COVID-19 – Emergency Preparedness & Privacy and Security Considerations

Though trustee obligations under PHIA remain static even during a public health event such as the COVID-19 pandemic, trustee capacity to meet policy direction on secure communication methods may be challenged as more people are advised to stay home and electronic communications becomes increasingly necessary.

Key points when disclosing PHI electronically

- Minimum amount need to know: The 'Golden Rule' of privacy is especially important when communicating PHI– such to an individual/ patient using their personal email address for example. Ensure that only the minimum amount of PHI as is necessary for the purpose is communicated or disclosed as well as only with those for whom it is necessary to know this information in order to do their jobs.
- When discussing PHI between providers or with clients/ patients, in-person remains the most secure option. However, when an in-person consultation is not possible, the following may be considered:
    - Telephone
        - For individuals requesting their own PHI or that of someone that they are authorized to receive– authentication is required e.g.
            - Does number calling from match number on file, basic fact questions such as name, DOB, PHIN, address, where did you last receive health care, name of GP etc.
    - Faxing
        - Should only occur in accordance with the **Transmission of Personal Health Information Via Facsimile ("Fax"),** policy
    - Email
        - The measures outlined in the WRHA Guideline for Email Communication should be observed to the greatest extent possible when emailing outside of the secure environment and include:
        - Take into account how urgently the recipient needs the PHI
        - Be sure you are sending the PHI only to the people who need to know the information and to the minimum amount necessary.
        - Double-check recipient address(es) in the "To" fields before you send the email. Send a 'test' email to ensure correct recipient
        - Where personal health information is being sent in the body of an email, only disclose the minimum amount of information required by the recipient and that all personal identifiers are removed (e.g. Mr. Alan Smith could be Mr. S or AS)
        - Encrypt where possible and at minimum password protect any attachments containing personal health information. Passwords should be communicated by phone.

- Where possible, confirm delivery of the email with a delivery receipt or follow-up phone call.

How to password protect a document:

- MS Word:
  - Open the Microsoft Office file you want to protect.
  - Click File.
  - Click Info.
  - Click Protect Document.
  - Click Encrypt with Password.
  - Enter a password and click OK.
  - Confirm your password and click OK.
- Excel:
  - Select File > Info.
  - Select the Protect Workbook box and choose Encrypt with Password.
  - Enter a password in the Password box, and then select OK.
  - Confirm the password in the Reenter Password box, and then select OK.
- PDF:
  - Open the PDF in Acrobat DC.
  - Choose File > Protect Using Password. Alternatively, you can choose Tools > Protect > Protect Using Password
  - Select if you want to set the password for Viewing or Editing the PDF.
  - Type and retype your password.
  - Click Apply.

*** If you are uncertain about what security/encryption tools you may have access to, please talk to your regional or site privacy officer or contact help desk to find out more about what solutions may be available to you.**

Video/Teleconferencing
There are a variety of options for meetings that do not require in person attendance. Contact your IT service provider / Digital Health for assistance with facilitating virtual meetings using technology.

If you have any questions about this or other privacy matters you may contact:

Shared Health
Christina Von Schindler, Shared Health Chief Privacy Officer at 204-926-7049, cvonschindler@sharedhealthmb.ca, or Valerie Gural, Manager of Privacy, Digital Health, 204-926-3634, vgural@sharedhealthmb.ca

Interlake-Eastern Regional Health Authority
Susan Dalman, Regional Privacy Advisor, 204-785-7240, sdalman@ierha.ca

Prairie Mountain Regional Health Authority
Nickie McGregor, Director, Health Information Services, 204- 534-8534, nmcgregor@pmh-mb.ca

Southern Regional Health Authority
Lee Bassett, Regional Officer-Privacy and Access, 204-822-2655, lbassett@southernhealth.ca

Northern Regional Health Authority
Mandy Prange, Regional Privacy and Access Officer, 204-778-1565, mprange2@nrha.ca