Clinical Secure Messaging

Bottom Line

Instant messaging refers to person-to-person communication tools optimized for short chat-like exchanges. Clinical Secure Messaging (CSM) adds encryption and user-validation for secure transmission of personal health information. This guide defines practices and conditions for safe use of CSM in conjunction with Alberta Health Services (AHS) facilities and records.

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. Non-transitory clinical communications about individuals and the care they receive (e.g., clinical images, consult requests) must be reproduced or referenced within the record of care (CIS or paper).
Obtain Consent	Solicit, obtain and record the message 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. Via CIS Portals – When available, use CIS-tethered patient or provider portals. 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 prior to transfer to and receipt by the receiver. If the receiver has an AHS email address but the sender does not, do not use AHS email for secure clinical communications. AHS secure email can be used on mobile devices and can transfer documents, images or other clinical evidence. External Approved CSM Solution - If none of the above are appropriate for clinical communications, consider use of an external CSM solution that meets Health Information Act requirements, with a CSM-specific addendum to the CIS Privacy Impact Assessment (PIA) accepted by the Office of the Information and Privacy Commissioner of Alberta (OIPC). Reference or copy to an appropriate CIS encounter, heeding Clinical Copy-Paste guides.
Manage Attachments	Extract any documents or images (e.g. consultation letter) and follow guides for selecting and attaching material to an appropriate CIS encounter.
Recognize risk	Use of any non-AHS sanctioned and tested system for confidential clinical communications, including texting/chat/messaging/email, 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.

Objectives

The intent of this guide is to provide direction for Alberta Health Services (AHS) Clinical Information System (CIS) users about appropriate use of Clinical Secure Messaging (CSM) applications in conjunction with digital health records applications; including all AHS CISs (see definitions).

Background

Instant messaging (IM) refers to a class of person-to-person communications applications optimized for exchange of text, and possibly documents or images, as might support an informal clinical 'chat'. Just as IM replaces many verbal communications outside of healthcare, many healthcare providers use IM tools on personal devices to supplement every day in-person or telephone conversations.

CSM extends instant messaging with sufficient encryption and user-validation protections to satisfy requirements for transmission of personal health information from one authenticated user to another in support of the provision of health care services. CSM stores messages on a secured server, avoiding use of electronic mail relay and storage technologies. CSM is further designed to handle sender/recipient identification, consent-to-share, message receipts, message alerts, non-repudiation, encryption, tracking, auditing, archive and other functions required or implied by legislation for electronic transmission of identifiable health information.

CSM can offer a simple way for clinicians to exchange encrypted messages over the Internet, irrespective of the users' computer, network, browser or digital health record context. Popularized by straightforward user interfaces on mobile devices, CSM is positioned as a convenient replacement for paging, telephone calls or conventional email. Like telephone and paging, but unlike email, CSM alerts the user to incoming messages with tactile or auditory cues that persist until the message is acknowledged. Many workplace communications (e.g., call to rounds, request for consult, activity announcements, or test result alerts) fit CSM better than either paging or email.

Appropriately configured, deployed and integrated, CSM can serve clinical communication, consultation and care coordination needs within or without a Digital Health Record (DHR, such as Electronic Medical Record [EMR] or Clinical Information System [CIS]; see definitions). Many transitory communications (e.g., location of patient care rounds) do not belong in DHRs. Other non-transitory communications (e.g. actionable response to a question about patient care) merit inclusion in a DHR as the clinical and/or legal record of care.

AHS presently offers full-function, standards-based, CSM as part of the Connect Care CIS offering. This includes secure messaging to patients through MyAHS Connect and to other providers through the Connect Care Link provider portal. As the CIS extends province-wide, AHS hopes that other standards-based offerings will interface with Connect Care messaging.

AHS also offers an add-on encryption tool (Trend-Micro) for its enterprise-wide Microsoft Exchange secure electronic mail service. This allows AHS staff and affiliates to encrypt e-mail communications outgoing to non-AHS recipients. However, there is no provision for incoming secure email from outside AHS, as might replace facsimile technology, outside of existing e-referral services.

Significance

The familiarity, simplicity, convenience and availability of instant messaging makes the associated technologies extraordinarily attractive to healthcare practitioners and trainees.

All smartphones and tablets come with instant messaging. Diverse mobile messaging apps are available for installation. Some, like "WhatsApp," purport to be "zero-footprint" with no enduring storage anywhere, further implying that use for clinical purposes could not be discovered. Finally, a variety of clinical CSM apps are emerging as commercial service offerings for clinicians; with various claims to encryption, clinical ease and legislation-compliant testing.

Growing frustration with facsimile technology increases demand for services that fit modern communication expectations. Many newer clinicians, including trainees, rarely use email.

Scope

- This guide should be followed by all clinicians who see patients in facilities where an AHS CIS is deployed. Clinicians may directly comply with CIS CSM guides; or ensure compliance with the help of other members of the health care team.

- Adherence to this guide should be supported by all authorized clinical administrators, managers, support staff, billing clerks, scheduling clerks and transcription staff who assist clinicians subject to the guide and may need to be aware of or support information transfers to or from non-AHS CSM solutions.

Best Practices

This CSM guide draws upon clinical documentation, privacy, information management and other AHS policies and procedures essential for safe health care communication and collaboration. The guides below emphasize best practices in a CIS context. They should be followed in the spirit of assuring safe, high quality care that does not unfairly increase documentation burdens or risks for other clinicians caring for the same patient in a shared digital health record.

Dependencies

This guide contemplates possible transfer of CIS-relevant communication transcripts from a CSM solution to or from an AHS-provisioned CIS. Given lack of integration between third-party CSM solutions and AHS CIS solutions, such transfers require manual copy-paste processes described in a Clinical Copy-Paste Guide. Other guides, policies and procedures also apply, including secure email, facsimile, mobile device and legal record of care policies.

Principles

- Recognize and specifically protect clinical communications.
    - Transitory communications about work processes (e.g. request to meet, alert to call someone, etc.) do not require the protections described in this guide if they do not contain information that might identify a specific patient and do not involve substantive clinical discourse not already in the clinical and legal record of care.
    - Non-transitory clinical communications about individuals and the care they receive need to be referenced, inserted or attached within the record of care, which may be an AHS CIS. It may be CIS-appropriate to simply refer to the existence of an e-communication and any conclusions drawn, as one might refer to the content of a telephone conversation.
    - Consider Instant Messaging for transitory, non-patient specific, communications
        - Use of smartphone or tablet instant messaging is acceptable if messages do not include individually identifiable confidential health information.
        - Follow AHS policies, procedures and guides about use of mobile technology, including provisions for encryption, strong passcode protection and remote-wipe-reset capabilities.
- Use the most secure and integrated CSM tool available within a particular clinical context, with preference, in declining order, for:
    - Within-CIS Messaging

- Always use messaging solutions offered within a particular CIS when both sender and recipient have access to the same CIS.
- Use of CIS-based communication tools does not expose users to potentially insecure information transfer or to the risks of copy-paste operations between systems.
- CIS messaging takes care of encounter-linking, attachment integrity and all required archiving.
- It is acceptable to use within-CIS communication tools for communications about process (e.g. clinical meetings), in addition to patient-specific communications.
- Advocate for release of CIS mobile applications, which increase the convenience of within-CIS communications.
- If concerned about possible poor recipient CIS in-basket awareness, consider an instant message (e.g. SMS) to the recipient; to the effect that there is a secure clinical communication awaiting their attention in the CIS.

- AHS Secure E-Mail
  - If neither of the above are available or appropriate, next prefer use of AHS email.
  - 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 follow the AHS secure e-mail guide and place the word “!Private” in the subject line. This will cause the outgoing email message to be encrypted using the Trend-Micro add-on.
  - If the receiver has an AHS email address but the sender does not, then do not use AHS email for secure clinical communications.
  - While AHS email services are archived, the duration of archiving may not meet medical record retention requirements. I
  - t is always necessary to reference any clinically important communication about a patient in that patient’s medical record. It may be sufficient to indicate within a CIS that a communication occurred via secure email, but a summary of what was asked or discovered should be recorded in the CIS; not unlike how a clinician would record the essence of an important telephone exchange about patient care.
  - As with other CSM options, the recipient may not check AHS email frequently enough. Consider use of instant messaging (e.g. SMS) to alert the recipient that an AHS email awaits attention.
- External OIPC-Approved CSM Solution
  - If none of the above are available or appropriate, consider use of an external CSM solution if it meets the functional characteristics described in this guide and has been subjected to Health Information Act compliance assessment.
  - That an external CSM solution was used should be indicated in the CIS, with reference to the nature of the communication and any clinically important outcome.

- Clinical communications archived outside of the CIS, as might occur within an external CSM solution, must be referenced, copied or attached to the CIS if the clinical communication is non-transitory and required for inclusion in the record of care.
- Use an appropriate communications transcript feature to extract a specific communication "thread" (series of messages about the same patient and question) for copy-paste to an appropriate communications encounter (e.g. "Telephone encounter") within the CIS; heeding Clinical Copy-Paste guides.

- Obtain and document recipient consent for secure communications.
  - Before adopting any of the above approaches to clinical communication, be sure to seek, obtain and record permission of the recipient(s); especially for use of any non-CIS CSM tool.
  - External CSM solutions must include a recipient user permission confirmation function; and this must be engaged before first communicating with a particular external CSM user.
  - Even if a recipient has indicated willingness to receive clinical communications via a particular CSM technology, consider using regular email or instant messaging to alert the recipient that something awaits their attention in the preferred CSM solution.
- Appropriately manage any documents, files or images attached to secure communications.
  - Attachments (e.g. letters, test results, reports) should be extracted from the secure communications transcript and attached to an appropriate CIS encounter record.
  - Follow CIS attachment selection, naming and management guides for a particular CIS.

Responsibilities

- Health care providers are responsible for ensuring the quality and accuracy of health information documented under their control, whether or not it is original CIS content or information transferred from an email or CSM transcript.
- Health care providers are also responsible for protecting the privacy and security of health information.
- The health care provider is responsible for ensuring that the meaning and purpose of CSM transcripts are correct, relevant to the current encounter, not redundant and credited to the participating clinicians.
- If CSM to CSM or CSM to CIS transfers result in a privacy breach, the breach is to be reported immediately to AHS Information & Privacy. (See AHS Information Security & Privacy Safeguards Policy).
- When health information errors are discovered in a CSM transcript after transfer to a CIS, the error should be noted in the CIS and participating clinicians should be alerted to the error(s).
- Any information transfer involving an AHS CIS should only involve non-AHS CSM products if the proposed technologies and uses have been subjected to an AHS Privacy Impact Assessment (PIA). A CSM PIA addendum needs to be linked to the AHS CIS PIA and this addendum must be reviewed and accepted by the Office of the Information and Privacy Commissioner of Alberta (OIPC).
- Use of non-approved CSM products or untested CSM to CIS transfer processes exposes the user to full accountability and responsibility for information sharing and any possible misadventure

during or after the information transfer; 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.

- The conditions for use of CSM services in conjunction with CIS solutions shall be reviewed by, validated and enforced by AHS Privacy and the clinical governance committees of affected CISs.
- The above principles, plus any CSM guides, should be included in CIS-specific training, handbook(s), user manuals, orientation and competency-based access.
- The existence, methods and meaning of application-to-application information exchange on organizational and personal computing devices shall be addressed in privacy instruction for all students, trainees, affiliates, staff, and employees.

Use Cases

The following examples illustrate specific clinical situations and the CSM tools that may be appropriate to each at this time. The appropriate uses will change as physician portal access opens up on some AHS CISs and will change completely when a Provincial AHS CIS solution is deployed.

Need	Context	Clinical Secure Messaging
Ambulatory Care Physicians need to securely transfer billings lists, transcripts, or other materials to and from clinical support staff.	Specialist ambulatory care services are provided using a 'hybrid' business model in many parts of the province. AHS may provide clinic facilities, infrastructure and clinical information systems. Physicians may have a primary affiliation with an alternate payment relationship, an academic group (university), private clinic or be working semi-independently. Clinical support staff may be non-AHS employees, without entitlement to AHS clinical email.	× Clinical support staff may have access to an AHS CIS for scheduling or communication purposes but no current CIS supports attachments for staff messages. × Lacking AHS email accounts, or entitlement to the same, clinical support staff can receive an encrypted email from a physician with an AHS account but cannot send materials in return. ✓ Until an AHS Provincial CIS is in play, the only alternatives for CSM are external solutions or possibly efforts to gain AHS email access for clinical support staff.
AHS hospitalists wishing to send discharge summaries, consults or other clinical materials securely to community-based physicians where fax is inconvenient, not available or inappropriate.	The AHS affiliate physicians have AHS email accounts, and access to an AHS. The inpatient physicians are able to use email and know the email address of the recipient community physician who has indicated willingness and consent to use email for this purpose.	× The receiving physician does not have CIS access, and outgoing CIS fax services are not available; CIS is not currently workable solution. ✓ The physician could send the attachment as a secure email from an AHS email address to a non-AHS address (using "!Private" in the subject line) if the receiving physician has indicated willingness and consent to use email for this purpose.
Community physicians who regularly refer to or collaborate with a group of specialist or inpatient physicians or service, wish to replace fax with CSM for making	The community physicians does not have CIS access or CIS physician portal access. The receiving physicians have CIS, as well as AHS email accounts.	× A CIS physician portal might work well but is not currently available. × AHS secure email does not currently provide a method for persons without AHS email accounts to send materials securely to AHS email accounts.

Need	Context	Clinical Secure Messaging
referrals and forwarding relevant clinical documents.		✓ An external approved CSM may be the only option currently able to address this need and a use case should be submitted.
Provider to provide exchange of clinical images	Clinical trainees wish to take pictures of physical findings using mobile devices and send these to members of the inpatient healthcare team for review. There is no CIS available for inpatient use.	× Were an inpatient CIS available with full CSM activated, it would be the tool of choice for this kind of information exchange, especially since the attachments constitute sensitive information that should have the full benefit of a secured and audited information sharing environment. ✓ AHS email is available to all trainees and all members of the inpatient health care team. This includes consultants and attending physicians. Secure messages can be exchanged and attachments (images) are supported. Key considerations are whether the patient consents to the acquisition and use of clinical images. The images may merit inclusion in the legal record of care, with logistical challenges printing and incorporating into a non-digital health record.

Definitions

[see glossary.connect-care.ca]

- **Breach**
  Failure to observe security or privacy processes, procedures or policies, whether deliberate or accidental, which results in health information being viewed, or having the potential to be accessed, used, transmitted, or held by unauthorized persons.
- **Clinical Secure Messaging**
  Instant messaging refers to a group of, usually informal, person-to-person communications applications optimized for exchange of short text, and possibly attachments, as might support a 'chat'. Clinical secure messaging extends instant messaging with sufficient encryption and user-validation protections to satisfy requirements for secure transmission of communications from one authenticated user to another in support of health care services. CSM stores messages on a secure server, avoiding electronic mail relay and storage technologies. CSM is further distinguished by its ability to handle sender/recipient identification, consent-to-share, message receipts, message alerts, non-repudiation, encryption, tracking, auditing, archive and other functions required or implied by legislation for electronic transmission of identifiable health information.
- **Copy-Paste**
  Duplicating selected digital or digitalized information (data, text and/or hidden meta-data or data properties) and inserting it in another location without changing, or minimally changing, the original source. Within the context of this guideline, it means the process of copying and pasting existing clinical information from a source and pasting it in a destination within the same or different digital health record, software or information system.

- **Destination**
  Location where information is pasted or where the information needs to go.
- **Encounter**
  Contact between a patient and a practitioner who has primary responsibility for assessing and treating the patient at a given contact, and exercising independent judgment.
- **External Email Account**
  Any electronic mail address (account) that is not an AHS email address (account; @ahs.ca, @albertahealthservices.ca).
- **Health Care Provider**
  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, in affiliation with, or in conjunction with Alberta Health Services.
- **Health Information**
  Confidential health information is, for the purposes of this guide, identifies an individual and is stored in any format that relates to the provision of health services, including diagnosis, treatment and care; or registration (e.g., demographics, residency, health services eligibility, or billing). *Personal identifiable health information* is, for the purposes of this guide, the same as confidential health information.
- **Health Record**
  For the purposes of this guide, the health record is any AHS medical record of health services (diagnostic, treatment, care, etc.) provided to a patient by any health care provider or provider team.
- **Internal Email Account**
  Any electronic mail address (account) that is an AHS email address (account; @ahs.ca, @albertahealthservices.ca).
- **Non-transitory Record**
  (see Transitory Record) Any file, transcript, image or other record in any form/media that uniquely documents actual patient care, clinical decisions, actions taken, interventions or outcomes that must appear in the clinical or legal record of care for legislative, organizational, or professional reasons; or which have unique research or archival value to AHS or the healthcare provider. Examples include: consultation requests, answers to clinical questions, digital photographs of clinical findings (not elsewhere recorded), clinical evidence attached to referral requests, case conference transcripts (including telehealth and telephone), refill requests and orders, etc.
- **Patient**
  All persons who receive or who request health care or services from or in conjunction with AHS and its health care providers or affiliates, irrespective of the context (inpatient, outpatient, community, etc.) where services are provided.
- **Source**
  Software and location from which information is transferred.
- **Transitory Record**
  Any document, file, transcript, image or other record in any form/media that:
  - has no clinical value or use beyond an immediate and minor transaction;
  - is only required for a short time during and not usually after the transaction;
  - is made obsolete by an updated version of the record, subsequent transaction or decision;

- is a duplicate or copy of a record elsewhere recording in the clinical or legal record of care;
- is a work-in-progress or non-committed draft record that will have no value once the final record is produced.
- Examples include: announcement of the time and place of a patient conference; reminder to see a patient in the emergency room; indication of the location of a patient or intervention; list of patients to be seen by a clinical team; etc.
- Transitory records do not document actual patient care, clinical decisions, actions taken, interventions or outcomes. They do not provide unique evidence of health services actions that must be documented for legislative, organizational or professional reasons and have no unique research or archival value to AHS or the healthcare provider.

- **Transmission**
  Sending of information (including any documents, files or images) using electronic means (e.g., facsimile, email, secure clinical messaging, instant messaging, paging, etc.).

Resources

- AHS Collection, Access, Use and Disclosure of Information Policy
- AHS Transitory Records Procedure
- 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