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 template for
vendor responses

This document has been designed as a companion to the Information Security Guide for Small Healthcare Businesses. It includes sample questions regarding a range of IT security considerations, which healthcare providers can ask their IT vendors to assist with selecting secure IT products and services. These discussion items can be used as a basis for a more in-depth conversation with IT vendors about security.

This document provides general guidance only and is not intended to be a comprehensive list of information security requirements.

Awareness – stay alert to stay secure

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?

Click here to enter text.

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

Click here to enter text.

Additional considerations:

- Is documentation available regarding 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)?

  Click here to enter text.
- Do you have a data breach response plan that includes documented processes for taking appropriate action if a suspected or actual data breach occurs?

  Click here to enter text.
- Does the product or service let you set up different levels of user access, relevant to their roles, as an extra security control?

  Click here to enter text.
- Do you offer a variety of training resources and support, to meet different skill levels within our team?

  Click here to enter text.
- Are 24/7 real-time monitoring and alerts are available?

  Click here to enter text.

Backups – prepare for 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?

Click here to enter text.

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

Click here to enter text.

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

Click here to enter text.

Additional consideration:

- What type of encryption algorithm(s) is used to encrypt the data, and how are cryptographic keys managed?

  Click here to enter text.

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

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

Additional considerations:

- Are automatic updates available, and/or manual reminders sent to ensure updates are applied, especially for security patches?

  Click here to enter text.

- What is the format of transaction and audit log files (if we need to be able to aggregate this data with your other log files)?

  Click here to enter text.

- Do settings within the product or service support restricting privileges and limiting access to information according to user roles, as an effective security control?

  Click here to enter text.

- Will other network security measures, such as anti-virus software and mobile applications, be compatible with the new product or service?

  Click here to enter text.

Passphrases – protect your information

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

Additional considerations:

- Does the product or service have the capability to set at least a 14 character complex passphrase?

  Click here to enter text.

- Is use of multiple authentication methods (multi-factor authentication) supported, especially for IT administrator accounts?

  Click here to enter text.

- Does the product require default passwords to be changed, or is this an optional process?

  Click here to enter text.

Privacy – keep your friends close and information closer

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?

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

Additional considerations:

- Do you have awareness of relevant privacy legislation; and does the product or service have sufficient security controls and audit logs to help our business comply with legislated privacy requirements?

  Click here to enter text.

- Is a full copy of healthcare information provided for data retention purposes?

  Click here to enter text.

- How is sensitive information destroyed or de-identified once data retention requirements have been satisfied?

  Click here to enter text.

Information provided for:

Click here to enter text.

Document completed by:

Click here to enter text.

Date completed:

Click here to enter text.

Additional information:

Click here to enter text.

Publication date: September 2020 – fourth edition

Contact for enquiries

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

Acknowledgements
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