# Cybersecurity Essentials for Healthcare

Reading time:
Jayson Nagpiing
Date created: 30/11/2020

Tags: Article | Medico-Legal | Medical Practitioner | Dental Practitioner | Practice Risk Management

IT and online security is essential to ensure that you, your staff, your practice and most importantly, your patients are protected from loss or theft of data and information. Poor IT security may lead to significant loss including practice interruptions, financial costs and reputational impact.

Effective IT security is a combination of human and machine approaches, it applies to both the individual level and the practice. You should seek the assistance of an IT professional to ensure you are operating a secure IT environment and may wish to consider some of the following guidelines when considering your IT and data security:

- Do not freely disclose personal, financial or credit card information. Always verify the authenticity of a caller or email sender before disclosing information, if unsure then immediately discontinue the conversation and contact the organisation directly via their advertised phone number, email address or website.
- When entering or viewing sensitive information such as passwords or patient details, make sure that no one else is watching. Politely ask others to move away or leave the room if you need to view sensitive or private information.
- Always use strong passwords, for example a combination of upper case, lower case, numbers and special characters such as '@' and '!'. Never repeat a password that you have previously used for Facebook, email or other online systems. Change your passwords regularly and never use the browser option to 'remember' your password.
- Be cautious in your approach to links received in emails and other communication. The safest route to a website is always via a Google search or directly to their known address. Be alert for websites that purport to be another website but do not have a correct website address.
- Become familiar with your internet browser and the features which verify a website's authenticity, for example many browsers include a green highlight or a closed padlock to indicate a secure connection. Refer to your browser online help.
- You should monitor your account transactions and other online systems on a regular basis to ensure that activity is consistent with your own.
- Never ask nor provide any information in relation to passwords, PIN numbers of other security details. A reputable organisation will never request this information.
- Ensure that all computers accessing your Cloud service are protected by a firewall and anti-virus program. Make sure you keep your security programs up to date and renew your subscriptions.

# Cloud Computing

For many entities, Cloud computing can provide a number of cost savings and benefits, potentially including functionality, mobility, scalability and security – however, these benefits can only be fully realised following an assessment of the relative benefits and risks of any particular service offering.

You should take a cautious and measured approach when considering both local and Cloud computing and should consider what's best for your practice and your patients before committing to a solution.

It is important to remember that all IT has an inherent risk associated with it, Cloud or otherwise. When considering the security of information, you should consider the whole information life-cycle, from the initial point of capture right through to secure disposal.

Risks and implications may vary substantially depending on the type of Cloud service. You may wish to consider the following additional IT security items when considering a cloud service provider:

- Cloud services are reliant on a continuously available Internet connection.
- There may be potential for loss of data, for example, a change in the provider's circumstances, such as the services offered, insolvency or sale.
- Carefully consider your backup strategy that will be applied to data stored in the Cloud. For example you may wish to download and retain a local copy of data.
- Consider who owns the data, what will happen to the data when your contract expires?
- Encryption is essential to protect private or sensitive information. Discuss with your IT adviser what encryption will be applied at rest and in transit.
- Cloud data may be physically stored anywhere in the world. Consider the jurisdiction in which your data will be stored and what impact this may have to your privacy obligations.

# Further Resources

The Australian Government Department of Communications provides an excellent Cloud consumer fact sheet on Cloud computing and privacy.

Many of the major banking websites provide information on protecting your personal online activities. While these sites have an online banking focus, many of the principles will apply across your online activities. For example, NAB's key points to help protect yourself online.