

**AR0500 – EMAIL & TEXT MESSAGING**

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dākelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tšilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

**1.0 PURPOSE**

To protect personal information from risks such as unauthorized collection, use or disclosure as required by the British Columbia Freedom of Information and Protection of Privacy Act (FIPPA).

To ensure reasonable safeguards are utilized to mitigate the risks associated with the use of Interior Health (IH) Email or Text Messaging for the exchange of Confidential Information including Personal Information.

**2.0 DEFINITIONS**

TERM	DEFINITION
<i>Clients</i>	<i>Patients and persons in care in IH facilities and programs.</i>
<i>Confidential Information</i>	<p><i>Whether oral, written, electronic or film, includes the following:</i></p> <ul style="list-style-type: none"> <li><i>a) Personal Information (see also definition below).</i></li> <li><i>b) Business information collected or created by Interior Health that exists regardless of form and includes, but is not limited to:</i> <ul style="list-style-type: none"> <li><i>• Information provided to Interior Health by an external vendor or service provider which, if disclosed, would harm the business interests of the third party;</i></li> <li><i>• Financial information provided by Clients and Users including but not limited to bank account information, Social Insurance Number (SIN),</i></li> </ul> </li> </ul>

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	1 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

	<p><i>credit card information, and Canada Revenue Agency (CRA) account information;</i></p> <ul style="list-style-type: none"> <li>• <i>Information prepared as part of pending or ongoing litigation, law enforcement investigation, quality assurance review, Workers Compensation Board or Ombudsman investigation;</i></li> <li>• <i>Information related to credentialing, discipline, privilege, quality assurance reviews and external review of quality of care;</i></li> <li>• <i>In-camera deliberations of Interior Health where such topics as budget strategies, personnel, labor relations, land acquisitions or litigation may be discussed;</i></li> <li>• <i>Unpublished statistical information and internal correspondence related to organizational initiatives; and</i></li> <li>• <i>Information supplied in confidence to a mediator or arbitrator to resolve or investigate a labor relations dispute.</i></li> </ul> <p>c) <i>All information that, if disclosed without authorization, could be prejudicial to the interests of Interior Health and associated individuals or agencies; and</i></p> <p>d) <i>Organizational business information that would harm Interior Health's financial interests and/or information that relates to the management of Interior Health that has not yet been implemented or made public; such as information that identifies the security architecture and infrastructure of the organizations' information systems.</i></p>
<p><i>Email</i></p>	<p><i>An electronically created mail message sent and received over electronic communication systems. Attachments to emails are considered part of the email.</i></p> <p><i>Email is a form of communication similar to facsimile (fax), phone calls, and Text Messages and are considered short-term and Transitory. Any Emails with content that must be retained (e.g. Email documenting a policy decision,</i></p>

<p>Policy Sponsor &amp; Chief Financial Officer (CFO) &amp; VP, Corporate Services</p>	<p>2 of 15</p>
<p>Policy Steward: Manager, Information Privacy and Freedom of Information</p>	
<p>Date Approved: February 2003</p>	<p>Date(s) Reviewed(r)/Revised(R): April 2024 (R)</p>
<p><b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b></p>	

**AR0500 – EMAIL & TEXT MESSAGING**

	<i>discussion that led to a decision for a Client's care, etc.) must be retained in the appropriate record keeping system (e.g. Meditech). Documentation in the appropriate record keeping system must be in accordance with, but not limited to documentation best practices, College standards, and <a href="#">IH Clinical Documentation Standards</a>.</i>
<i>Encryption</i>	<i>The process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.</i>
<i>Instant Messaging</i>	<i>Instant Messaging is a type of online messaging over the internet and not reliant on a telecommunication provider cellular phone service (e.g. MS Teams, Signal, Slack).  Instant Messaging is outside the scope of this Policy. Interior Health Users have access to <a href="#">Microblogging MD</a> which is IH's secure Instant Messaging and notification application for clinical use.</i>
<i>Offensive Material</i>	<i>Includes, but is not limited to, pornography, hate literature or any material which contravenes the BC Human Rights Act.</i>
<i>Personal Information</i>	<i>Personal Information includes any information which may be associated with or identifies an individual except business contact information. Personally identifiable information includes things such as a person's name, social insurance number, account number, health care number, employment history or medical information.  Personal information does not include business contact information, such as a person's title, business telephone number, business address, email or facsimile number. References to "personal information" within this policy apply to any documents or records (whether in hard copy or electronic form) on which personal information is recorded and all verbal comments or conversations in which personal information is mentioned or discussed.</i>
<i>Sensitive Information</i>	<i>Sensitive Information may include Confidential, Personal or health information that would be most appropriately delivered in person or protected using additional controls such as Encryption. Unauthorized disclosure of sensitive information such as Personal Health Number (PHN) or a</i>

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	3 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

	<i>sensitive health service may cause significant mental or physical harm to the individual.</i>
<i>Text, Text Message, or Text Messaging</i>	<p>Also called SMS (Short Message Service), and allows short text messages to be sent and received on a mobile phone. Text messaging is inherently unsecure. Messages can be forwarded to anyone, remain unencrypted on telecommunication providers' servers, and reside on a mobile device indefinitely. Wireless carriers may encrypt text messages, but interception and decryption are risks associated with text messaging.</p> <p>Text Messaging is a form of communication similar to facsimile (fax), phone calls, and Email and are considered short-term and Transitory. Any Text Messages with content that must be retained (e.g. documenting a policy decision, discussion that led to a decision for a Client's care, etc.) must be retained in the appropriate record keeping system (e.g. Meditech). Documentation in the appropriate record keeping system must be in accordance with, but not limited to documentation best practices, College standards, and <a href="#">IH Clinical Documentation Standards</a>.</p>
<i>Threat</i>	<i>For the purposes of this policy, a threat refers to all types of malware that are annoyance or malicious software designed to intentionally compromise computer systems and networks.</i>
<i>Transitory Information</i>	<p>A record of temporary usefulness needed only for a limited time in order to complete a routine action or to prepare an ongoing record that does not reflect the functions, business activities, and decisions of IH and/or is not an integral part of a Business Record or a Patient record.</p> <p>Common categories and examples of Transitory information can be found in Appendix B of <a href="#">AL0700: Retention, Storage, and Destruction of Records</a>.</p>
<i>Trusted Institution</i>	<i>For purposes of this Policy, a Trusted Institution is an organization who is covered under FIPPA in the province of B.C. who have reasonable security arrangements in place to protect IH data. Trusted Institutions include government ministries, provincial agencies, self-governing professional bodies (e.g. College of Physicians and Surgeons of B.C.), and universities within B.C. (e.g.</i>

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	4 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

	<p>University of British Columbia).</p> <p>Trusted Institutions do not include organizations outside of Canada.</p> <p>Consult with Information Privacy if you are unsure if an organization is considered a Trusted Institution.</p>
User	<p>Includes all employees, medical staff, independent contractors, students, volunteers, and any other persons acting on behalf of IH.</p>

**3.0 POLICY**

IH Users may use Email and Text Messaging for conducting both clinical and corporate activities and communications in accordance with this policy.

- All Email, Text Messages and associated information system resources are the property of IH.
- Emails and Text Messages are records (see [AL0700 Retention, Storage, and Destruction of Records](#)) and as such management of these records must comply with existing legislation, regulations, policies, and standards.
- Email and Text Messaging is provided to users primarily for business purposes. Use of Email and Text Messaging and its contents are subject to audit and Freedom of Information (FOI) Requests.

**3.1 Use of Email**

- [Email etiquette](#) and [best practices](#) should be followed at all times.
- Transmission of Confidential Information external to the IH Email system must be encrypted when it is Sensitive Information. *Exception: Email may be sent between Interior Health and the other B.C. Health Authorities securely without encryption.*
- Business communications between IH Users must be conducted using IH Email accounts. Exceptions may apply where a User’s personal email may be used for human resources related matters such as for initial recruitment and onboarding, health and wellness checks, etc.
- Email must not be used for:
  - Commercial solicitation or for conducting or pursuing personal business interests or those of another organization;
  - Distribution of hoaxes, viruses, malware, advertisements, Offensive Material, or harassing messages; nor

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	5 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<p><b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b></p>	



**AR0500 – EMAIL & TEXT MESSAGING**

- o Subscriptions to non-work related services.
- Email with Sensitive Information between IH Users and health care providers (includes internal and external care providers or other partners in care delivery for direct care purposes) must be conducted under the following conditions:
  - o Email from IH Users are only sent using their IH Email account; and
  - o Recipient health care provider Email accounts must be issued by Interior Health, another B.C. Health Authority, or a Trusted Institution. Personal accounts which store Sensitive Information outside Canada (e.g. @shaw, @gmail, etc.) must not be used for business purposes with other health care providers unless the Sensitive Information is encrypted (e.g. in a password protected and encrypted file) and the external email is strictly for business purposes (e.g. registered with the College, issued by the practice’s IT department, etc.).
  - o Any exception to the above must be in consultation with the Information Privacy and/or Information Security Offices to ensure appropriate controls are in place to mitigate any privacy and/or security risks.
- Email between IH Users and Clients is permitted under the following stringent conditions:
  - o Email from IH Users are only sent using their IH Email account.
  - o IH users involved in Email communication with a Client have reviewed the Email and Text Messaging Guidelines (Appendix A) and understand the restrictions and their responsibilities.
  - o The Notice of Risks (Appendix B) for Email and Text Message communication has been explained to the Client and verification of their Email address done prior to any Email communications.
  - o If there is a need to for IH to communicate Sensitive Information or health records via Email the information must be appropriately severed and/or encrypted.
  - o If there is a need for Clients to communicate Sensitive Information or health records via email to IH that the information be emailed only to the program’s generic IH Email account under the direct ownership of a minimum of one IH Manager/Director. Additionally, the information received must be deleted from the Email folders at the earliest possible time when no longer required.

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	6 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

**3.2 Use of Text Messaging**

- Text Messaging between IH Users and health care providers must be conducted under the following conditions:
  - Text Messages are sent only from an Interior Health-issued mobile phone; and
  - If deemed necessary that Confidential Information and/or Client identifiers be communicated through Text Messaging, **only the minimum amount of information** necessary to support the purpose be included.
- Text Messaging between an IH User and a Client is permitted under the following stringent conditions:
  - Text Messages are sent only from an Interior Health-issued mobile phone;
  - IH Users involved in Text Messaging communication with a Client have reviewed the Email and Text Messaging Guidelines (Appendix A) and understand the restrictions and their responsibilities.
  - The Notice of Risks (Appendix B) for Email and Text Message communication has been explained to the Client and verification of their mobile phone number is obtained prior to any text messaging communications; and
  - **Only the minimum amount of information** necessary to support the purpose be included in the Text Message.
- See Appendix A for examples of permitted Text Messaging Communications.

**3.3 Authenticating the Recipient**

Users must take appropriate measures to authenticate the identity of the intended Email or Text Message recipient prior to communicating Confidential Information.

Methods of authentication include, but is not limited to:

- Sending an initial Email or Text Message to confirm the right User or Client is being contacted before sending any Confidential Information;
- Confirming the correct Email address or telephone number in person or verbally over the phone before sending the Email or Text Message;
- When Emailing or Text Messaging with Clients, family members or representatives, asking the recipient to verify one of the Client’s birthdate,

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	7 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	





### AR0500 – EMAIL & TEXT MESSAGING

last 4 digits of PHN, or other piece of information that only the individual would know; and/or

- Providing your contact information to the Client and asking them to send the first Email or Text Message, ideally with a piece of information that only the individual would know and previously agreed upon providing.

#### 3.4 Personal Use

Although the IH computer system and IH issued mobile phones (as well as other mobile devices such as laptops and USB keys) are provided to Users for the primary purpose of business functions, a limited amount of personal use in accordance to [Policy AR0150 – Mobile Device Personal Use](#) is permitted.

The computer, mobile phones and other mobile computing devices, and all data contained on them including email, text messages, photos, etc. are the property of Interior Health, and as such are subject to auditing, monitoring, [Freedom of Information access requests](#) and may be disclosed as required by law (e.g. court order or reportable conditions) as well as internally to authorized IH staff).

#### 3.5 Use of Personal Devices, Personal Cloud, and Personal Accounts for Emailing and Text Messaging

- Personal computers (desktops and laptops) may be used to access the IH email system through IH Anywhere or IH Webmail technologies.
- Personal smart phones may be used for limited work purposes by Users to:
  - Access their IH email account using IH Webmail or directly from their smart phone once they submit a Smartphone Agreement via the [Access Management Portal](#).
  - Text Message to a co-worker or physician provided there is no communication of Confidential Information.
- Text messaging clients from personal smart phones is prohibited
- IH provides the necessary technology to conduct IH business. Users must not link personal cloud to IH Email and Text (e.g. Users must not back up IH Email and Text Messages to personal cloud storage).
- Personal Email accounts must not be used to conduct IH business.

#### 3.6 Compliance

Failure to comply with acceptable use standards will result in consequences that range from termination of access, employment and/or contract,

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	8 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i>	



**AR0500 – EMAIL & TEXT MESSAGING**

withdrawal of privileges in accordance with Medical Staff Bylaws, and/or professional sanctions.

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	9 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

**4.0 PROCEDURES**

**4.1 All Users will:**

- Include the standard IH email disclaimer as documented in the [Email Signature Guidelines](#) for all initial external email communications.
- Review the Email & Text Messaging Guidelines (Appendix A).
- Only Email or Text a Client after explaining and providing the Client a copy of the Notice of Risks for Clients (Appendix B) and verifying the Client’s Email and/or mobile phone number.
- Use their IH email account and/or IH issued mobile phone to communicate with a Client.
- Comply with this policy and ensure the type of Email and Text Messaging Communications are Permitted (Appendix A).

**4.2 Managers / Chief of Staff will:**

- Follow-up on compliance audits in consultation with Human Resources and/or Senior Medical Directors and take appropriate action when required.

**4.3 Digital Health will:**

- Ensure controls are in place to prevent threats from compromising the computer system.
- Conduct security audits as necessary.

**4.4 Information Privacy will:**

- Conduct privacy audits as necessary.

**5.0 REFERENCES**

1. [AF0100 – Transparency and Freedom Of Information](#)
2. [AL0700: Retention, Storage, and Destruction of Records](#)
3. [AR0100: Acceptable Use Policy](#)
4. [AR0150: Mobile Device Personal Use](#)
5. [AR0400: Privacy & Management of Confidential Information](#)
6. [AR0450: Managing Privacy & Security Breaches /Violations](#)
7. [AR0600: Internet Policy](#)

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	10 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i>	

**AR0500 – EMAIL & TEXT MESSAGING**

- 8. [AU0100: Standards of Conduct](#)
- 9. [Medical Bylaws](#)
- 10. [Guidelines: Emailing Personal Information](#)
- 11. [Email Etiquette](#)
- 12. [Email Signature Guidelines](#)
- 13. [Email Security and Confidentiality](#)

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	11 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<p><b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b></p>	

## AR0500 – EMAIL & TEXT MESSAGING

### APPENDIX A – Email & Text Messaging Guidelines

Email and Text Messaging has many advantages for Clients and Health Care Providers, including appointment reminders, increased accessibility, education and health promotion. However, the use of Email and Text Messaging to support Client care comes with inherent risks.

Email and Text Messaging are not secure, private, or confidential modes of information transmission. IH Users must follow the below noted precautionary measures to help mitigate the risks, as well as review and understand Interior Health policies/guidelines related to email and text messaging communication:

- [AR0400 - Privacy and Management of Confidential Information Policy](#)
- [Emailing Personal Information Best Practices](#)

### Conditions for Using Email and/or Text Messaging

- Email and Text Messaging Clients must only be conducted using IH Email and/or an IH issued mobile device.
- Email to identified health care providers must be to a secure Email account issued by Interior Health, another B.C. Health Authority, or a Trusted Institution (e.g. UBC). Personal email accounts must not be used for business (clinical and corporate) purposes with other health care providers.
- The Notice of Risks for Email and Text Message Communication (Appendix B) have been explained to the Client and verification of their Email address and/or mobile phone number has been done, and is noted in the permanent chart within the requesting department. Clients must be informed of the inherent risks to using Email and Text Messaging. Implied consent is assumed if, after knowing the risks, the Client provides their Email address and/or mobile phone number.
- If there is a need to communicate *sensitive information or health records via email the information must be appropriately severed as is needed*, (contact your local Health Records department for assistance) *and/or encrypted*. [7-Zip](#) is appropriate to create a self-extracting encrypted file with password protection.

### Permitted Email and Text Messages Communications Using IH Email Accounts and IH Devices

1. Responding to general inquiries for information about IH or its services.
2. Health Education or Promotional Purposes
  - Sharing health education resources that may be of interest to the Client

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	12 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

- Invitations to health promotion events

The above #1 and #2 do not typically require the transmission of Personal Information to provide general information.

3. Administrative Purposes

- Scheduling appointments
- Appointment reminders
- Providing location, hours of operations, or travel instructions

The above #3 may include Personal and limited Sensitive Information about a Client (e.g. reminder of an upcoming appointment). Information contained in Email and/or Text Messaging must be limited to need-to-know information and in compliance with section 3.1 and 3.2 of this Policy.

4. Communication with a Client that requires the transmission of Personal Information to that Client.

- Checking on a Client (e.g. Do you need anything? How are you doing?)
- Responding to a Client’s request for services

The above #4 involves transmission of Personal Information and must adhere to principles outlined in this Policy such as consent, identity verification, and encryption where information is Sensitive.

**Examples of Breaches or Violations to this Email and Text Messaging Policy**

1. Sending an IH business (clinical or corporate) email to a health care provider’s personal email.
2. Sending an email external to Interior Health (or other B.C. Health Authority or trusted organization) that contains Client or Confidential Information that is not encrypted.
3. Emailing and/or Text Messaging a Client without having informed them of the inherent risks as per the Notice of Risks (Appendix B).
4. Sending an Email that contains Client or Confidential information to a distribution group – not limiting distribution to individuals on a “need to know” basis.
5. Sending an email advertising merchandise, non-work related events or information that may be interpreted as a conflict of interest.

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	13 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

6. Emailing and/or Text Messaging the incorrect Client another Client's Confidential Information.
7. Disclosing other Client Email addresses and/or phone numbers in a mass Email (e.g. not using blind cc) or Text message.
8. Communicating financial information (e.g. credit card numbers) using Text Messaging.
9. Engaging in clinical discussion or counseling using Text Messaging.
10. Informing a Client or Family Member of a Client's diagnosis using Text Messaging.

Upon discovering or suspecting that a breach or violation has occurred, Users must contain and report the breach to their Manager and Information Privacy as outlined in Policy [ARO450: Managing Privacy & Security Breaches/Violations](#).

**The Bottom Line**

- Before engaging in Email or Text Messaging communications, staff must review Appendix A, relevant policies and understand the legal, privacy and security risks associated with Email and Text Messaging.
- Clients must be aware of risks of communicating by Email or Text messaging, and the limitations of its use by IH staff.
- Data on Interior Health computer systems (including Email) and mobile phones are subject to auditing, monitoring, Freedom of Information (FOI) Access requests and may be disclosed as required by law (e.g. court order or reportable conditions). This caution is especially pertinent during any FOI or litigation needs.

Policy Sponsor & Chief Financial Officer (CFO) & VP, Corporate Services	14 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed(r)/Revised(R): April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	

**AR0500 – EMAIL & TEXT MESSAGING**

**APPENDIX B – Email & Text Messaging - Notice of Risks for Clients**

In the course of providing your care, INTERIOR HEALTH (IH) is offering to communicate with you through Email and /or Text Messaging. Messaging sent by IH may include, but is not limited to, notifying you when you have been added to a wait list, providing contact information for your local booking office, scheduling appointments, and sending appointment reminders.

Your privacy is very important to us. IH is committed to make sure your personal health information remains safe and protected. It is important that you understand:

1. Getting your basic personal health information by email or text message may not always be secure. Your email/phone could be broken into and your personal health information could be seen or shared with others or changed without your permission. We recommend deleting communications that include personal health information from your email or phone to reduce the risk to you.
2. If you delete email or text messages from IH, backup copies could still be on your computer or on servers of your provider.
3. Depending on what company your cell phone or email plan is with (such as Gmail or Yahoo), information sent and /or received may be stored outside of Canada, and outside of IH's control.
4. Do not email or text IH if you have an emergency. If you have an emergency, call 911 or go to the closest emergency department.
5. IH Staff will not provide health advice by email or text. If you have questions about your health, please call or visit your specialist, family physician, hospital, or IH Clinic.
6. It is your responsibility to let us know if your email address or phone number changes. Please contact your local booking office at the number provided in the messages you receive.
7. It is your responsibility to tell IH if you change your mind and no longer want to get messages by email or text. The messages you receive will provide instructions on how to stop receiving electronic notifications from IH.

Policy Sponsor: VP & Chief Financial Officer	15 of 15
Policy Steward: Manager, Information Privacy and Freedom of Information	
Date Approved: February 2003	Date(s) Reviewed-r/Revised-R: April 2024 (R)
<b><i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i></b>	