Secure digital communications within the NZ health & disability sector

Implementation guidance

June 2019

Context

Health agencies that hold health information must ensure that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss; access, use, modification, or disclosure, except with the authority of the agency; and other misuse[1].

Communication between health agencies is an essential part of healthcare delivery. Digital communications – e-mail, text, messaging etc. - are commonplace and provide significant operational benefits in improving communication between people and agencies, providing access to health information and supporting clinical and business workflow.

Ensuring that communications, whether analogue or digital, are secure is a fundamental requirement of a modern health system.

Health Information Security Framework (HISF)

The HISF provides guidance on the security safeguards that should be applied by health agencies. Health agencies **must** align their security policies and assess their current security practices, and the digital tools they use, against the guidance provided in the HISF. Security controls must be practical and the impact on agencies workflow and business practice needs to be understood and effectively managed.

This implementation guidance is specific to e-mail and fax; similar guidance on other aspects of the HISF will be released over time.

Problem

The HISF asserts that all patient identifiable information must be protected at rest and in transit. Specifically, chapter 8 of the HISF (Communications) notes that health agencies are required to "ensure the integrity of information communicated across networks… [and] use appropriate encryption standards, when exchanging health information between external parties."

E-mail and fax are two of the most common communication tools used in the health sector. The security of information communicated using these tools currently does not always comply with the HISF; this needs to be addressed.

Fax is an analogue technology that is widely used by health agencies. A common use case is transmission of prescriptions in a legally compliant and clinically assured way between a prescribing physician and receiving pharmacist. Fax poses a number of information and physical security risks and the technology is becoming increasingly incompatible with more modern digital communications solutions.

[1] Health Information Privacy Code [Rule 5]

The Ministry of Health and ACC[2] have collaborated to provide this guidance to support health agencies address the security of e-mail and fax communications. It should be noted that this advice represents an initial step in improving the technical security of these communications; further advice will be forthcoming. This guidance also does not address user generated security issues that agencies should be mitigating through effective cyber security user education.

Guidance

Health agencies are expected to implement the following guidance. The Ministry of Health will work with agencies to support the implementation of this guidance and to provide learnings for subsequent updates.

Health agencies should engage with their technology suppliers for additional advice and support in implementing this guidance.

Secure e-mail

1. All health sector agencies **must** enable opportunistic Transport Layer Security (TLS) version 1.2 or later, on e-mail servers that make incoming or outgoing e-mail connections over public Internet infrastructure no later than January 2020 and advise the Ministry of Health when they have done so (itsecurity@moh.govt.nz).

Fax

2. New analogue fax machines **should not** be purchased, with immediate effect.
3. Health agencies **should** implement one of the following digital alternatives to the use of analogue fax[3] for external communication no later than December 2020 and advise the Ministry of Health when they have done so (itsecurity@moh.govt.nz):
    a. Migrate use of analogue fax to fully digital, security assessed, communication solutions such as e-mail of scanned documents, secure messaging or cloud hosted secure collaboration platforms; or
    b. Utilise the "scan-to-e-mail" capability on a multi-function device (MFD)[4] to scan documents and send them as e-mails (compliant with the secure e-mail requirement in point 1 above).

Ministry of Health

Accident Compensation Corporation

June 2019

[2] The health and disability sector interact frequently with ACC using both fax and digital communications; ACC support a transition to the use of secure digital communications

[3] Where the replacement of analogue fax with digital alternatives is inconsistent with current regulations and policy agencies should contact the Ministry of Health for support. The Ministry of Health is actively seeking a waiver to allow the use of digital alternatives to fax for prescriptions.

[4] Note that some MFDs will provide an analogue fax function. This should not be used unless it has been configured to use secure email to transmit the document as it will continue to have the same security risks as a standalone fax machine.

Supporting technical information

Transport Layer Security (TLS)

TLS, as defined in Internet Engineering Task Force's RFC 3207 standard, is a protocol which provides privacy between communicating applications and their users, or between communicating services. When a server and client communicate, well-configured TLS helps protect against eavesdropping or tampering with messages.

- Detailed guidance for configuring, implementing, and deploying TLS for web servers can be found here; and
- Detailed guidance for configuring, implementing, and deploying TLS for mail servers can be found here.

While it is acknowledged that TLS is not a complete solution to the security of e-mail, the primary advantages are that it:

1. can be easily integrated into existing e-mail servers;
2. is universally interoperable across a wide range of e-mail environments;
3. is able to be easily implemented into/configured within existing ICT environments; and
4. often has no/very low financial barrier to entry.

Securing fax-to-e-mail

To support this technology migration, the following detailed guidance and advice is provided:

- MFD configuration guidance and advice;
- MFD risk-assessment: FTC advice and NIST guidance
- MFD networking: SMTPS and its configuration.