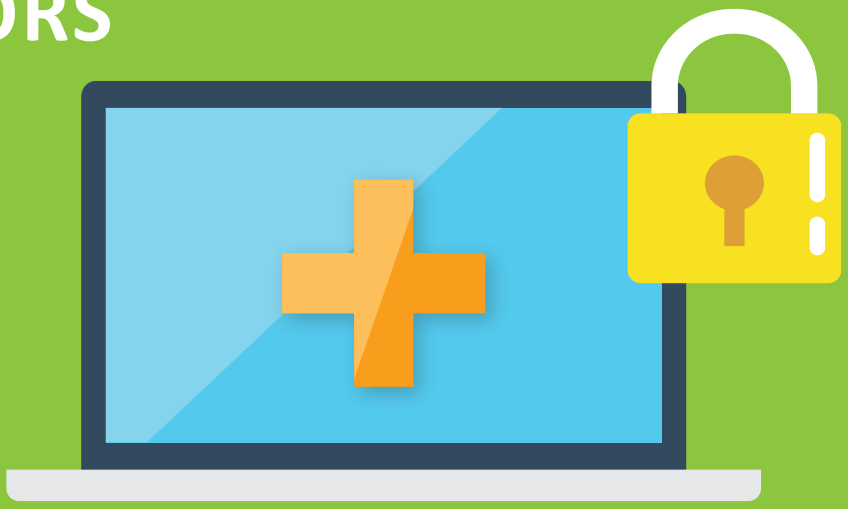
Australian Government
Australian Digital Health Agency

Selecting secure IT products and services

QUESTIONS TO ASK YOUR IT VENDORS



A companion for the Information Security Guide for small healthcare businesses

A guide for
healthcare providers

This document has been designed as a companion to the Information Security Guide for Small Healthcare Businesses. It provides guidance regarding a range of IT security considerations, and includes sample questions for healthcare providers to ask their IT vendors, to assist with selecting secure IT products and services.

This document provides general guidance in relation to IT security and is not intended to be comprehensive.

Key trends in information security

In 2018, the average number of individuals affected per healthcare breach reached 39,739, more than twice that of 2017. [1]

In 2016-17, Australian organisations reported 47,000 cyber security incidents, representing a 15% increase on 2015-16. [2]

A malware attack on a healthcare business can significantly affect service delivery by making systems or devices unusable and preventing access to data. [3]

Questions to ask your IT vendors

Your healthcare business or practice uses a variety of digital information that healthcare consumers, suppliers and employees expect you to keep safe. The computer systems that help your business to store and manage access to this data, are vital to your ability to operate.

The value of the information your business holds can make it a target for criminals who break into your computer systems to steal important business and healthcare information. These attacks have the potential to compromise healthcare information, cause reputational damage, impact patient safety and result in financial loss for your business.

This document has been developed by the Australian Digital Health Agency (the Agency) to assist small healthcare businesses to select secure Information Technology (IT) products and services. Healthcare business owners, principal practitioners and practice managers may wish to discuss this information with IT vendor(s) to understand or review the security aspects of the product or service they offer your business. This document is designed to accompany the simple steps outlined in the Agency's Information Security Guide for small healthcare businesses that can be found at www.digitalhealth.gov.au.

Information security – it's all about trust

Good clinical hygiene and IT hygiene are important to delivering healthcare services, and contributing to the trusted relationship healthcare consumers have with your business. Building trust with healthcare consumers involves taking care of their physical needs, along with keeping their sensitive personal information private and secure.

As the use of digital health records and internet-enabled medical devices increases, your business has a growing responsibility to prevent data being compromised. Ensuring your systems are secure instils confidence from healthcare consumers in your ability to look after all aspects of their care.

This document was developed to help your business take a multi-layered approach to information security. The questions and sample answers can help you prepare for a conversation with your IT vendor(s) about keeping your systems and data secure. In addition, this document may assist you to understand how you can comply with legislative requirements, such as the requirement to take reasonable steps to secure personal information (*Privacy Act 1988*, Australian Privacy Principle 11).

Note: This is not intended to be a comprehensive list of information security requirements. It provides some key discussion items for you to start a more in-depth conversation with your IT vendors.

Awareness – stay alert to stay secure

Having regular health check-ups can make you more aware of what you need to do to stay healthy or manage a chronic health condition. Similarly, frequent checks on the security status of your systems and the level of staff awareness of security risks, means you can prevent or manage an incident.

Whether you are considering a new product or reviewing your existing systems, **ask your IT vendor(s) the following questions**:

1. What do you offer in terms of documentation, guides or user training about the security aspects of your product or service, and when is this made available to us?

Good:

- ☐ *System documentation, including a description of all security controls, is available on request*
- ☐ *Guides are available for users (eg help files), and include details of security functions*

Better:

- ☐ *System documentation, including an explanation of security controls and system design, is provided up front*
- ☐ *Comprehensive guides are available for users (eg help files), including details of security functions*
- ☐ *Training is provided, including some security training*

Great:

- ☐ *Clear, detailed system and security documentation is provided, including documented security risks and mitigations*
- ☐ *Comprehensive guides are available for users, including implementation guides for secure configuration of each function*
- ☐ *Tailored training is provided that covers all aspects of security for the system*

Examples of what to look for:

"We can provide extensive documentation on the system settings and configuration, including for secure use on devices."

"User guides are provided for different levels of user accounts such as the IT administrator and business user and they include tips on using the product or service securely."

"Training is offered and other support resources are available, such as online tutorials, to keep users up to date on the current and new security functionality within the product or service."

2. How do you monitor the product or service for unusual activity and contact us if you detect something unusual?

Good:

- ☐ *Time stamped logs are available on request for failed and successful logons, user activity, changes to privileges, system changes, and network activity*
- ☐ *The service provider is contractually obligated to contact you if they identify unusual activity on the system*

Better:

- ☐ *Time stamped logs are available on request for failed and successful logons, user activity, changes to privileges, system changes, and network activity*
- ☐ *Regular reporting on logged activity is available*

- ☐ *Logs are kept for at least 6 months (specific length to be determined based on business needs)*
- ☐ *An automatic alert service is available for unusual or high risk activity that is detected on the system*

Great:

- ☐ *Configurable time stamped logs are available on request for failed and successful logons, user activity, changes to privileges, system changes, and network activity*
- ☐ *Regular reporting on logged activity is available*
- ☐ *Logs are kept for at least 6 months (specific length to be determined based on business needs)*
- ☐ *An automatic alert service is available for unusual or high risk activity that is detected on the system*

Examples of what to look for:

"Your solution is monitored for any unusual activity."

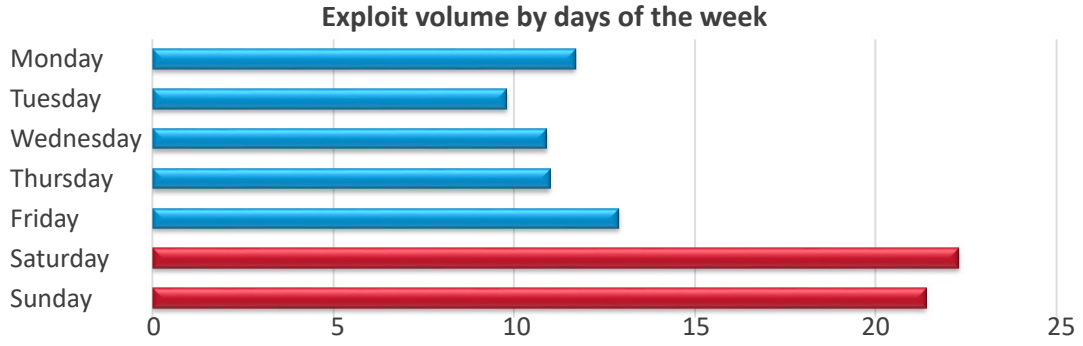
"We would contact you if our high-level investigation revealed something that may need your input to determine if it is legitimate - such as confirming a new user has joined the business."

"Alerts regarding the software and devices used by your business are provided as soon as we become aware of a potential security issue, along with advice on mitigating the risk."

Things to check with your IT vendor(s) include:

- Is documentation available for you to see how the product or service is put together, and where the data will be stored (e.g. healthcare information is stored within Australia, to meet privacy requirements)?
- Does the vendor have a data breach response plan that includes documented processes for taking appropriate action if a suspected or actual data breach occurs?
- Check whether the product or service lets you set up different levels of user access, relevant to their roles, as an extra security control.
- Does the vendor offer a variety of training resources and support, to meet the different skill levels within your team?
- Depending on the level of security risk, you may need to see if 24/7 real-time monitoring and alerts are available.

For example, if the product or service is only monitored during business hours does this increase your exposure to attacks that would have a major impact on your business, as 43% of exploits are detected on weekends[4] - see figure below:



Backups – prepare for an emergency!

Health insurance offers people peace of mind that, should they need an ambulance, they won't need to worry about the cost of getting to hospital quickly. Similarly, having a backup of your business data offers assurance you can avoid the cost of a ransom demand to regain access to your data, and the backup can help you recover if data loss or data corruption occurs.

Discuss the following questions with your IT vendor(s) to ensure you are prepared in the event of an emergency:

1. Support for our backup regime

a) for backups captured by our practice – how does the product or service help us to ensure regular backups are captured and verified?

Good:

- ☐ *Functionality is provided to support capture of regular backups (for example, daily)*

Better:

- ☐ *Functionality is provided to support capture of regular and ad-hoc backups, according to business requirements*

Great:

- ☐ *Automated full daily backups are supported, and automated intermittent backups can be configured, to suit business requirements*
- ☐ *Documentation and support is provided to enable you to regularly test that information can effectively be restored from back up*

Examples of what to look for:

"Our software includes a daily backup feature to ensure a backup of all business information is completed after close of business."

"Our product or service also has an automatic backup function that captures new data every 15 minutes."

b) for backups conducted by the IT vendor – how often are backups conducted and verified; and where are the backups stored?

Good:

- ☐ *Backups are conducted regularly (for example, daily)*
- ☐ *Once the backup is captured, it is disconnected from the IT network for storage purposes*
- ☐ *Data does not leave Australia*

Better:

- ☐ *A daily backup is conducted with more frequent backups available on request*
- ☐ *Backups are stored at multiple locations, and the backup is disconnected from the IT network once the backup is complete.*
- ☐ *Data does not leave Australia*

Examples of what to look for:

"A daily backup of all business information is completed after close of business."

"Our product or service also has an automatic backup function that captures new data every 15 minutes."

"The information will be stored securely off site without being connected to the business network, to prevent loss due to fire, theft or malware."

"Your information is stored at a location in Australia and with protections that meet your legal obligations."

Great:

- ☐ *A full daily backup is conducted each day with automated intermittent backups available, to suit business requirements*
- ☐ *Backups are stored at multiple locations, and the backup is disconnected from the IT network once the backup is complete.*
- ☐ *Testing is conducted regularly to confirm that information can effectively be restored from back up*
- ☐ *Data does not leave Australia*

2. How will the information you store and process for the business be protected from unauthorised access, while the data is at rest and in transit?

Good:

- ☐ *All data in transit is encrypted*

Better:

- ☐ *All data in transit, or a rest, is encrypted using non-proprietary algorithms*

Great:

- ☐ *All data in transit, or at rest, is encrypted using one of the non-proprietary algorithms listed in Appendix A*

Example of what to look for:

"Your information will be encrypted during transit and at rest using a proven encryption method."

Things to check with your IT vendor(s) include:

- Support for your business to implement appropriate backup routines.
- Awareness of the legislative requirements regarding storage of healthcare information, including compliance with relevant federal, and state and territory legislation.
- Use of appropriate algorithms when encrypting data, and appropriate encyrption key management, noting it is safer to use a widely used algorithm, such as Advanced Encryption Standard (AES). Look for a non-proprietary algorithm that has been tested for at least 10 years, rather than a proprietary algorithm that may not have had as rigorous testing. Proprietary algorithms can also limit your ability to use multiple IT vendors or move services to a different IT vendor (a table of non-proprietary algorithms is provided at Appendix A).

Case study – Ransomware attack locks up 16,000 patient records[5]

On 25 September 2017, a medical centre in the United States was unable to access 16,476 patient records. This was due to a malware infection that had encrypted the data in their computer system. A demand for a ransom was sent to the medical centre requiring payment to unlock their records. The medical centre did not pay the ransom as they had access to an offline backup copy of the data. This incident was reported to officials, and patients were notified and given instructions to monitor their information. Stronger security measures were put in place to prevent future incidents.

Network and device security – lock down your computers and networks!

No single part of the body is more important than others when it comes to maintaining your overall health. Similarly, all of the parts connected to your IT network, including mobile and medical devices, require equal attention to maintain overall information security.

Speak with your IT vendor(s) to understand how they protect all parts of your network.
Start by asking the following questions:

1. How does your software or service support the business' overall information security, including when it is accessed remotely or via a mobile device?

Good:

- ☐ *The software or service is able to work effectively while your anti-virus and anti-malware software is running.*
- ☐ *Regular system updates and security patches for all device types are included in the contract*
- ☐ *An automatic log out function is available*

Better:

- ☐ *The software or service is able to work effectively while your anti-virus and anti-malware software is running.*
- ☐ *Automated system updates and security patches for all device types are included in the contract*
- ☐ *An automatic log out function is provided*

Great:

- ☐ *The software or service is able to work effectively while your anti-virus and anti-malware software is running.*
- ☐ *Automated system updates, security patches and a reminder service for all device types are included in the contract*
- ☐ *An automatic log out function is provided and is configurable by users*

Examples of what to look for:

"You will be able to set automatic updates; and users and administrators will receive reminder messages to apply patches."

"The software or service has the ability to set different levels of access for users, relative to their roles within the business."

"The software or service is compatible with your anti-virus software and other anti-malware filters that you are using on your network."

"Users are logged out of the software or service after a short period of inactivity (e.g. 10 minutes)."

"The documentation we provide outlines additional security measures that need to be applied when the software or service is accessed remotely or via a mobile device."

2. What types of information do you provide to assist the business or a third party to monitor use of the product or service?

Good:

- ☐ *Separate access levels are available for business and IT administrator user types*
- ☐ *Transaction logs and reports are available on request*

Better:

- ☐ *Separate, role-based access levels are available*
- ☐ *Transaction logs and reports are available on request, along with custom reporting options*

Examples of what to look for:

"You will receive transaction logs and user audit reports at the frequency you or your third party require."

"Additional reports can be provided on request and we offer the ability for your IT administrator to create custom reports."

Great:

- ☐ *A configurable user access function is provided*
- ☐ *Transaction logs and custom reports are provided*

3. Who has access to the business' information, to maintain and support the product or service used by the business?

Good:

- ☐ *Clear protocols exist for IT vendor access to sensitive information*
- ☐ *Key activities are logged and audited*
- ☐ *Reports are provided on request*

Better:

- ☐ *Clear protocols exist for IT vendor access to sensitive information*
- ☐ *All activities are logged and audited*
- ☐ *Regular reports are provided*

Great:

- ☐ *Clear protocols exist for IT vendor access to sensitive information*
- ☐ *All activities are logged and audited*
- ☐ *There is a reporting system that allows regular and ad hoc reporting to be conducted, to view and correlate IT vendor activities*

Examples of what to look for:

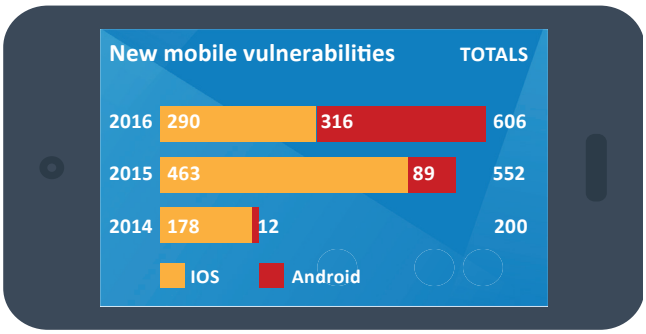
"Your business information rarely needs to be accessed by members of our team and all activity is monitored."

"There is an audit log kept of all activities relating to accessing, amending or destroying your business data."

Things to check with your IT vendor(s) include:

- Are automatic updates available, and/or manual reminders sent to ensure updates are applied, especially for security patches?
- It is helpful to understand the format of transaction and audit log files, if you need to be able to aggregate this data with your other log files.
- Check whether settings within the product or service enable you to restrict privileges and limit access to information, according to user roles, as an effective security control.
- It is important to check that other network security measures, such as anti-virus software and mobile applications, are not going to conflict with the new product or service.
- When using an application that works on a mobile device, it is important to understand how to keep the data it uses and transmits secure. Extra consideration needs to be given to ensure the security of devices that are not supplied by the business to employees.

The number of mobile vulnerabilities detected has more than tripled since 2014, so understanding how to mitigate this risk is critical to protecting your business information when using mobile devices.[6]



Passphrases – protect your information

A dentist will tell you that simply brushing your teeth is not enough to protect your teeth from cavities – you need to brush, floss and rinse with a mouthwash. Setting a passphrase is better than using a simple password to protect your information from unauthorised access. Additional protection can be achieved through use of multi-factor authentication methods.

Have a conversation with your IT vendor(s) and **ask the following questions:**

1. How does your product or service support the creation and use of strong and complex passphrases?

Good:

- ☐ *The use of complex passphrases is supported*

Better:

- ☐ *The use of complex passphrases is supported*
- ☐ *The minimum length of passphrases is enforced*

Great:

- ☐ *The use of complex passphrases is supported*
- ☐ *The minimum length and combination of characters in in passphrases is enforced*
- ☐ *Users are prevented from reusing recent passphrases*

Examples of what to look for:

"Users are required to create a passphrase with at least 14 characters and a combination of upper and lower case letters, numbers and special characters."

"Users of our system are prevented from reusing any of their previous 8 passwords."

2. Can multi-factor authentication be applied to your product or service?

Good:

- ☐ *Multi-factor authentication is available as an additional service, but is not implemented by default*

Better:

- ☐ *Multi-factor authentication is an included option in your service*

Great:

- ☐ *Multi-factor authentication is provided, with a number of options available*

Example of what to look for:

"The product or service can be configured to require the user to set a passphrase and then enter a code that is either sent to their phone via SMS when they log on, or obtained from a hard or soft token."

3. What support do you provide to ensure we are not using any default passwords associated with the product or service?

Good:

- ☐ *Setting a new IT administrator passphrase is forced on installation of the product or service*

Better:

- ☐ *Setting an IT administrator passphrase is forced on installation of the product or service*
- ☐ *IT administrator passphrases are forced to be changed every 90 days*

Example of what to look for:

"When our product is installed, unique IT administration credentials are required for your organisation. Default passwords are not used."

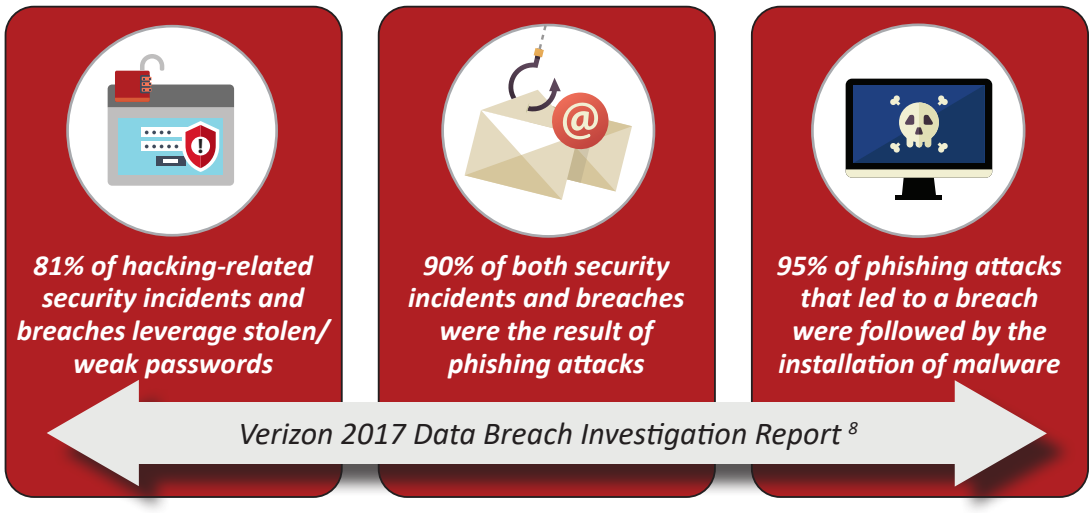
Great:

- ☐ *Setting an IT administrator passphrase is forced on installation of the product or service*
- ☐ *IT administrator passphrases are forced to be changed every 90 days, or less, to suit business needs.*

Things to check with your IT vendor(s) include:

- Whether the product or service has the capability to set at least a 14 character complex passphrase.[7] The longer the passphrase the better the level of protection for your data, as it makes it harder for a cyber-criminal to crack. A strong passphrase is made up of at least four random words that are meaningful to you so you can remember them.
- Whether use of multiple authentication methods is supported, especially for IT administrator accounts. For example, a code being sent to a separate device, an email being sent to the IT administrator to verify activity or conifrm access for a new user, or use of a token or app that generates security codes similar to online banking.
- What support is provided to ensure default passwords are changed. It is helpful if the product or service automates the changing of default passwords, rather than this being an optional process.

Strong passphrases are one of several security controls that you need to apply to keep healthcare and business information safe, as the following statistics show:



Privacy – keep your friends close and information closer

In Australia, all healthcare providers are required by law to keep personal and health information secure. The applicable privacy legislation for public and private entities may vary depending on jurisdiction. The Commonwealth's *Privacy Act 1988* applies to Australian government entities and all heath service providers in the private sector, regardless of size. State and territory legislation varies from one jurisdiction to another.

Of particular relevance in the context of this document, the *Privacy Act 1988* requires organisations to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure (Australian Privacy Principle 11). While this document may assist you to meet this requirement, it is important that you also consult the Office of the Australian Information Commissioner (OAIC) Guide to securing personal information, available on the OAIC website: www.oaic.gov.au

Discuss your legislated obligations with your IT vendor(s). **Start by asking the following questions:**

1. This business is subject to privacy requirements under the *Privacy Act 1988*, the *My Health Records Act 2012*, and applicable state and territory legislation. How does your product or service help us comply with these Acts?

Good:

- ☐ *The vendor has a good understanding of the legislation relevant to your business*
- ☐ *In-built access controls prevent access or modifications to specific documents*

Better:

- ☐ *The vendor has a good understanding of the legislation relevant to your business*
- ☐ *The vendor offers reference sites for similar healthcare business that use their product/service*
- ☐ *Configurable access controls prevent access or modifications by user role*

Great:

- ☐ *The vendor has a good understanding of the legislation relevant to your business*
- ☐ *The product or service is used by many healthcare providers*
- ☐ *Configurable access controls prevent access or modifications by user role*

Examples of what to look for:

"Inbuilt access controls exist to prevent unauthorised access to the personal and health information the business may collect, store and amend."

"Once the personal health information held is no longer needed for business or legislated data retention purposes, you are provided with verification it has been irretrievably destroyed."

"In the event the information cannot be completely destroyed it will be de-identified, including copies that have been archived or are held as backups."

"The product or service takes into account limits for the collection, use and disclosure of information contained in the My Health Record System."

2. What support do you provide should our business need to conduct an investigation and report a data breach?

Good:

- ☐ *The vendor describes the process that would be followed to investigate and report on a data breach*
- ☐ *The vendor is willing to provide appropriate support and information for investigations*

Better:

- ☐ *A documented data breach support process is available*
- ☐ *Clear support arrangements exist should an incident require investigation*

Great:

- ☐ *A documented data breach support process is provided*
- ☐ *A support team can be made available to assist with investigations, if required*

Examples of what to look for:

"We understand that as a healthcare business you are subject to mandatory data breach notification requirements under the Privacy Act and My Health Records Act."

"There is an established process should you need assistance to investigate the audit logs for the product or service we provide."

3. How is access to the personal and health information monitored?

Good:

- ☐ *Detailed logs are kept showing specific items that have been accessed by each user*
- ☐ *Reports are available on request*

Better:

- ☐ *Detailed logs are kept showing specific items that have been accessed by each user*
- ☐ *Reports are provided at pre-defined intervals*

Great:

- ☐ *Detailed logs are kept showing specific items that have been accessed by each user*
- ☐ *Reports are provided at pre-defined intervals*
- ☐ *Organisation-specific alerts are available*

Example of what to look for:

"All activities associated with the product or service are logged. Activity is tracked using each individual user's account identifier, to mitigate the risk of data being lost or modified and to assist with identifying any unauthorised access."

Things to check with your IT vendor(s) include:

- Confirm the IT vendor has awareness of relevant Acts; and their product or service has sufficient security controls and audit logs to help you comply with privacy requirements.
- Verify that the vendor is able to provide you with a full copy of healthcare information for data retention purposes.
- Check that the IT vendor can explain the way sensitive information is destroyed or de-identified data retention requirements have been satisfied.

Visit the Office of the Australian Information Commissioner (OAIC) website to learn more about privacy obligations: www.oaic.gov.au. These pages may be of particular interest:

- **Guide to securing personal information:** https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information
- **Information about the Notifiable Data Breaches Scheme:** https://www.oaic.gov.au/privacy/notifiable-data-breaches
- **Information about privacy and the My Health Record system:** https://www.oaic.gov.au/privacy/other-legislation/my-health-record
- **Information about state and territory health privacy laws:** https://www.oaic.gov.au/privacy/privacy-in-your-state

Glossary

Term	*Description*
anti-virus and anti-malware	Software designed to protect against computer viruses and other malicious software that may cause harm or provide unauthorised access to computers and the information they hold.
automatic updates	An automated process for downloading and installing updates to computer systems.
backup	The process of making copies of data or data files to use if the files are lost or destroyed.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
data at rest	Data that is currently in storage and is not being read, accessed, used or transmitted.
data breach	An incident that results in unauthorised access to data.
data corruption	When data becomes unusable, unreadable or in some other way inaccessible.
data in transit	Data that is travelling over an IT network, from one computer or server to another.
default password	Preset passwords provided with computer hardware or software. If default passwords are not changed, attackers can use known default passwords to gain unauthorised access.
encryption	The process of transforming data into an unintelligible form to enable secure transmission.
exploit	A general term for any method used by hackers to gain unauthorised access to computers.
hacking	Gaining unauthorised access to a computer or a network by exploiting system flaws, using deception, or using malicious code to bypass security controls.
IT administrator	A user that has privileged access, enabling them to modify IT system configurations, user accounts, audit logs, data files or applications.
logs, audit logs, system logs	A chronological record of system activities, including system access and operations.
multi-factor authentication	Using more than one method to verify the identity of a user before allowing access to a system.
non-proprietary algorithms	A type of mathematical procedure (algorithm), which can be used by any organisation to encrypt data. Non-proprietary algorithms are generally widely used and well tested.
passphrase	Similar to a password, consisting of a phrase or a sequence of words and characters.
phishing	Use of email or other online communication methods to trick users into sharing information, opening an infected attachment or clicking a malicious link.
privileges	Access that enables the user to modify IT system configurations, user accounts, audit logs, data files or applications.
ransomware	A type of malicious software that denies access to computers and files and demands that affected organisations make a payment to regain access to their information
security patches	A piece of software designed to fix or update, a computer program or its supporting data.

References

1. Healthcare Breach Report 2019 - Hacking and IT Incidents on the Rise. Available from: https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_HeathcareBreachReport_2019.pdf
2. 47,000 cyber incidents in 12 months. Available from: https://ia.acs.org.au/article/2017/australia_s-cyber-security-compromised-.html
3. Top 10 Health Technology Hazards for 2018. Available from: https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_18.pdf
4. Threat Landscape Report Q2 2017. Available from: https://www.fortinet.com/demand/gated/Fortinet-Threat-Report-Q2-2017.html
5. Ransomware attack on NJ provider locks 16,000 patient records. Available from: http://www.healthcareitnews.com/news/ransomware-attack-nj-provider-locks-16000-patient-records
6. Internet Security Threat Report – Government, Vol 22. Available from: https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf
7. Passwords for business. Available from: https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/passwords-business
8. Verizon 2017 Data Breach Investigation Report. Available from: https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/
9. Information Security Manual. Available from: https://www.cyber.gov.au/ism

Appendix A: Non-proprietary encyrption algorithms

The following tables outline three categories of widely used non-proprietary encryption algorithms[9].

Table A1. Asymmetric (public) key algorithms

Algorithm	*Criteria for use*
Elliptic Curve Diffie–Hellman (ECDH)	Use a field/key size of at least 160 bits, preferably 256 bits.
Diffie–Hellman (DH)	Use a modulus of at least 1024 bits, preferably 2048 bits.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Use a field/key size of at least 160 bits, preferably 256 bits.
Digital Signature Algorithm (DSA)	Use a modulus of at least 1024 bits, preferably 2048 bits.
Rivest–Shamir–Adleman (RSA)	Use a modulus of at least 1024 bits, preferably 2048 bits; and ensure that the key pair used for passing encrypted session keys is different from the key pair used for digital signatures.

Table A2. Hashing algorithms

Algorithm	*Criteria for use*
Secure Hashing Algorithm 2 (SHA–2) family	Use SHA–224, SHA–256, SHA–384 or SHA–512.

Table A3. Symmetric encryption algorithms

Algorithm	*Criteria for use*
Advanced Encryption Standard (AES)	Use key lengths of 128, 192 and 256 bits.
Triple Data Encryption Standard (3DES)	Use three distinct keys.

Publication date: September 2020 - fourth edition.

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Acknowlegements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au