EMAILING POLICY AND GUIDELINES: FREQUENTLY ASKED QUESTIONS

POLICY BACKGROUND

What is the emailing policy?

The emailing policy and guidelines provide guidance to staff and physicians on safe and secure use of email when communicating with clients, other staff and care providers and external parties.

I thought email is unsecure and we should not be using it to send personal information?

In developing this policy, the Information Privacy Office researched and carefully assessed the primary risks associated with using email to communicate confidential and personal information. We identified the two key risks: 1) misdirection of emails (i.e. accidentally sending to the wrong recipient) and 2) phishing attacks (i.e. staff having their VCH email inboxes compromised through clicking on links or downloading viruses/malware in response to email scams). As such, a key component of this new email policy asks staff to take steps to ensure they have the right recipient(s) before sending. Additionally, the Information Privacy Office is working with IMITS to implement multi-factor authentication for VCH webmail in order to safeguard staff email accounts against phishing attacks.

With this update to the previous VCH email policy of 2004, VCH acknowledges the fact that emailing is one of many ways we communicate with clients and, in some cases, might even be the only practical means of communication in order for us to deliver quality care to certain population groups. This guidance has been provided to help staff and physicians to provide care while ensuring we are emailing in ways that mitigate privacy and security risks to our clients and VCH as a whole.

How do I safely email with my clients or other care providers?

To protect clients' information and privacy and mitigate security risks to VCH, ensure you do the following when emailing with clients, other staff and care providers and external parties:

- ***Confirm recipient:*** confirm the identity of those you are emailing before sending any personal or confidential information through email e.g. by verifying the person's email address in person or over the phone, or asking the other person to send the initial email.
- ***Small amounts of personal information are acceptable:*** small amounts of personal information about individuals can be sent via regular email to provide care or conduct other health authority business. "Small amounts" generally means information, including health records, pertaining to a particular individual per message. Where large amounts of personal information must be sent e.g. entire patient charts or lists of patient information pertaining to more than 10 individuals, files must be encrypted. For secure transmission of datasets for quality improvement, research or other secondary uses, contact the VCH Data Release Management Office.
- ***Retain client care records in chart***: retain and/or document any emails and attachments relating to client care that are of clinical significance in the client's chart, and then delete this information from your email account once this is done.
- ***Client notification:*** communicate to clients the common risks associated with emailing by forwarding them this link: www.vch.ca/emailtext.

AUTHENTICATING EMAIL RECIPIENTS

Do I have to ask my colleagues or patients to verify themselves every time I email them?

Only when contacting somebody for the very first time do you have to check whether you've got the right person on the other end of your email - and this must be done *before* sending any personal information via email. Once you know the intended recipient is the right person, you do not need to verify his/her identity again, unless a long time has passed since the last communication and it would be prudent in the circumstances to ensure that the person's email address has not changed.

RECORDS RETENTION

The policy says I need to ensure any relevant care information in the emails is recorded in the client's chart. Do I need to tell clients about this? Is there a privacy waiver they need to sign?

Retention and/or documentation of relevant care information by staff and physicians is something that is expected by clients when we provide care; this includes anything that may be received by email or in an email attachment. Therefore, no additional notifications or details to clients regarding privacy are needed.

Why can't I just keep my emails with client care information? Why do they have to be transferred to the client's chart or onto the network?

For system performance, data manageability and security reasons, email folders are not suitable as long-term records storage solutions, particularly as they relate to the storage and retrieval of client care records. Email communications that contain information of clinical significance would be considered a record under the *Freedom of Information and Protection of Privacy Act (FIPPA)* of British Columbia. Because of this, and to be consistent with Health Information Management (HIM) policies and standards on records retention, emails and attachments that contain relevant care information about our clients must be retained and/or documented in the client's chart.

How often do I need to delete my emails?

At the earliest opportunity, as soon as an email or email attachment containing information that is clinically significant has been retained or documented - either in the client's chart or in a secure network folder.

ENCRYPTING EMAILS

What is encryption? Why do I need to do this?

Encryption is a process for transforming readable information (e.g. text) into unreadable information, such as a code made up of letters, numbers and symbols. Such information remains unreadable until it is decrypted by using some form of key, such as a password. Encryption is used to protect the confidentiality of information from persons who are unauthorized to view such information.

Are encryption and password protection the same thing?

While encryption and password protection are related, they are not the same thing. Password protection can stand on its own without encrypting a file. It is similar to putting a document in a vault and locking the door. The text of the document has not been altered in any way i.e. converted into a code, but remains readable to anyone who is able to get into the vault. This is different to encryption,

which actually transforms text into unreadable information that must be decrypted before it can be read. Fortunately, most current software that allows users to password protect files also encrypts them at the same time, so you do not have to worry about doing both separately.

How do I encrypt?

There are different ways of doing this, depending on whether you are using a Word document, PDF, spreadsheet or a database. Refer to the Guidelines for Encrypting Common Electronic Files for guidance, as well as the Encryption and Password Recommendations. If you still have questions, contact the Information Privacy Office for help.

I'm still not clear about what is acceptable or unacceptable to include in an email. Can you specifically spell this out for me?

As it says in the policy, sending personal information in an email when conducting VCH business is acceptable, so long as steps are taken to minimize privacy and security risks to our clients and VCH as a whole. Just be sure to:

- Confirm your email recipient's identity before sending any personal information;
- Send only small amounts of personal information via email (or encrypt, otherwise);
- Retain client care information from your emails in the client's chart; and
- Notify clients of the common risks of using email by forwarding them this link: www.vch.ca/emailtext.

Bottom line: use good judgment when emailing, be professional in your email correspondence and follow the instructions above and in the policy. When in doubt, contact the Information Privacy Office.

VCH EMAIL VERSUS INTERNET-BASED EMAIL

VCH email is filled with unwanted messages so I don't use my VCH email address. Why can't I use my own email address?

As representatives of a public body, any email sent on behalf of VCH and/or related to client care must be from a VCH email address. This is to ensure we are in compliance with *FIPPA* regarding the collection, use, disclosure, storage, protection and retention of our clients' personal information. The Information Privacy Office is working with IMITS and other stakeholders to explore possible strategies for reducing the number of unwanted messages sent to VCH email account holders.

Most of my clients use Gmail, Hotmail or other kinds of internet-based email addresses. Does this mean I cannot email them?

Where clients have indicated interest for us to send them personal information via email, and as long as we have taken the steps to minimize privacy and security risks, it does not matter what type of email address they use. As we consider information and records within a client's email account to belong to them, protection of their personal information, once received by them in an email, is their own responsibility as set out in the notification to clients at www.vch.ca/emailtext.

USING EMAIL AS AN ALTERNATIVE TO FAXING

Can we use email to replace faxing?

This policy does enable programs to explore using email to communicate as a potential alternative to faxes. We recommend that departments and staff contemplating replacing their faxes with email contact the Information Privacy Office to determine whether a privacy impact assessment needs to be done to ensure that privacy, security, records management and other related risks are properly addressed when making these workflow changes.

SPECIFIC TERMS

What do you mean by "clinical discussion"?

This generally refers to any kind of lengthy or detailed discussion about a client's care or diagnosis.

What do you mean by "small" amounts of information?

This generally means information, including health records, pertaining to a particular individual per message. By contrast, examples of large amounts of personal information might include entire patient charts or lists of patient information pertaining to more than 10 individuals; in these cases, files must be encrypted.

What do you mean by "secure server" or "secure network folder"?

As specified in Section 30 of *FIPPA*, public bodies in BC are responsible for ensuring that personal information within their custody or control is protected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Files stored in network folders of public bodies, such health authorities, are considered secure to meet *FIPPA* requirements.

HOW-TO

I've mistakenly sent an email to the wrong person. What do I do?

For any misdirected emails you've sent that contain personal or confidential information, immediately try to recall the message and then contact the person you emailed in error to request they delete the email both from their inbox and then deleted folder box.

To recall an email, click on your Sent Items folder and open the message that you want to recall. Under the Message tab, choose Actions/Recall This Message.

I'd like to add the privacy disclaimer to my email signature. How do I do this?

This can be done by going to Outlook under the File tab/Options/Mail. Here you will find the option to "create or modify signatures for messages."

CONTACT INFORMATION

Where can I find the policy?

The policy is available on VCH Connect here. The guidelines can be found here.

When does the policy come into effect?

The policy is in effect as of July 7, 2017.

Who can I contact for more information about the policy?

Contact the VCH Information Privacy Office at privacy@vch.ca or (604) 875-5568 if you have questions or would like help in updating or creating emailing guidelines for your unit or department.