful for staff who are first starting work, but can also be useful for staff that have been in an organisation for an extended period to remind them.

It should not be taken for granted that all staff are conscious of their responsibilities of how to handle patient health information. It should also not be taken for granted that staff know what is acceptable to use systems for at work and not.

# 4 BACKUPS

*Do you take at least daily backups of your system?*

## 4.1 Rationale

A backup is a copy of some or all of the files and information stored on a system. The purpose of a backup is to be able to recover lost files or information if something happens to the original information.

In the case a general practice, this should always include the PMS database, but may also include other computer files contained on your system. The exact nature of what should be a part of a backup and how often is a more appropriate conversation with your third party IT provider.

Taking a backup of your most important files at least every day is important. In the event of a catastrophic loss of your system (perhaps a fire to your building that destroys or a computer virus that renders the files or system unuseable), the backup is used to retrieve important information. In order to retrieve information from backups, you use your most recent backup. This means that you will loose any information between the time you last have a backup of your system and when you wish to restore it.

For those that take daily backups, this is likely to be 24 hours. Losing 24 hours of information from a medical system is not ideal, however in a crisis situation it may be an acceptable loss. Ultimately 24 hours is an arbitrary measure but is the basis of good practice for most small businesses.

Some larger businesses may choose to take backups of their system more frequently. Determining the frequency of backup is a function of the businesses appetite for cost and risk.

# 5 STORE BACKUPS OFFSITE

*Do you store backups securely off-site either through a paid online system or through a professional off-site archiving company? Note that staff taking backups home doesn't count and free online storage e.g. Dropbox doesn't count.*

## 5.1 Rationale

Backups are taken to protect against various events that may cause you to lose some or all of your important files and information. Holding a copy of those backups and files offsite is important to protect against events such as fire or theft, where both the original files and backups could be compromised.

You protect against total loss by holding your backup files in a physical location other than where your original files are held.

Because your backups will almost always contain sensitive information, it is also important that the physical location in which the backups are being stored are secure. Generally staff that are taking backups to their homes is not considered to be a secure way of keeping off-site backups. There may be issues with staff having the potential to lose the backups en-route to their home or having those backups stolen from their home. Both of these situations would compromise your information security. If you take physical backups, we recommend that you use a professional service that can satisfy the requirement for secure transport and storage of those media.

If you backup directly to an online service, then this provides similar protection to that service. Ensure however that you have credentials to retrieve those files stored somewhere safe that would be accessible if the practice was compromised. Those files will not be any use to you if you are not able to access them when you need them.

## 5.2 Clarity

While a backup is a copy of your system information, simply duplicating files is not a backup in and of itself. There are some key criteria you should consider when working out whether you take a backup or not.

It should be clear what files are backup files and which are live.

A backup should almost always be isolated from your main computer systems. This can be done by either using physical media that can be removed (e.g. tape drive, or portable hard drives), or virtually, but sending backup files to a separate physical location (preferably a dedicated backup service).



If you are using an online service to store your backup files, you should use only a secure and paid service. By paying for the service, you have a reasonable expectation that you can retrieve your files should you need to. A free service will unlikely provide any such guarantee.

# 6 BACKUPS RESTORES

*Have you ever tested your backup restoration process?*

## 6.1 Rationale

Backup of a system is only half of the equation needed to protect your important health information from loss. If your original information stored on your practice computers were lost, you would need to retrieve backups and successfully restore them.

It is possible that in some backup configurations you may not be undertaking a backup of all files required to get you system back into a working state quickly and easily.

You should very occasionally check that it is possible to retrieve and restore your systems to a safe working state. We would recommend doing this when your backup method is first established and at any time more than a minor change is made to that scheme. We would also recommend that you plan this in conjunction with a third party IT provider. You would normally test the restoration process into an environment outside of your normal practice system (to simulate what may happen in a disaster situation).

To undertake this test may require some time. We acknowledge that for most small businesses that this task would only be undertaken sporadically.

# 7 INFORMATION ACCESS

*Do your staff have access to only the information that they need and no more within the PMS (e.g. Reception staff can't access clinical notes in the PMS).*

## 7.1 Rationale

Most sensitive information in general practice is likely to be stored within the Patient Management System. Most of these systems have a facility to assign roles to people, and to restrict the access of information at varying levels.

People with access to the PMS should be assigned an appropriate role based on their need within the practice. Custodial or cleaning staff should not have access to the PMS. Reception staff should only have access to the information that they need to do their jobs, which likely includes patient administration information but not clinical.

By limiting the availability of patient health information, you limit the risk that it will be inadvertently or deliberately misused.

# 8 PHYSICAL SECURITY

*Is your PMS server secured against theft after-hours (e.g. in a separate locked, entry proof location) OR your PMS is in a hosted data centre.*

## 8.1 Rationale

Patient Information will most likely be stored a server within your practice. This server therefore contains the sensitive patient health information that requires protecting. If a burglar was to target your practice it is important that they cannot simply pick-up and walk-away with your entire server. Aside from costing you financially, it will cripple your practice until you can restore your information from backup, and the health information on your server may be compromised if they can access it.

You should take steps to secure the physical server equipment in some way so as to protect against such eventualities. This may include physically shackling the server to a wall or floor, or keeping it in a room with increased security (e.g. strengthened doors, no windows, or barred windows etc).

If your systems are offsite, it is reasonable to assume any commercial data centre or hosting facility is physically secure.

# 9 SECURE COMMUNICATION

*Do your staff always send patient information using secure means? Note that sending by plain email is almost never secure.*

## 9.1 Rationale

Modern clinical practice requires the sharing of patient information from general practice to other facilities. This information must be kept secure, even when in transit from your facility to the next. Some modern communication mechanisms although convenient are not secure.

You need to continue to educate your staff to make sure that they are using the right way to share information. Secure ways of sharing information generally include:

- Anything sent by HealthLink
- Electronic Referral Forms (generally)
- ManageMyHealth, Health365 and other Patient and Provider Portals
- hMael
- Fax
- Post

Both Fax and Post can be used if there are no other methods to share information, although both have significant weaknesses and should be avoided if possible.

The most commonly used in-secure communication mechanism used is email. Email is convenient and nearly ubiquitous but not secure. Patient information should almost never be sent via email.

## 9.2 Clarity



If your staff are using email to send patient health information, then you must answer no to this question. Viable alternatives are portals, hMael, Fax or Post.

The one exception to the email issue is if they are sending information internally in a corporate environment. This will almost never be the case in small to medium sized general practices, and can confuse the messaging to staff.

# 10 SECURITY UPDATES

*Does your server have critical security updates and patches applied at least every month?*

## 10.1 Rationale

Computer operating systems are complex. They often contain flaws that can be exploited by others to gain access to systems that they are not authorised to do so. Software manufacturers are constantly updating their software when they discover these issues.

In order to ensure that your software on your computers is not vulnerable you will be needed to update your software on a regular basis. Best practice would suggest that this should happen to all computers and devices connected to your computer network; although the most critical device is most likely to be your server which contains your patient health information.

Updating your systems regularly gives those wanting to attack them with known vulnerabilities less of a chance to do so.

You would either usually have your computers set to receive critical updates automatically from the internet, or your third party IT provider may install these on your server regularly.

# 11 ACCESS REQUIRES PASSWORD

*Do all computers in your practice require a password to access them from start-up?*

## 11.1 Rationale

Security and convenience are often at odds with each other. It would be far easier if we did not have to remember passwords and could simply turn computers on and gain access immediately without the user of such passwords. Not having passwords enabled on your computers is a risk, because if those computers are accessed, it means that unauthorised personnel may be able to access them.

## 11.2 Clarity

PMS passwords do not count towards this measure. If you can get into the operating system environment without a password, then you must answer no to this question.

# 12 WORKSTATIONS LOCK

*Do all computers 'lock' after no more than 15 minutes of inactivity?*

## 12.1 Rationale

It is important that computers automatically require a password to access them after a period of inactivity. This protects against un-attended computers if staff forget to log-off or walk-away and are longer than they expect. This is important for all computers.

The purpose of setting such a short window of time as 15 minutes is intended to limit the opportunity for others to access an un-attended system, while balancing the convenience of not having to log-in if you briefly leave a workstation.

# 13 ANTI VIRUS

Do all computers in your practice have anti-virus software installed, running and updated regularly?

## 13.1 Rationale

Viruses and malware (malicious software) are a common way in which information is leaked from systems inadvertently. The front-line defence against virus and malware is staff behaviour, encouraging them to practice safe-computing. This means not downloading software from the internet or opening attachments within email or social media that they are not certain of the purpose of.

Unfortunately safe-computing does not always protect against all of the threats present in a modern computing world. Anti-virus software is designed specifically to act as a second line defence against malicious software. It scans high risk files and blocks suspicious or known threats.

In order for this software to be the most effective, it must be updated regularly.

## 13.2 Clarity

There are anti-virus and anti-malware software available that is free (and built into operating systems). Although this is better than nothing it should not generally be relied upon to fully protect a computer in a small business environment.

Anti-virus software must be installed on all computers within your network. If you have anti-virus software only on some computers, or on your server only, you are likely still at risk.

# 14 DISASTER RECOVERY

*Does your practice have a documented plan for disaster recovery and business continuity that addresses patient health information and the ongoing operation of the practice if your information systems are unavailable for an extended period.*

## 14.1 Rationale

Thinking about and planning for the loss of your computer systems is important. Having written documentation of what you will do in the event that you cannot access them for an extended period is useful in that it allows you to plan ahead of time, with little pressure. It is easy to forget important aspects of your operation if you are managing a situation in an ad-hoc way.

Think of all the ways in which you may lose access to your health information. If you have your server self-hosted, then what will happen if you have a fire. If you use a hosted solution (e.g. your PMS is in



a data centre), then what happens if you lose your internet connection ( and if you have a backup internet connection, what happens if you lose that too).

A good plan will consider various common scenarios and outline the steps that need to be taken in order to accommodate the situation and restore services.