AHS Emailing
Personal Identifiable Health Information Procedure

Leading Practice User Guide

Alberta Health Services
Enterprise Information Management
Access, Confidentiality and Security

August 8, 2016
Contents
INTRODUCTION ................................................................................................................................. 4
USER GUIDE ........................................................................................................................................ 6
1. Risks of using emails ..................................................................................................................... 6
   1.1. Risks related to Confidentiality, Privacy and Security .............................................................. 6
      1.1.1. The privacy and security of email communication cannot be guaranteed .................. 6
      1.1.2. Authentication of sender is not possible .......................................................................... 6
      1.1.3. Email accounts and its content do not always have exclusive access ......................... 6
      1.1.4. Email accounts and content can be altered or falsified ............................................... 7
      1.1.5. Emails can be misdirected, intercepted, circulated or stored ...................................... 7
      1.1.6. Emails have a permanent nature ...................................................................................... 7
      1.1.7. Email can introduce viruses .............................................................................................. 7
   1.2. Risks related to timelines associated with email ..................................................................... 7
      1.2.1. Email delivery time is not consistent .............................................................................. 7
      1.2.2. Response time to an email is not guaranteed .................................................................. 8
   1.3. Risks related to unclear email communication ..................................................................... 8
      1.3.1. Inherent limitations of using email .................................................................................... 8
   2. Conditions of using email .......................................................................................................... 8
      2.1. Encounter management ....................................................................................................... 8
      2.1.1. Determine who the recipient is .......................................................................................... 8
      2.1.2. Determine appropriate type of email encounter ................................................................ 8
      2.1.3. Determine content of email ............................................................................................. 9
      2.1.4. Determine responsibilities ............................................................................................... 9
   3. Mitigating the risks: (Instructions for communicating by email) ............................................... 10
      3.1. Requirements for Computer use .......................................................................................... 10
      3.1.1. Use only AHS approved email accounts to send personal identifiable health information ... 10
      3.1.2. Take precautions to preserve the confidentiality of emails ............................................ 10
      3.1.3. Use Encryption when sending an email to all non-AHS email addresses ....................... 10
      3.2. Requirements for emailing personal identifiable health information to a patient ............... 11
      3.2.1. Obtain permission to use email as a means of communicating personal identifiable health information ................................................................. 11
      3.2.2. Verify the email address with the patient using encryption .......................................... 11
      3.2.3. Adhere to standard formats and requirements when sending encrypted emails to patients .... 12
      3.2.4. Adhere to Email Lifecycle Standards .............................................................................. 13
      3.2.5. Adhere to Clinical Documentation Standards ................................................................. 13
      3.2.6. Adhere to Confidentiality, Privacy and Security ............................................................... 14
      3.3. Requirements for emailing personal identifiable health information to health care providers .... 14
      3.3.1. Obtain agreement to use email as a means of communicating personal identifiable health information with another health care provider .................................................. 15
      3.3.2. Verify the receiving health care provider’s email account .............................................. 15
      3.3.3. Use Encryption when sending personal identifiable health information by email to all non-AHS email addresses ................................................................. 15
      3.3.4. Adhere to Email Lifecycle Standards .............................................................................. 15
      3.3.5. Adhere to Clinical Documentation Standards ................................................................. 15
      3.3.6. Adhere to Confidentiality, Privacy and Security Standard .............................................. 15
      3.3.7. Type of personal identifiable health information that cannot be sent by email ................... 16
   3.4. Respond in a Timely Way ....................................................................................................... 16
      3.4.1. Measures to help mitigate the potential legal risks associated with timeliness ............... 16
   3.5. Communicate Clearly ............................................................................................................. 16
3.5.1. Measures to help mitigate the potential risks associated with clarity of communication ...........17
Appendix A DEFINITIONS ..................................................................................................................18
Appendix B REFERENCES ..................................................................................................................20
Appendix C STEP BY STEP PROCESS ............................................................................................21
Appendix D TRANSMISSION - FLOW ...............................................................................................30
Appendix E REQUIREMENTS - FLOW ...............................................................................................31
INTRODUCTION

This User Guide document aligns with the procedure “Emailing Personal Health Information”. Alberta Health Services (AHS) offers health care providers (HCP) and patients the opportunity to transmit personal identifiable health information via email. Policy #1113 Transmission of Information by Facsimile or Electronic Mail sets out conditions by which personal identifiable health information may be transmitted by fax or email. Transmitting personal identifiable health information poses several risks of which the HCP and patient should be aware. The HCP and patient should only agree to communicate via email when these risks are understood and accepted.

Always use methods of transferring personal identifiable health information with fewer risks if they are available and appropriate for the situation.

**Recognize risk**
Use of any non-AHS sanctioned and tested system for clinical communications, exposes the user to accountability for fault or breach, subject to the full force of fines, penalty and loss of privilege specified in the Alberta Health Information Act, civil litigation or any AHS bylaw, rule, policy or procedure.

**Recognize and Protect Clinical Communications**
Transitory communications about work processes (e.g. request to meet) do not require CSM protections if they do not contain information that might identify a patient or record substantive clinical discourse. Communications about individuals and the care they receive must be reproduced within a CIS.

**Obtain Consent**
Solicit, obtain and record the recipient’s consent to use a particular secure communication technology in support of patient care.

**Use the most Integrated and Secure CSM Option**

- **Within-CIS Messaging** - Always use messaging solutions within a CIS when sender and recipient can use the same CIS. Consider alerting the recipient via email or instant messaging that they have a CIS message awaiting attention.

- **Within-EHR Messaging** - Prefer within-EHR messaging if the sender and recipient(s) are not on the same CIS and are willing to use Netcare messaging. Consider alerting the recipient via email or instant messaging that they have a Netcare message awaiting attention.

- **AHS Secure E-Mail** - If both sender and receiver have AHS email addresses (@albertahealthservices.ca or @ahs.ca), then clinical communications can be sent and received without further protections. If the sender has an AHS email address but the receiver does not, then add “!Private” to the subject line so the email message is encrypted. If the receiver has an AHS email address but the sender does not, do not use AHS email for secure clinical communications.

- **External OIPC Approved CSM Solution** - If none of the above are appropriate, consider use of an external CSM solution that meets Health Information Act requirements. Use an appropriate CSM transcript feature to extract a clinical communication “thread” for copy-paste or attachment to an appropriate CIS.
encounter (e.g. “Telephone encounter”).

Manage Attachments
Extract any objects (e.g. consultation letter) attached to a secure communication and follow CIS-specific guides for selecting material to attach to an appropriate CIS encounter record.

Many forms of electronic transfer exist. This procedure and user guide applies to the method of transferring personal identifiable health information via email and excludes any advice on other methods such as texting, portal use, dropbox etc.

AHS will use reasonable means to protect the security and confidentiality of email information sent and received.

This User Guide applies to all AHS registered patients that have a patient-health care provider relationship (excluding prospective and virtual patients – see section 2.1.1) and have agreed to use email as a means to communicate personal identifiable health information and all health care providers who wish to use email as a means to transmit personal identifiable health information.

Note: This document and links were up to date on “August 2016”
For accurate up to date information please visit the appropriate internal and external websites.

Note: Appendix C provides a step-by-step example of the process of sending encrypted emails
USER GUIDE

1. Risks of using emails

1.1. Risks related to Confidentiality, Privacy and Security

1.1.1. The privacy and security of email communication cannot be guaranteed

- Risks through intended or unintended actions associated with sending personal identifiable health information by email.
  - There are always risks associated with sending personal identifiable health information by email.
  - Most of these risks are unintended as explained in the following sections.
  - Some risks are due to intended wrongdoing. Examples include but are not limited to:
    - hijacking of accounts in which an account is taken over with the intention of wrongdoing
    - altering of information to deceive

1.1.2. Authentication of sender is not possible

- Risk of not knowing the true identity of the sender of the email.
  - It is impossible to verify the true identity of the sender.
  - The fact that the email originates from the sender’s email account (either patient or health care provider) does not authenticate the sender.
  - Emails unlike a written paper or a faxed paper do not contain a handwritten signature.

1.1.3. Email account and its content do not always have exclusive access

- Risk that personal identifiable health information will be disclosed to or accessed by individuals other than the intended recipients.
  - Patient’s email accounts may not be individual accounts:
    - other individuals may have access to these accounts or
    - the accounts may be family/joint accounts or
    - the account could be on an employer’s server and be accessed by the employer
  - Health care provider’s email accounts may not be individual accounts:
    - other individuals such as co-workers may have access as a delegate or
    - the account may be a group account
  - Receiving emails from AHS or specific AHS programs/departments may identify or infer the potential nature of the personal identifiable health information. This may be something the patient may not want others to see. E.g. an email from AHS – Cancer Clinic in a shared email account.
  - AHS has the legal right to inspect and retain emails that pass through its system.
  - Use of email to discuss sensitive information can increase the risk of such information being disclosed to third parties.
  - As risk of disclosure is greater, provide the least amount of information needed for the communication.
1.1.4. **Email accounts and content can be altered or falsified**  
- Risk of altering or falsifying personal identifiable health information.  
  - Email is easier to alter or falsify than handwritten or signed hard copies or entries in an audited electronic health record.  
  - Adding or deleting text is easier.  
  - It is possible to take over possession or mimic legitimate accounts.

1.1.5. **Emails can be misdirected, intercepted, circulated or stored**  
- Risk of using personal identifiable health information for anything other than intended.  
  - Email can be forwarded, intercepted, circulated, or stored by the patient or health care provider or without the knowledge or permission of the patient or health care provider.  
  - Email senders can easily misaddress an email, resulting in it being sent to many unintended and/or unknown recipients.  
  - Do not use BCC (Blind Carbon Copy) in order to be as transparent as possible.  
  - Do not automatically “reply to all”. Be selective who needs to have this information for the care of the patient.

1.1.6. **Emails have a permanent nature**  
- Risk of never being able to truly delete personal identifiable health information in emails.  
  - Email is indelible.  
  - Even after the sender and recipient have deleted their copies of the email, back-up copies may exist on a computer or in cyberspace.  
  - Email can be used as evidence in court.

1.1.7. **Email can introduce viruses**  
- Risk of introducing unwanted elements such as viruses to the electronic systems.  
  - Emails can introduce viruses into a computer system, and potentially damage or disrupt the computer.  
  - Viruses come in many forms and may forward information from your account automatically.

1.2. **Risks related to timelines associated with email**

1.2.1. **Email delivery time is not consistent**  
- Delays in email delivery make email a poor method for exchanging time-sensitive information.  
  - Contrary to common belief, email is not instantaneous and can arrive hours or even days after it is sent.  
  - Email may therefore be a poor method for exchanging time-sensitive information.

> Never use email in an emergency.  
> Instead call 911 or call [Health Link Alberta - 811](http://www.healthlinkalberta.ca)
1.2.2. **Response time to an email is not guaranteed**
- AHS cannot guarantee that any particular email will be read and/or responded to within an expected period of time.
  - Email may introduce expectations about response time
  - Although health care providers will try to read and respond promptly to an email from the patient, AHS cannot guarantee that any particular email will be read and responded to within any particular period of time.
  - Thus, the patient should not use email for medical emergencies or other time-sensitive matters.

1.3. **Risks related to unclear email communication**

1.3.1. **Inherent limitations of using email**
- Email is text based, making it more difficult to clearly convey intended messages.
  - It is more difficult to express something by typing text only. Remember the person receiving the email cannot see your body language or facial expressions.
  - The intended messages may be misinterpreted.

2. **Conditions of using email**

2.1. **Encounter management**

2.1.1. **Determine who the recipient is**
- Email communication is mutually agreed between existing patients and health care provider(s).
  - Email Communication should only be used with existing AHS patients where a prior professional relationship exists. The email communication is in the context of a patient-health care provider relationship.
  - Likewise email communication when used between health care providers needs to be mutually agreed to.
  - Communication with prospective patients (no prior relationship exists) or virtual patients (only an online relationship exists) is not part of the procedure and this user guide.

2.1.2. **Determine appropriate type of email encounter**
- Email communication has limitations and associated risks, therefore other types of transferring information needs to be considered first, including but not limited to, phoning, faxing, mailing or handing the information in person. The encounter needs to be suitable for the type and level of information exchanged. For example email communication must not be used where an in-person meeting would be more appropriate, where it is critical that a patient has received and understood the information and where appropriate follow up is crucial.
  - Determination of the type of information exchanged needs to be made in advance as an agreement between patient and health care provider.
  - Email communication is not an appropriate substitute for clinical interaction.
  - Expanding on the examples of email use as outlined in the procedure document:
Administrative activities may include scheduling appointments including rebooking and cancellation; payments for uninsured services; providing directions to the practice location or other facilities; and providing privacy policy, clinic operations guidelines and access and disclosure information.

Education and health promotion may include general educational and health promotion attachments and resources; providing links to resources on websites; incorporate personal identifiable health information messages; providing links to online self-assessment and help tools; providing newsletters and community support resources.

Patient care information or instructions such as receiving patients requests for prescription refills; clarifying or reiterating instructions; receiving and answering follow up questions; or providing post procedure instructions.

Research purpose means any information that is transferred by email related to research associated with personal identifiable health information of a patient.

2.1.3. Determine content of email
- Health care providers and patients must agree and keep updated which if any sensitive medical information can be transmitted.
  - Due to considerable risk in sending personal identifiable health information health care providers and patients must agree which if any sensitive medical information can be transmitted.
  - The patient is responsible for informing the health care provider of any types of information the patient does not want to be sent by email.
  - The patient can add to or modify this list at any time by notifying the health care provider.

2.1.4. Determine responsibilities
- The patient is responsible for following up on the health care provider’s email and for scheduling appointments where warranted.
  - If the patient’s email requires a response from the health care provider and the patient has not received a response within a predetermined reasonable period of time, it is the patient’s responsibility to follow up to determine whether the intended recipient received the email and when the recipient will respond.
- The health care provider is responsible to ensure that any following up and scheduling concerns that arise through email communication with the patient is in line with the practices and procedures that exist in the care setting or care context where the patient is receiving services as related to the email.
- The health care provider is responsible for all documentation and records management processes to ensure the appropriate information is added to the health record.
- Health care providers may forward emails internally to other health care providers involved, as necessary, for diagnosis, treatment, reimbursement, health care operations and other handling in accordance with the Procedure and section 3.3 of this User Guide.
- Health care providers will not forward emails to independent third parties without the patient’s prior written consent, except as authorized or required by law.
3. Mitigating the risks: (Instructions for communicating by email)

3.1. Requirements for Computer use

3.1.1. Use only AHS approved email accounts to send personal identifiable health information

- Sending personal identifiable health information from a non-AHS email account (not ending in @albertahealthservices.ca or @ahs.ca) needs prior authorization from Information Risk Management.
- Email sent outside the AHS network is not secure; when you send an email, it could be intercepted or forwarded to other recipients.
- Even if the email address is located in AHS-global email list it cannot be assumed to be secure if it does not have the @albertahealthservices.ca or @ahs.ca extension.
- Organizations that use the Alberta Supernet may not comply with the security requirements and encryption must be used to communicate with those organizations unless authorized by Information Risk Management.
- Check with IT service-desk if contracts exist between AHS and certain institutions to determine if sending personal identifiable health information to those email accounts is considered secure.
- Any accounts external to AHS (E.g. private offices, personal accounts) must not be used unless they have been determined to be secure by Information Risk Management.
- If you are unsure about the status of an external email account, contact your local IT service-desk to start the verification process.
- Only use email accounts that you (or someone else in case of a group account) have access to.

Note: University of Alberta (UofA) and University of Calgary (UoC) clinical staff are not permitted to access or transmit personal identifiable health information on either UofA or UoC email systems.

3.1.2. Take precautions to preserve the confidentiality of emails

- Use caution when using computers and email by following safe practices.
  - use screen savers
  - safeguard computer passwords
  - log off or lock computers when away from keyboard
  - only use accounts assigned to you

3.1.3. Use Encryption when sending an email to all non-AHS email addresses

- If you are emailing sensitive information to an external address (one that does not end in @albertahealthservices.ca), you must encrypt your email to make sure only your intended recipient can open it.
- Use of encryption technology must be manually added when emailing personal identifiable health information to an external email account by using the AHS encryption guidelines.
- Within the AHS network email does not need encryption. The first.lastname@albertahealthservices.ca will indicate that the connection is secure. For other secure email addresses refer to section 3.1.1.
- Sending an email from an internal account to another internal account does not require encryption because the information does not leave the physical network. When sites are remote e.g. rural Alberta to an urban centre and the information leaves the physical network, AHS will use the Supernet, which uses encryption on both ends of the connection.
- Follow AHS guidelines on “Guide to Email Encryption” on InSite by typing: !Private in the subject line, or how to change the sensitivity settings in MS-Outlook.
  - The patient or external health care provider will receive an email with instructions to log into a secure website to retrieve the email.
  - The word “!Private” will also appear in the subject line of the email the patient or external health care provider receives.
  - Some internet providers will mark this type of email as “junk” or “spam”. Tell your patients/other recipients to look in spam or junk email folders as well.
- As per policy Transmission of Information by Facsimile or Electronic Mail (1113) (https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-transmission-information.pdf) a disclaimer will automatically be attached to each transmission sent to an external email account.

3.2. Requirements for emailing personal identifiable health information to a patient

3.2.1. Obtain permission to use email as a means of communicating personal identifiable health information
- Obtain permission to communicate by email by obtaining the patient’s valid email address and informing the patient about the risks and encryption process.
  - To use email as a means of communicating a prior relationship must exist.
  - Inform the patient about risks and avoiding risks.
  - Obtain the patient’s permission to communicate by email.
  - Obtain a valid secure email address from the patient.
  - Explain the encryption process to the patient, requiring registration at a website.
  - Document this action in the patient’s health record.

**Example** <<Documenting permission>>

02 Apr 2014 14:15  Mrs. Jones was informed about benefits and risks of using email. She was informed about ways to avoid these risks including the need for encryption. Mrs. Jones is willing to proceed with sending and receiving personal identifiable health information by email excluding lab-results and she was informed that she can revoke or change this permission at any time. Mrs. Jones provided her email to be YouAtHome@YourProvider.com. The encryption process was explained.--------

---------------------------S. James RN {signature}

3.2.2. Verify the email address with the patient using encryption
- Before sending encrypted personal identifiable health information the email address needs to be verified with the patient by sending an encrypted email requesting confirmation.
  - Send a verification email to the provided email address containing this text:
    - Subject line: “Verification of email address !Private”
Body of email: “To verify that this email address belongs to the intended individual, please provide the following information about the patient in your reply: First and last name, and Personal Health Number”

Attachment: attach the brochure “Emailing personal identifiable health information Leading Practice User Guide”

- Once verified this email address can be used to send encrypted personal identifiable health information.
- Re-confirm verification if the last email communication was not recent.
- Document this action in the patient’s health record.

3.2.3. Adhere to standard formats and requirements when sending encrypted emails to patients

- Subject lines cannot contain identifiable personal identifiable health information but can provide general details about the purpose of the email.
- Do not put any identifiable personal identifiable health information including patient’s name or personal health number in the subject line
- Provide general detail about the purpose of the email. Example: “Confidential - Communication from AHS or program !Private” or “Confidential - Communication from AHS or program” and use the sensitivity settings in MS-Outlook.

- Body of the email and attachment must positively identify the patient by providing identifiers: first name, last name, and personal health number.
  - Each email and attachment must positively identify the patient by providing identifiers: first name, last name, and personal health number.
  - Each email and attachment must contain the health care workers identifiable information including a AHS Email Signature. AHS Email Signature Standard.
    - The signature block should contain: name and credentials, title, department name, address and contact numbers as well as the words “Alberta Health Services” and Alberta Health Services website address. If program information is appropriate you may want to indicate this program information in the body of the email.
    - Some licensing bodies have specific requirements for the format of signature information.
  - It is good practice to put a message in the body of the email requesting confirmation of the receipt of this email and if the message was understood. Example: “Please confirm that you have read and understood this email with # attachment(s) by sending a reply indicating “read and understood with # attachments”
  - In order to prevent expectations to use email as a means of contact in an emergency, the content must include the following standard statement: “Never use email in emergency. Call 911 or Health Link Alberta 811.”

Outlook email allows for the setup of several email blocks. Create a special “email personal identifiable health information” block containing the last three bullets.
3.2.4. **Adhere to Email Lifecycle Process**

- Personal identifiable health information contained in an email message that is in an individual or group email account is not part of the health record until it is filed on the health record as such. Refer to the [Records Management policy (#1113)](https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-records-management.pdf)

  - It is up to the health care provider to determine (often guided by regulation/medical staff rules), which part or all of the content is relevant to be part of the health record.
  - Determining relevance should adhere to the same rigor a health care provider would use in any other form of communication (verbal, telephone).
  - Depending on relevance of the content an email message may be transferred in its entirety such as imported into the electronic health record as a direct email feed, or imported as a PDF version of the record, or printed and placed on the paper health record. In this situation the entire original email becomes a permanent part of the health record.
  - If the health care provider determines that only part of the email content is relevant to patient care the health care provider must make a narrative note of this information or sever by copy-paste and file on the health record. If none of the information in the email is relevant to patient care and the content does not serve any other retention value, the health care provider can delete the email without making any part of the content a part of the health record. In this situation the original email content was a transitory record and does not become a permanent part of the health record. See [Clinical Copy-Paste guide](http://ahs-cis.ca/ccp), [Records Management policy #1113](https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-records-management.pdf), and [Transitory Records procedure #1133-03](https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-records-management.pdf)

  - The first method of making the entire email a part of the health record is preferred because it carries less risk.
  - Regardless of method when any part of the email or email narrative is entered into the health record, reference of date of the original email, person the information was received from needs to be logged in the health record.
  - Once relevant information is transferred to the health record the original email and any copies must be permanently deleted (purged) from any individual or group accounts.

3.2.5. **Adhere to Clinical Documentation Standards**

- The health care provider uses his/her professional judgment (often guided by regulation/medical staff rules) to determine if part or all of the information is relevant to add to the health record.
- Any relevant information contained in the email must be added to the health record using appropriate documentation standards.
- Because emails and content may become part of the health record they must conform to clinical documentation standards. e.g.:
  - Identify the patient
  - Identify the health care provider
  - Remain on topic and about one patient only
- If all content of an email is relevant to be added to the health record:
  - Print the email and add to health record following documentation standards
- If part of the content of an email is relevant to be added to the health record:
  - Sever the information that is not relevant before printing the email.
Print and then sever the non-relevant information before adding to the health record.

- Transcribe the relevant information directly into the health record
- When adding a printed email document to the health record follow documentation standards by:
  - Appropriately labeling the printed document: e.g. Identification label.
  - Making an entry in the appropriate section in the health record including date/time of entry, description of content to be added indicating the number of pages and name/designation and signature of the health care provider adding the information to the health record.
  - Adhering to rules of chronological entries by drawing a line through the remaining empty space on the page to add the printed email as the next page(s).
- As per Transitory Records procedure (1133-03) a duplicate record may be appropriately purged. (Delete email and empty trash)
- As per Transitory Records procedure (1133-03) a record that contains information that has value substantiating or providing background material must be kept.

Example: <<2 page email printed and added to the health record>>
02 Apr 2014 18:15  Added email (2 pages) received from Dr. Jones on April 01, instructing on movement limitations after surgery.------------------------ S. James RN {signature}

Example: <<1 page email severed then printed and added to the health record>>
02 Apr 2014 18:15  Added email (1 page non-relevant content severed) received from Dr. Jones on April 01, instructing on movement limitations after surgery. ------------------------ S. James RN {signature}

Example: <<transcribed information from an email>>
02 Apr 2014 18:15  Transcription of email received by writer from Dr. Jones on April 01 16:05 addressed to all staff, received by writer, instructing on movement limitations after surgery: no external rotation of the Left hip allowed for 6 weeks. Email purged after transcription.------------------------ S. James RN {signature}

3.2.6. **Adhere to Confidentiality, Privacy and Security**
- Forwarding and transmitting any emails must comply with Collection, Access, Use and Disclosure of Information policy #1112.
- Using the Clinical Copy-Paste guide ([http://ahs-cis.ca/ccp](http://ahs-cis.ca/ccp)) any relevant information is transferred to the health record.
- Personal identifiable health information transmitted by email must be related to the need to transmit the personal identifiable health information and is to limit to the one patient the email was intended for or about and contain only the least amount of information required for healthcare service delivery.

3.3. **Requirements for emailing personal identifiable health information to health care providers**
3.3.1. Obtain agreement to use email as a means of communicating personal identifiable health information with another health care provider

- Ensure the other health care provider has agreed that using email is an acceptable means to send the agreed upon personal identifiable health information.
- Obtain a valid secure email address from the health care provider that is monitored on a regular basis.
  - As per process described in 3.1.1 above make sure the recipient’s email address is secure.

3.3.2. Verify the receiving health care provider’s email account

- Non-AHS email accounts:
  - Before sending personal identifiable health information the email address needs to be verified with the health care provider by sending an encrypted verification email.
- AHS email accounts:
  - Verify the receiving health care provider’s email address verbally or for extra security by sending a verification email.
  - Verification emails sent to AHS email accounts do not need to be encrypted.
  - A verification email may be appropriate if the email address is not in the “global” list or was not sufficiently confirmed by the health care provider.
  - Once confirmed that the recipient has agreed to receive personal identifiable health information via a secure specific email account that email account can be used for receiving non encrypted personal identifiable health information.

3.3.3. Use Encryption when sending personal identifiable health information by email

- Encryption is needed when sending personal identifiable health information to a health care provider without an AHS email account (@albertahealthservices.ca or @ahs.ca ) using the methods described in 3.1.3
- Never place identifiable information in the subject line regardless if the email is transmitted internal or external. Adhere to rules about subject line, and body of email as described in 3.2.3
- Only email accounts that have the @albertahealthservices.ca or @ahs.ca extension in the AHS global email listing ‘global’, are secure. For others verification by IT is needed.

3.3.4. Adhere to Email Lifecycle Process

- Refer to section 3.2.4 for guidance on email lifecycle standards.
  - Lifecycle standards for emailing personal identifiable health information to health care providers are the same as for the patient section.

3.3.5. Adhere to Clinical Documentation Standards

- Refer to section 3.2.5 for guidance on clinical documentation standards.
  - Documentation standards for emailing personal identifiable health information to health care providers are the same as for the patient section.

3.3.6. Adhere to Confidentiality, Privacy and Security Standard

- Refer to section 3.2.6 for compliance to the Collection, Access, Use and Disclosure of Information policy #1112.
Using the Clinical Copy-Paste guide (http://ahs-cis.ca/ccp) any relevant information is transferred to the health record.

Personal identifiable health information transmitted by email must be related to the need to transmit the personal identifiable health information and is to limit to the one patient the email was intended for or about and contain only the least amount of information required for healthcare service delivery.

3.3.7. Type of personal identifiable health information that cannot be sent by email

- Orders are not to be transmitted by email to health care providers with the exception that hand-signed, scanned medication orders (new, refills, or changes) may be transmitted by email to health care providers with an internal email account.
- Health care providers must decide if information is appropriate for communicating by email or would be better done in person or other methods.

3.4. Respond in a Timely Way

3.4.1. Measures to help mitigate the risks associated with timeliness

- Standardize format of emails to easily triage priorities.
- Locally establish target turnaround times for your service and make sure contingency is in place if this cannot be met due to absence of health care provider, or other priorities.
  - Establish a target turn-around time for messages received from patients and other health care providers who are involved in your patients' care.
    - Different enquiries may warrant different response times
    - Consider response during times of service closure (weekends, vacations, statutory holidays)
- Use automatic replies to acknowledge receipt of emails indicating the protocol for response with directions to alternative contacts in case of urgency.
- Standardize subject heading categories with triaging priorities to facilitate timely responses. The subject headings content and context of the message can indicate the expected turnaround time, and responses can be prioritized accordingly.
- Limit time required to read and respond to patient communications by encouraging or requiring limited text from patients; restricting communications to single or simple issues; encouraging or requiring office visits for complex matters.
- Use templates to limit information and standardize information if appropriate.
- Inform patients of escalation procedures to follow if they do not receive a response from the health care provider in a reasonable amount of time, or if the symptoms or problems worsen.
- Include a statement to clarify that the patient is responsible for initiating any follow-up on health care provider - patient emails.

3.5. Communicate Clearly
3.5.1. Measures to help mitigate the potential risks associated with clarity of communication

- Emails lack the characteristics of face to face human interaction. Therefore avoid emotions, acronyms or abbreviations that can be misinterpreted.
- Inform patients that the content of their emails may be included in their health record.

  - Avoid acronyms or medical terms unless they are explained in the first instance the acronym appears.
  - Be aware that lay people may not know that common words can have medical meaning.
  - Avoid anger, sarcasm, harsh criticism, gratuitous comments and libellous references. Since most email is text based, it is difficult to communicate humour or wit, sensitivity, warmth and other emotions, and such comments can be taken out of context or overemphasized by the recipient. Consider first whether it is appropriate to communicate by email in this context.
  - Word emails carefully. Emails create an indelible trail, even after copies have been deleted from the computers of the sender and recipient.
Appendix A  DEFINITIONS

**External email account** means an email account without an AHS email address or not verified as secure by the Information Risk Management in accordance with the *Transmission of Information by Facsimile and Electronic Mail Policy*.

**Health Care Provider** means any person who provides goods or services to a patient, inclusive of health care professionals, staff, students, volunteers, and other persons acting on behalf of or in conjunction with AHS.

**Personal identifiable health information** means information that identifies an individual and is stored in any format that relates to:
   a) diagnosis, treatment and care; and
   b) registration (e.g., demographics, residency, health services eligibility, or billing).

**Health record** means the AHS legal record of the patient’s diagnostic, treatment, and care information.

**Internal email account** means an email account with an AHS email address or an email account that has been verified as secure by the Information Risk Management in accordance with the *Transmission of Information by Facsimile and Electronic Mail Policy*.

**Order** means a direction given by a regulated health care professional to carry out specific activity(ies) as part of the diagnostic and/or therapeutic care and treatment to the benefit of a patient. An order may be written (including handwritten and or electronic), verbal, by telephone or facsimile.

**Patient** means all persons who receive or have requested health care or services from Alberta Health Services and its health care providers, and also means, where applicable:
   a) a co-decision-maker with the person; or
   b) an alternate decision-maker on behalf of the person.

**Signature block** means an individual’s name, title, credentials, and contact information that is added to the end of an email. A signature block is not an electronic/digital signature.

**Transitory record** means records in any media that:
   - have no further value or usefulness beyond an immediate and minor transaction;
   - are only required for a short time during and not usually after a transaction;
   - are made obsolete by an updated version of a record, subsequent transaction, or decision;
   - are a duplicate or copy of a record filed elsewhere; or
   - are a work in progress or draft version that will have no further value once the final version is produced.

Transitory records do not document client care, document a decision or transaction, support business activities, provide evidence of compliance with legislative requirement, nor have future business, financial, legal, research or archival value to AHS (see *Transitory Records Procedure*).
Transmission means the sending of information (including files and images) using electronic means such as fax, email, or other technologies.
Appendix B REFERENCES

1113-01 - Procedure: Emailing Personal Identifiable Health Information

Clinical User Guide: Clinical Copy-Paste guide

How to Encrypt Email/ Changing Sensitivity settings in Outlook

Visual Identity Standards Email Signature – Microsoft Outlook

1112 - Collection, Access, Use and Disclosure of Information

Office of the Information and Privacy Commissioner of Alberta (OIPCA)
Communicating with patients via email: Know the risks

1133 - Records Management

1133-03 – Transitory Records

1113 - Transmission of Information by Facsimile or Electronic Mail
Appendix C

STEP BY STEP PROCESS

What are the steps involved to transmit personal identifiable health information by email to patients?

**Step 1**
**Determine suitability** refer to section 2.1.1

You, the health care provider, and your patient would like to use email to transfer personal identifiable health information. You have a prior professional relationship and you have assessed that email would be the best way of communicating the intended type of information.

**Step 2**
**Inform about risk and process** refer to section 3.2.1

You explain the risks, benefits and requirements to use email to transfer personal identifiable health information to the patient. Remind the patient to look for the message which may be located in their junk or spam email folder. You document this action in the health record.

**Step 3**
**Obtain agreement** refer to section 3.2.1

You and your patient agree to use email to transfer personal identifiable health information.

**Step 4**
**Obtain an email address** refer to section 3.2.1

You obtain your patient’s email address: e.g. You.AtHome@yourprovider.com

**Step 5**
**Verification of the email address** refer to section 3.2.2

You send your patient an encrypted email to confirm that the email address that was provided to you by the patient is the correct one.
**Example:** The email as it appears to your patient when you send an encrypted email and the steps they need to follow (step 6 – 14)

From: Your.HealthCareProvider@albertahealthservices.ca  
To: You.AtHome@yourprovider.com  
Date: Monday 2012-12-03 13:06  
Subject: Verification of email address - !Private

---

**Your.HealthCareProvider**  
Speech Language Pathologist  
Our Program Services  
Health Care Centre  

67 The Address  
City, AB  
Your.HealthCareProvider@albertahealthservices.ca

403-000-0000  
Alberta Health Services  
www.albertahealthservices.ca

---

**Step 6**  
**Encryption process** locate the attachment to the email

There is an attachment to the email e.g. Encrypted_Message.htm  
(NB. All computer systems are different and the above message examples may appear different on your patients' computer. However the steps and process are the same).
**Step 7**

Encryption process Launch the attachment to the email

Click on the “htm” file. This will open a web-browser

**Example:** The message as it appears to your patient

![Encryption Portal](image)

**Step 8**

Encryption process Installing the software

Click on “Open Message” which will open an install program (if not already installed on your patient’s computer) and install the program by clicking on “Install”

**Example:** The message as it appears to your patient

![Internet Explorer - Security Warning](image)
Step 9

Encryption process

Registration

Once installed the patient will need to register their email address.

Step 10

Encryption process

Registration

The patient completes the registration information and clicks continue

NB The patient needs to make sure to memorize their password for future logon.
Step 11

**Encryption process**

Your patient will now be prompted to check their email folder for a message to activate their account.

**Activation**

---

**Please Check Your Email to Activate Your Account**

Check your inbox for a registration confirmation email message and follow instructions in the email message to confirm your encryption account.

From: accounts-noreply@trendmicro.com
To: You.AtHome@yourprovider.com

Note: If you do not see a registration confirmation email in your inbox, check your spam folder.

---

Step 12

**Encryption process**

In your patient’s email folder there will be an email from the encryption server to click a link to complete the registration.

**Activation**

---

**Example:** The message to confirm registration as it may appears to your patient

From: You.AtHome@yourprovider.com
To: accounts-noreply@trendmicro.com
Date: Monday 2012-12-03 13:20
Subject: Registration confirmation – Trend Micro Email Encryption

---

Visit the link in the email to confirm your email address.

http://www.myprivatemail.com/zero/setup/email.aspx?email=YourEmailAddress&confirm=1

---

If you need more information, please visit:

http://support.privatemail.com

Sincerely,
Trend Micro

---

Step 13

**Encryption process**

**viewing encrypted emails**
Your patient has now registered and activated their account. They can open the encrypted email which may look like this:

**Example:** The patient now can access the email you sent online in the website

```
From: Your.HealthCareProvider@albertahealthservices.ca
To: You.AtHome@yourprovider.com
Date: Monday 2012-12-03 13:06
Subject: Verification of email address - !private

To verify that this email address belongs to the intended individual, please provide the following information about the patient in your reply: First name, last name and Personal Health Number (PHN).

Y our.H ealthC areP rovider
Speech Language Pathologist
Our Program Services
Health Care Centre

67 The Address
City, AB
Your.HealthCareProvider@albertahealthservices.ca

403-000-0000

A lberta H ealth S ervices
www.albertahealthservices.ca
```

This message and any attached documents are only for the use of the intended recipient(s), are confidential and may contain privileged information. Any unauthorized review, use, retransmission, or other disclosure is strictly prohibited. If you have received this message in error, please notify the sender immediately, and then delete the original message. Thank you.
Step 14: Confirming receipt (refer to section 3.2.3)

Your patient should now reply with the requested information

Example: example of a reply to health care provider with verifying information

---

Reply Securely

From: You.AtHome@YourProvider.com
To: Your.Healthcare.Provider@albertahealthservices.ca
CC: 
BCC: 
Subject: Re: Verification of email address - [private]
Attachments: [Browse, Upload]

First: John
Last: Doe
PHN: 99999999999999

-------Original Message-------
From: Your.Healthcare.Provider@albertahealthservices.ca
Sent: 02 Dec 2012 11:48
To: You.AtHome@YourProvider.com
Subject: Verification of email address - [private]

To verify that this email address belongs to the intended individual, please provide the following information about the patient in your reply: First and last name, and Personal Health Number (PHN).
Does your patient have to register and activate their account every time?

- The next time you send a secure email your patient does not have to register and confirm their account again.
- The patient will receive an email similar to the one in Step 8. By clicking on the “htm” link a browser will open and they will need to log in with their password that they created at time of registration.

Can emails be forwarded that are accessed on the encrypted service?

- Yes emails can be forwarded to any email account.
- The information will continue to be encrypted, so the person this information is sent to will have to follow the same process to register and activate their email address to view the message.
- This is the patient’s personal identifiable health information so it is up to them what they do with it; however they should be aware that private information of this nature can be misused.

So once the email account has been verified to be the correct one, what happens next?

- Once you have verified the patient’s email account to be the correct one belonging to your patient, this account can now be used for you to send your patient the agreed upon personal identifiable health information.
- Likewise your patient can use the secure server to send encrypted emails to you or other health care provider. Make sure to agree with the patient that you are ok with the patient communicating this way. You may prefer to phone or send regular mail to receive information from your patient.

What does a typical email from you the health care provider look like?

- The initial verification of account email example is given in step 14.
- Typically a health care provider will not put identifiable information in the subject line. Example: "Confidential - Communication from AHS! Private" or "Confidential - Communication from AHS cardiac rehabilitation clinic"
- NB as stated before the subject line may still identify the patient (see previous examples)

    **Example:** example of a typical header of an email

```
From: Your.HealthCareProvider@albertahealthservices.ca
To: You.AtHome@yourprovider.com
Date: Monday 2012-12-03 13:06
Subject: Confidential - Communication from AHS! Private
```
• Each email and attachment must positively identify the patient. We need to be absolutely sure that the personal identifiable health information is about the patient and for the patient.
• At a minimum it must contain first name, last name and PHN. (#1)
• Please make sure that the information is correct and is indeed intended for the patient.
• The body of the email will have the message of the health care provider to the patient.
• It will usually also prompt the patient to reply to confirm that the patient received the email and attachments. (#2)
• The signature block should contain your name (the health care provider) as well as credentials, title, department name, address and contact numbers, as well as the words “Alberta health Services” and the Alberta Health Services Website address. (#3)

• **Example**: example of a typical body of an email

This message is addressed to the recipient only:
John Doe
PHN 9999999999999

Dear Mr. Doe,

Find attached the exercises that we have discussed at your last clinic visit.

Please confirm that you have read and understood this email with # attachment(s) by sending a reply indicating “read and understood with # attachments” #2

“*Never use email in an emergency. Call 911 or call HealthLink Alberta 811*”

______________________________
Your HealthCare Provider
Speech Language Pathologist
Our Program Services
Health Care Centre

67 The Address
City, AB
Your.Healthcare.Provider@albertahealthservices.ca

403-000-00000

Alberta Health Services
www.albertahealthservices.ca

This message and any attached documents are only for the use of the intended recipient(s), are confidential and may contain privileged information. Any unauthorized review, use, retransmission, or other disclosure is strictly prohibited. If you have received this message in error, please notify the sender immediately, and then delete the original message. Thank you.
Procedure – Emailing Health Information

Transmission of Health Information by Email

AHS representative wishes to send an email

Email contains Health Information?
- Yes → Refer to Policy #1142
- No → Not covered by this procedure
  → Refer to Policy #1113

Originates from email address approved by AHS?
- Yes → Get authorization from Information Risk Management
- No → Not covered by this procedure
  → Refer to Policy #1113

Target location of the email is ...
- INTERNAL → No encryption needed
  → Refer to Policy #1113
- EXTERNAL → Use encryption
  → Refer to InSite for the process

... If...
- ... sent to the wrong recipient?
  - Yes → Contact recipient to delete email
    → Record corrective action
    → Immediately report event to AHS Information & Privacy Department as a potential Privacy Breach. Use form (#09579)
  - No → Document (add) any pertinent information on the Health Record
    → Purge email content from email account
AHS Emailing Personal Identifiable Health Information
Leading Practice User Guide

Appendix E

REQUIREMENTS - FLOW

Procedure – Emailing Health Information
Requirements for Emails containing Health Information

AHS representative wishes to send an email containing Health Information

- Consider other means of providing health information first (2.2)
- Obtain permission of the recipient, and only send least amount (2.3)

Requirements for: Subject Line (2.4)

- Provide general detail regarding purpose
- No Identifiable health information

Requirements for: Body of email (2.4)

- Can contain health information
- Attachments can contain health information
- Attach a signature block (2.5)
- Remain on topic (2.6)
- Only information from the intended patient (2.6)
- Ensure that recipient has received and read email ... (if the email contains important or time sensitive information) (2.7)

Email to patient [alternate decision maker] (3.1)

- Obtain permission to send health information by email (3.3)
- Document the permission in the health record (3.3)
- You must have an existing professional relationship with patient (3.2)
- Make patient aware of benefits & risks (3.4)
- Inform patient that email cannot be used in emergencies (3.4)
- Email does not replace in-person consultation need (3.9)
- Refusal to communicate by email cannot affect care (3.5)
- Acceptable use (3.6)
  - Administrative activities
  - Education and health promotion
  - Patient care information that can be reasonably shared indirectly
  - Research purposes (Policy #1146)
  - Verify patient’s identity by sending a verification email (3.7)

Email to other internal or external health care provider

- Obtain permission to send health information by email (5.1)
- Orders cannot be transmitted by email to health care providers (5.2)
- Exception: Hand-signed, scanned medication orders may be transmitted to an internal email account (5.3)

Documenting (adding/recording) of emailed Health Information (4)

- Record, store, manage and dispose according to records management policy & procedure (6.1) / (Policy #133; Procedure #133-01)
- Print and file on the health record relevant emails/attachments (6.2)
- Transcribe relevant information as a narrative if email contains non-relevant passages or sever the printed copy (6.3)
- Do not file transitory records in the health record (6.3)
- Purge/delete email containing health information from the email account once added to the health record (6.4)

Access & Disclosure (4)

- Requests for access to health information to be sent by email need to follow policy (4.1) / (Policy #1112)
- Email communication with patient must follow policy (4.1) / (Policy #1112)