Guidance: emailing personal health information

Protecting health information

OFFICIAL

Background

There are many privacy and security risks associated with the use of email services. Emailing personal health information **is not** recommended by the Department of Health.

All health information is sensitive by nature. Communication of personal health information, including by electronic means, must be secure and adequately protect patient privacy.

This advice outlines items to be considered with day-to-day health electronic communication delivery, including the use of email and alternatives to using email.

Responsibilities

Victorian laws protect health information

Health information is sensitive information under the *Health Records Act 2001*. This means there are added restrictions on how service providers must handle health information compared to other types of personal information.

Rights and privacy principles come from two Victorian Acts: *The Health Records Act 2001* and *Information Privacy Act 2000.* Reasonable steps must be taken to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

Further information about the Acts is available at Victorian legislation.

Cybersecurity controls

The department's Digital Health Branch Health Sector Assurance cyber security team specifies several baseline cybersecurity controls for health services to improve the maturity of their cyber security practices.

These controls are best practice and must be applied in all Victorian health services.

One of the controls deals specifically with email. It states that *"Victorian public health services must protect all personal and sensitive data-at-rest and in transit, on portable devices, when using remote cloud-based file storage and during communication over public networks with encryption"*.

What is meant by email security?

Confidentiality

Confidentiality refers to protecting information from being accessed by unauthorised parties. Confidentiality is more than just securing the message content. **Metadata**, information about with whom health services communicate with and when, may be as important and sensitive as the actual content of the email.

Integrity

'Can I trust that a message I receive is correct and unaltered?' And especially important for email, 'Can I trust that the sender really is the claimed one?' Email senders can easily misaddress an email. Email can be received by unintended recipients. Sender **authentication** is critical to electronic communication of health information.

Availability

'Is the message available when authorised users need to access it?' Problems in the emailing system could make it impossible to access information, making the information unavailable when it is required.

Challenges with email security

The device of the sender and receiver

Emails on a sender and a receiver's **device** are easily accessed by others. Others can sit at an unlocked computer, pick up a phone, or read information on a tablet. Email applications are often left open. Even locked screens and passwords are regularly breached, particularly if these are known to others.

Email data is stored in 'files' on devices. 'Malware' programs can access and read those files, and even read and display attachments. Rifling through email is the most common process of malware - software that is specifically designed to gain access or damage a computer without the knowledge of the owner.

Networks the email is sent through

Public email networks are much more open to access from numerous locations. In a scenario where email is hosted external to the organisation and you email a contact external to your organisation, the email is sent over the internet using multiple links or connections before it reaches the recipient. If one connection is secure, there is no guarantee any other connection in the sequence is secure. Even if both end connections are secure, there is no guarantee all other connections in the sequence are secure.

The servers where the email is stored and forwarded

Public email service providers have their own **servers** where they physically store email. If someone cracks or guesses an email password, they can login to the email provider directly and read any email stored there. Many email services store messages as plain text. So, any attacker who can access those servers can easily access all the stored email and attachments.

EMAIL IS NOT A SECURE FORM OF COMMUNICATION

Options

Those handling sensitive health information must take reasonable steps to protect the information, including from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Options which provide greater security and support the electronic exchange of health information include:

- ***Secure messaging or secure message delivery (SMD)*** - secure messaging supports the delivery of messages containing clinical documents and/or other healthcare specific information relating to a client. The Australian Digital Health Agency publishes the details of secure messaging vendors that offer integrated software for health information exchange on their Registers of Conformity. SMD can be set up within clinical software to enable safe and secure transmission of your patient information.
- ***Encryption*** – encryption is achieved with specialist software that renders emails unreadable from the start to the point at which the intended recipient opens them. ICT staff should seek specialist advice on the most appropriate forms of encryption software to enable health services and clinicians to exchange sensitive health information.
- ***Communication via a secure Website portal*** – web-based communication tools with established methods to ensure the data is protected during entry, transit and secured after it arrives.
- ***Microsoft Office 365, OneDrive & SharePoint*** – the Office 365 and/or the Microsoft 365 environment includes protection against common threats. However, IT administrators must configure the recommended security features and perform the security-related tasks to ensure it is up to date. Microsoft Outlook can be configured to send encrypted email. Further advice should be sought from health service IT departments or service providers.

Need further advice

Please contact the Cyber Security team at the Digital Health Branch:
Digital.Health.Incident.Notification@dhhs.vic.gov.au

To receive this document in another format, phone 03 9456 3621, using the National Relay Service 13 36 77 if required, or email the Digital Health Branch, digitalhealth@health.vic.gov.au.

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.