Guidelines for Health Practitioners to securely send Special Authority Application forms to the Ministry of Health.

Scanned Applications attached to an e-mail

This approach provides the lowest acceptable level of security for identifiable data. When using email to move identifiable information, those involved must consider the full lifecycle of the email concerned, including:

- The workstation on which the email is created (copies may remain in draft or in temporary file storage)
- The end-to-end security of each step in the email delivery trail
- Whether all components of the email delivery support encryption-in-transit
- Copies of the email will remain:
    - in the 'sent items' folder of the sender
    - in the 'inbox' of the receiver (or any other file/folder location, if filed)
    - in any system backups for servers that may be running backups whilst the email is in transit
    - in backup copies of either the sender or receiver mailboxes, if a backup is taken whilst the content is present
    - in any email archiving systems that may be active in any part of the mail delivery system.

The Ministry suggests the following protocol for sending Special Authority application forms via e-mail:

- review the document to ensure the correct data is being released (peer review strongly recommended)
- transmit the file via email, ensuring the recipient's email address is accurately entered and that no other recipients are included on the email
- The source file must then be deleted from:
    - Any transient working space not approved for the security of identifiable information
    - The sent items folder of their email system
- The Ministry will extract the required information from the received document, and then:
    - remove the e-mail from their inbox once the data has been extracted, and
    - delete any copies located in transient working space not approved for the security of identifiable information

  Consideration at both ends must be given to the security applied to all components of the system, including workstations, servers, email vendors involved, including backups. The New Zealand Information Security Manual (NZISM) and the Health Information Security Framework (HISF) should serve as baseline security targets, with an appropriate risk-based accreditation in place for all systems.

In addition to the above, Practitioners will need to ensure they send a separate email for each individual form.