Emailing Policy

1. Introduction

When used appropriately, email can be a valuable, fast, and convenient communication tool used to support Providence Health Care (PHC) business and activities.

1.1. Purpose

This policy provides guidance about acceptable use of email by staff and physicians in communicating with clients, patients, residents, family members, representatives, care providers and other staff.

1.2. Scope

This policy applies to all staff, including physicians, and is applicable to all personal information and confidential information transmitted through email, including through Outlook Web Access and mobile devices such as tablets and smart phones.

2. Policy

2.1. Email Use

Staff may use email for conducting both clinical and corporate activities in accordance with this policy.

Email is a record as defined under the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA) and, therefore, may be subject to disclosure under freedom of information requests (FOI).

Where available, staff must use a VCH or PHC email address to conduct VCH or PHC business. Email addresses issued by another health organization or trusted institution may also be used, based on where the staff member primarily works.

Email must not be used for the following, as per the Acceptable Use of Information Technology policy:

- Commercial solicitation.
- Distribution of offensive material or harassing messages.
- Subscriptions to non-work related services.

2.2. Authenticating the Recipient and Minimizing Amount of Personal Information

Email may be used to communicate personal and confidential information so long as staff take appropriate measures to reduce the related risks, including ensuring they have the correct recipient and minimizing the amount of personal information contained in each email message.

Authenticating the identity of intended email recipients is paramount. Ways of authenticating include:

- If you are sending the initial email: confirm the right person is being contacted before sending any personal or confidential information.
- If the client, patient or resident initiates the email: ask the sender to verify, by text or phone, their birthdate, personal health number (PHN) or other piece of information that only the individual would know.
- Confirm the correct email address in person or over the phone.

Authentication must be done on communication with any recipient who has not been previously authenticated. Subsequent email communications do not require recipient authentication. Until measures have been taken to authenticate the recipient's identity, staff must avoid emailing personal or confidential information.

Emails containing personal information about more than one individual (per message) should be done by capturing the information in an encrypted attachment, unless it is a small amount of personal information in total. Consider both the number of individuals it pertains to and the amount and sensitivity of personal information about each individual, e.g. less than 10 individuals with minimal health information about each individual. (see resources pertaining to encryption and password protection).

For transmitting large or more sensitive data sets e.g. for secondary use of health information such as quality improvement or research, email (even encrypted) should not be used. Consult with the PHC Information Access and Privacy Office for more secure and effective methods of transmission.

2.3. Emailing Care Providers and Other Staff for Care Purposes

Staff must follow the VCH/PHC Emailing Guidelines that accompany this policy.

Staff must not use personal email accounts such as Gmail, Yahoo, or Hotmail to send emails containing personal information when conducting PHC business.

2.4. Communicating the Risks of Emailing

Staff must communicate to clients, patients, residents, family members or representatives the common risks associated with email, including that:

- Email messages can include personal information, which will be at risk if an email account is compromised.
- Email should not be relied upon in urgent or emergency situations.
- Detailed clinical discussions, counseling or crisis-related support will not be provided by VCH or PHC staff or physicians through email.

Staff can inform recipients of these risks by providing them with a link to the information online at Emailing or Texting your Health Care Provider, or by printing and distributing the

information as a handout (see Appendix A: Notice Regarding Emailing or Texting your Health Care Provider.

2.5. Email Signature

When emailing with clients, patients, residents, family members or representatives, this language must be used in staff email signatures:

Clients/patients/residents: please visit www.providencehealth.bc.ca/ Emailing or Texting your Health Care Provider for the common risks and limitations you should be aware of when communicating health information through email or text.

It is recommended that all staff email signatures contain the following information:

The content of this e-mail, including any files attached, is confidential and may be privileged. Any unauthorized copying or distribution is strictly prohibited. If you receive this email in error, please contact the sender immediately and delete this email

2.6. Risks around Replying All/Forwarding

Staff must only use the "Reply All" function if everyone in the distribution list needs to know the information. If an email message has been received in error, staff must reply only to the sender versus the entire distribution list via "Reply All".

During short leaves or absences, staff members are not permitted to auto-forward email from a PHC email account to a personal email account unless an exception has been provided by Information Management/Information Technology Services (IMITS), in consultation with the PHC Information Access and Privacy Office.

Prior to sending the email, the staff member must check that the content of the email being forwarded, including previous content sent from others, is appropriate to send.

2.7. Distribution/Mailing Lists

Email sent using distribution or mailing lists must be of significant importance and relevant to all the staff in the list.

The blind carbon copy (BCC) feature in Outlook must be used to avoid displaying the recipients' email addresses.

Personal information must not be sent in a mass email communication, except as reasonably necessary for communications supporting the proper management of PHC business.

2.8. Broadcast Emails

Broadcast emails must relate to VCH or PHC business and operations, and be relevant to all staff. Communications & Public Affairs can be consulted regarding broadcast emails prior to their distribution.

2.9. Record Keeping

Email communications relating to care that are of clinical significance must be retained as part of or documented in the client's, patient's or resident's chart (either electronically or on paper) in accordance with Health Information Management policies and standards.

If email content and/or attachments of clinical significance cannot be captured in the chart, they should be saved in a secure network folder and deleted from all email folders at the earliest opportunity.

For further information on retention of electronic records of a clinical nature, including emails, refer to the Health Information Management policy on Records Retention & Disposal - Health Records.

For retention of corporate and business emails, refer to PHC policies and/or guidance on records retention.

2.10. Phishing Emails

Staff may occasionally receive spam or scam (phishing) emails at their PHC email accounts. When phishing or suspected phishing emails are received, staff must NOT reply or click on any links contained in the email, and must delete these emails promptly. Spam or phishing attempts may also be reported by forwarding such emails to spam@phsa.ca. If a link in a phishing email has been clicked, call the PHC Service Desk immediately for further instruction.

2.11. Privacy and Policy Considerations

2.11.1. Misdirected Emails

For misdirected emails sent containing personal or confidential information, staff must immediately try to recall the message and contact the recipient to request deletion of the email both from their inbox and then deleted folder box.

If you are in receipt of a misdirected email, respond only to the sender advising of the error and delete the email.

Misdirected emails containing personal or confidential information must be reported to the PHC Information Privacy Office.

2.11.2. Actual or Potential Privacy Breaches Involving Email

Unauthorized attempts to access or use an email account other than the account assigned to staff is considered a breach of policy.

Staff or their manager must report all actual or potential privacy breaches or breaches of this policy to the PHC Information Privacy Office. Staff will cooperate with the PHC Information Privacy Office in responding to any privacy breaches associated with emailing as per PHC Reporting and Management of Privacy Breaches Policy.

2.11.3. Compromised Email Accounts

Staff members are accountable for the content of all emails sent under their name.

Any staff member who believes there has been unauthorized access to their email account, including victims of a phishing attack, malware, etc. or otherwise compromised must immediately notify his/her manager and the PHC Service Desk.

2.11.4. Existing Policies

Emailing must also be done in compliance with other existing policies, including:

- Acceptable Use of Information Technology which provides details about what staff can and cannot do with PHC technology, including legal, ethical and responsible use of devices, and PHC's right to monitor and audit use of PHC technology;
- Information Privacy and Confidentiality which governs collection, use, disclosure and safeguards to be used in the protection of personal and confidential information;
- Remote Access which details permitted use of remote access to confidential information;
- Standards of Conduct and Respect at Work/Respectful Workplace & Human Rights policies, which provide guidance on appropriate conduct and behavioural expectations, in addition to any other professional code of ethics or standards of practice;
- User Identification and Passwords which details standards and rules governing the use of user IDs and passwords; and
- Consent forms governing restrictions and the permissible use and distribution of photography and video recordings.

Regarding the involvement of and client, patient or resident consent for personal information to be shared with family members, staff can refer to the Information Privacy and Confidentiality and Family Involvement with Mental Health & Addiction Services policies and guidelines for guidance.

3. Responsibilities

3.1 Information Access & Privacy Office (IAPO)

- Maintain and administrate the policy and associated Emailing Guidelines;
- investigate, coordinate, and document all privacy breaches related to email; and
- responding to Staff questions about acceptable and/or appropriate email use.

3.2 Leaders/Managers/Department Heads

- Authorize email accounts for their staff members;
- ensure Staff is aware of and abide by this policy; and
- assist Staff and the PHC Information Access & Privacy Office if there is a privacy breach per the Reporting and Management of Information Privacy Breaches Policy.

3.3 Staff

- Comply with this policy and its related policies and legislation;
- notify clients, patients, residents, family members and representatives to not use email for urgent or emergency situations and of the risks to personal information should their email account be compromised;
- immediately report all actual or potential privacy breaches or breaches of this policy to their manager and the PHC Information Access & Privacy Office;
- consult with their manager and/or the PHC Information Access & Privacy Office if they are unsure if their use of email is acceptable and/or appropriate; and
- consult the PHC Information Access & Privacy Office if considering creating further guidelines relating to this policy.

4. Compliance

Failure to comply with this policy may result in disciplinary action including, but not limited to, the termination of employment, loss of privileges as a student or volunteer role, prosecution and restitution for damages.

5. Supporting Documents

5.1 Related Policies

Related Policies and Guidelines

- Acceptable Use of Information Technology
- British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA)
- Cellular Phones and Smartphones
- Emailing Guidelines
- Family Involvement with Mental Health & Addictions
- Family Presence (Visitation) Policy
- Information Privacy and Confidentiality
- Record Retention/Destruction: Clinical Records
- Record Retention/Destruction: Non-Clinical Records
- Remote Access
- Managing Privacy Breaches
- Respect at Work
- Texting
- Standards of Conduct

5.2 Tools/Forms/Other Resources

5.2 Guidelines/Procedures/Forms

- Communications & Public Affairs (PHC)
- Emailing or Texting your Health Care Provider (Appendix A and online)
- Emailing Retention Decision Diagram (VCH/PHC) (Appendix B)
- Emailing Patient Information (College of Physicians and Surgeons of British Columbia)
- Emailing Guidelines for Researchers
- Password Recommendations (IMITs)
- Steps for Encrypting Common Electronic Files (IMITs)
- IMIT Computers, Phones & Technology (PHC Service Desk)

6. Definitions

"**Blind Carbon Copy**" **or** "**BCC**" allows the sender of an email to conceal the person entered in the BCC field from all other recipients.

"**Broadcast Email**" is defined as email distributed to all staff members across VCH or PHC.

"**Care Provider**" means any person who is involved in providing healthcare services to a client, patient or resident.

"**Client**", "**Patient**" and "**Resident**" means anyone receiving care or services from VCH or PHC, including Assisted Living tenants.

"**Confidential Information**" means all information, other than personal information, that is specifically identified as confidential or is reasonably understood to be of a confidential nature, that staff receive or have access to through VCH, PHC or other Lower Mainland Consolidation parties, including vendor contracts and other proprietary information that a Lower Mainland Consolidation party may have received from a third party.

"**Device**" means an asset that remotely connects to and accesses corporate information and resources. This includes, but is not limited to, smartphones (i.e. BlackBerrys, Android devices, iPhones), tablets, laptops, computers, or PDAs.

"**Email**" or "**Electronic Mail**" means messages sent and received electronically using VCH or PHC IT facilities. Attachments to emails are considered part of the email.

"**Family**" or "**Family Member**" is defined by the patient/resident. When the patient/resident is unable to define family, the patient/resident's next of kin or substitute decision maker provides the definition. Family members are the people who provide the primary physical, psychological, or emotional support for the patient or resident. Family is not necessarily blood relatives.

"**Personal Information**" means any information about an identifiable individual including, but not limited to: clients, patients, residents, volunteers, students, staff, physicians, or members of the public. Personal information does not include business contact information, such as a person's title, business telephone number, business address, email or facsimile number. Personal information can

include financial identifying information, such as a credit card, social insurance, bank account numbers or similar information that identifies an individual's financial account or record.

"**Phishing**" is the general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It's also known as brand spoofing.

"**Privacy Breach**" or "**Breach**" means unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information. Such activity is 'unauthorized' if it occurs contrary to Part 3 of FIPPA or VCH or PHC policies and procedures. The most common privacy breaches happen when personal information of clients, patients, residents or staff is inappropriately accessed, stolen, lost or mistakenly disclosed.

"**Representative**" means a person who has been verified by staff to provide assistance to the client, patient or resident outside of VCH or PHC. A representative could also be a substitute decision maker i.e. committee of person, representative or temporary substitute decision maker for the client (a copy of legal document or representation agreement must be provided).

"**Staff**" means all employees (including management and leadership), medical staff (including physicians, midwives, dentists and nurse practitioners), residents, fellows and trainees, health care professionals, students, volunteers, contractors, researchers and other service providers engaged by VCH or PHC.

7. References

Include citations for sources used in developing/reviewing the policy using the American Psychological Association (APA) bibliographic style. While the emphasis is upon current literature, cited references will reflect the strongest evidence/best practice.

Example of an APA citation:

Field, M.J. & Lohr, K.N. (1990). Clinical practice guidelines: Directions for a new program. Washington, D.C. National Academy Press.

8. Appendices

If the document includes appendices, list each appendix here by its proper name and hyperlink to the appendix.

- Appendix A: Emailing or Texting your Health Care Provider
- Appendix B: Emailing Retention Decision Diagram

Appendix A: Emailing or Texting your Health Care Provider

Emailing or Texting your Health Care Provider

Vancouver Coastal Health (VCH) and Providence Health Care (PHC) staff and physicians are committed to communicating with you about your care while protecting your privacy and personal information. Email and text communication however, comes with risks and limitations that you should be aware of.

What you need to know:

- Detailed clinical discussions, counselling or crisis-related support will not be provided by VCH or PHC staff or physicians through email or text messages.
- Emails and texts are not an appropriate substitute for in-person or over-the-telephone communication, clinical examinations or for attending the Emergency Department when needed.
- Personal information that you send in email or text messages could be at risk if an email account and/or device is compromised. It is your responsibility to protect your accounts and devices from inappropriate access and/or loss.
- There is no guarantee that VCH or PHC will receive or be able to respond to emails or texts in a timely manner; therefore, email and text messaging should not be relied upon in urgent or emergency situations.

If you send an email or text to a VCH or PHC staff member or physician expecting a reply and do not hear back within a reasonable time period, it is your responsibility to follow up with that person regarding your care and/or appointments.

Contact Information

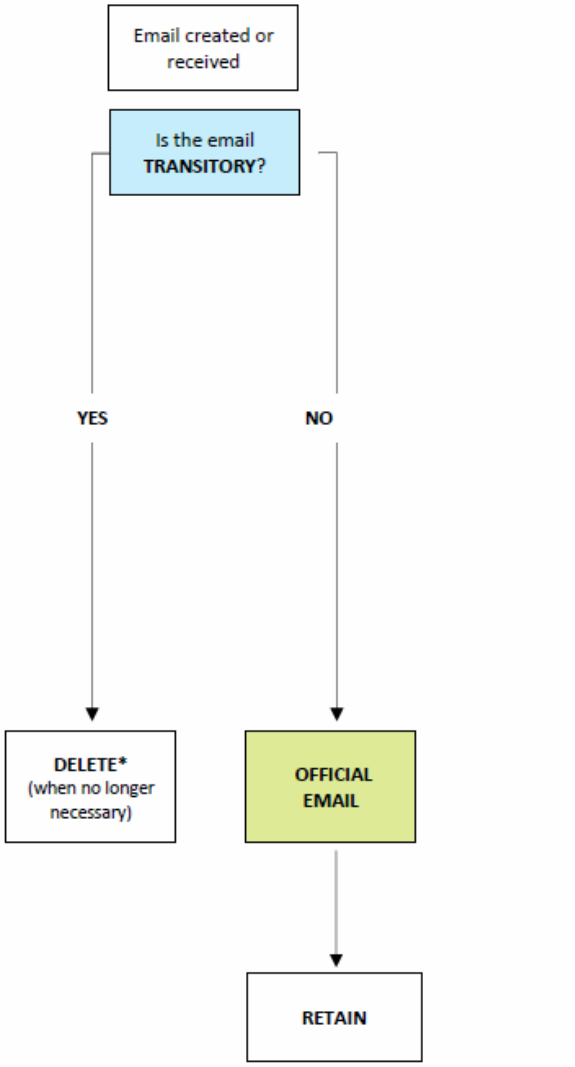
We welcome your comments and questions regarding emailing and texting between patients and VCH and PHC care providers. If you have questions, please contact us at the following:

VCH Information Privacy Office
Phone: (604) 875-5568
Email: privacy@vch.ca

PHC Information Access and Privacy Office
Phone: (604) 806-8336
Email: privacy@providencehealth.bc.ca

Appendix B: Emailing Retention Decision Diagram

Email Retention Decision Diagram



Detail: Transitory Emails and Official Emails

TRANSITORY EMAILS are records of temporary usefulness that are needed only for a limited period of time to complete a routine action or prepare a final record. Generally, they are not required for financial, legal, audit or statutory purposes.

Examples:

- Advertising material
- Announcements of social events
- Cc copies (unless you are the main individual responsible for the matter)
- Meeting arrangements
- Personal messages
- Simple messages reflecting commonplace interactions (i.e. a request to call someone)
- Outlines, calculations, preliminary notes and other rough content used to prepare a final record
- Drafts and revisions that are not needed to document decisions and associated approvals
- Routine correspondence about drafts and revisions

HOWEVER: Do not delete any transitory emails that ARE relevant to a FIPPA request or legal discovery. In these exceptional circumstances, transitory emails should be retained.

OFFICIAL EMAILS are emails that document or provide evidence of business activities. They must be retained and filed in appropriate folders.

Examples:

- Directives or approvals for courses of action
- Draft or revisions with information about a decision or associated approvals that is unavailable elsewhere (i.e. directions to change a proposal and recommend a different course of action)
- Final report or recommendations
- Meeting agendas and minutes
- Policy changes or developments
- Formal communication about official business
- Integral to understanding a client/patient relationship issue, decision or project
- Work and project plans

Effective Date:	21-Aug-2017		
First Released:	21-Aug-2017		
Last Revised:	01-Oct-2022		
Last Reviewed:	01-Oct-2022		
Approved By:	PHC		
	Shaf Hussain		
Owners:	PHC		

Revision History: *(optional)*	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
	2	01/OCT/2022	Minor change to 2.3 to reflect changes in FIPPA	Janet Scott