Clinical Email

Bottom Line

As tempting as it is to send clinical queries via email, this can be risky. Alberta Health services (AHS) provides clinicians with tools for secure transmission of clinical information via email, including encrypted email to external addresses. However, security has more to do with understanding and behavior than tools or technology. This guide highlights knowledge and skills that clinicians should master.

Recognize and Protect Clinical Communications

Transitory communications (e.g. request to meet) do not require secure transmission if they do not contain information that might identify a patient. Non-transitory clinical communications about individuals and the care they receive (e.g., clinical images) must be protected and may need to be referenced in the clinical information system (CIS).

Obtain Consent

If sensitive communications will be regularly sent to a particular recipient (e.g., patient, billing service, referring clinician), solicit, obtain and record the recipient's consent to use a particular communication technology in support of patient care.

Use the most Integrated and Secure Clinical Communication Option

Within-CIS Messaging - Always use messaging solutions within the Connect Care CIS when sender and recipient both have access. This includes clinicians who do not use Connect Care as the record of care but have access to the Provider Portal. If necessary, alert the recipient via email or instant messaging that they have a CIS message awaiting attention.

Via CIS Portals – When available, use Connect Care patient or provider portals.

AHS Secure E-Mail

- If both sender and receiver have AHS email addresses (@albertahealthservices.ca or @ahs.ca or @covenanthealth.ca or @albertapubliclabs.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 Approved Solution - If none of the above are appropriate for clinical communications, consider use of an external clinical secure messaging solution that meets Health Information Act requirements.

Recognize risk

Use of any email system, even encrypted AHS email, increases the risk that the message goes to an unintended recipient (addressing error), is viewed by the wrong recipient, is not accessed in a timely manner, is altered or falsified, bears a virus or malware, is inappropriately copied, is inappropriately forwarded or fails to surface in the clinical and/or legal record of care. General communications vigilance is essential even with secure (encrypted) email.

Guides

- InfoCare: Email Encryption and Decryption Instructions

Policies

- AHS Transmission of Information by Facsimile and Electronic Mail Policy
- AHS Emailing Personal Identifiable Health Information Procedure
- Emailing Personal Identifiable Health Information Leading Practice User Guide
- AHS Collection, Access, Use and Disclosure of Information Policy
- AHS Transitory Records Procedure