PURPOSE

This protocol defines the rights, responsibilities and procedures for communicating and/or transferring Bay of Plenty District Health Board (BOPDHB) held and/or created sensitive data via electronic means.

To accommodate the need to protect sensitive data and the need for efficient communication of such data in support of patient care or business process, sensitive data may be transmitted electronically but only in a manner that meets the requirements of the relevant NZ legislation and health sector standards. When circumstances allow electronic transmission of sensitive data, reasonable and appropriate security measures shall be implemented.

STANDARDS TO BE MET:

1. General Rules for Electronic Communication of Sensitive Data

1.1 Electronic communication or transfer BOPDHB held data should only occur as part of the normal execution of an employee's or contractor's responsibilities and in a manner that is consistent with the BOPDHB's standards of conduct.

1.2 Staff and contractors should be aware that their electronic communications, once sent, can be forwarded, printed and/or stored by recipients. As BOPDHB responsibilities for maintaining the confidentiality of data collected by BOPDHB extend to data communicated to external parties, staff and contractors must exercise extreme caution when communicating sensitive data to third parties.

1.3 While the use of electronic communication tools is recognised as essential to support the administration and communication of all information, the transmission of sensitive data must be constrained by adequate security protocols and guidance.

1.4 Staff or contractors communicating or transferring sensitive data must ensure that the means they use is appropriate for the confidentiality of the data. This includes but is not limited to communication and information exchange:

a) between DHB staff or contractors that is internal to the DHB network resources – eg emails sent within the DHB email system
b) between DHB staff of contractors that is outside of DHB network resources – eg emails sent to private practice or home addresses
c) from DHB staff or contractors to external parties whether those external parties are:
    i. involved in the delivery of clinical care to our patients - eg electronic exchange of data with primary care providers, other DHBs, or
    ii. involved in governance or business related activities – eg Government agencies, contracted service providers/vendors.

1.5 Sensitive data must only be sent using an approved method of secure communication. E-mail and other electronic communication methods are not secure unless data encryption mechanisms are in place at both sender and receiver ends. Confirmation of the security status of a recipient can be sought from Information Technology.

1.6 Sensitive data must be limited to the minimum information necessary for the permitted purpose.

1.7 A BOPDHB email account or other electronic communication mechanism that may send or receive sensitive data must not be auto-forwarded to an external and/or insecure account.

1.8 Notwithstanding the use of secure communication mechanisms the sender of sensitive data has an obligation to ensure they have verified the accuracy of the recipient address.

1.9 Communication of sensitive data to the wrong recipient will be classed as a breach of confidentiality even if the recipient is another BOPDHB employee or contractor. Any breach of confidentiality resulting from using email or other electronic communication means for sensitive data will be investigated and may be deemed as serious misconduct.

2. File Transfers and Temporary Storage

2.1 The use of external file transfer systems to enable the communication of large quantities of data and/or the communication of sensitive data is permitted under specific circumstances and only when approved file transfer systems are used.

2.2 Use of "cloud storage" mechanisms to transfer BOPDHB held data, including sensitive data, is not permitted except where approved cloud storage mechanisms are used.

2.3 For the purposes of clauses 2.1 and 2.2, approval of the transfer and storage mechanisms is the responsibility of the General Manager Information Management or authorised delegate and must comply with Department of Internal Affairs and/or Ministry of Health Cloud Computing Requirements.

3. Retention and Purging of Electronic Messages

3.1 Electronic communication and transfer mechanisms should be used for temporary messaging purposes only and should not be used for filing or otherwise storing information. Electronically communicated sensitive data that is required to be kept for clinical or business activities should be transferred into the DHB's official applications and/or databases.

3.2 Patient specific electronic communications that relate to a patient's treatment while under the care of the DHB, are part of the patient's record and must be transferred into the DHB's relevant patient record system (whether electronic or hardcopy).

3.3 Subject to the DHB's Recordkeeping policies and protocols, all temporary electronic communications once acknowledged and acted upon are to be periodically purged by users from their personal electronic message storage areas.

3.4 Where the DHB provides email capability specifically for communicating sensitive data, users are required to regularly review and act upon the messages in their email accounts to ensure that correspondence and messages relating to patients are promptly dealt with.

4. Patient / Staff Requests for email or other electronic correspondence

4.1 Patient and/or staff requests that email or other electronic correspondence is used to communicate sensitive data are to be treated with care. While such requests imply patient/staff consent for the use of email, the onus remains on the sender to both minimise the risk of unsecure transmission and formalise the consent.

4.2 Patient requests to receive clinical and other personal information via email, or other electronic forms, must be formally recorded in the patient health record.

4.3 Staff requests to receive sensitive data, such as payroll information, via email must be subject to a formal authorisation process with the staff consent recorded within their personal record held by Human Resources (HR).

4.4 The recipient must be informed that responsibility for the confidentiality of the received correspondence rests with them and their personal communication service provider (email or text messaging).

5. Monitoring of Use

5.1 Procedures will be in place to enable the auditing of electronic communication and transfer process use.

5.2 BOPDHB reserves the right to monitor, restrict, suspend or terminate a user's access to any BOPDHB provided electronic communication and/or file transfer system under the following circumstances:

a) The DHB's business need including but not limited to:
   i. routine system administration and/or network traffic management
   ii. an Executive manager's reasonable request
b) A manager's reasonable concern that an individual's use is inappropriate.
c) A reasonable complaint from an affected party that an individual's use is inappropriate.

5.3 Information obtained via monitoring and auditing activities may be disclosed to line managers of staff members involved and other authorities if necessitated by the information retrieved.

6. Breach of Policy and Protocol

6.1 Any breach of this policy will be investigated and may be subject to action under policy 3.50.02 protocol 9 Investigation Process and 3.50.02 protocol 15 Disciplinary Process.

6.2 Staff and contractors must recognise that their actions in communicating sensitive data are subject to NZ legislation and/or the ethical standards of a number of health professional groups. As such a breach of BOPDHB policy may also result in action being taken against an individual by external parties.

ASSOCIATED DOCUMENTS

- Bay of Plenty District Health Board policy 2.6.2 Digital Communication
- Bay of Plenty District Health Board policy 2.6.2 protocol 1 Email Usage
- Bay of Plenty District Health Board policy 2.6.2.protocol 2 Internet Usage
- Bay of Plenty District Health Board policy 2.6.2.protocol 3 Social Media
- Bay of Plenty District Health Board policy 3.50.02 protocol 9 Investigation Process
- Bay of Plenty District Health Board policy 3.50.02 protocol 15 Disciplinary Process