Texting Policy

1. Introduction

Description

Vancouver Coastal Health (VCH) Staff are using Text Messaging, or Texting, as one way to communicate with Clients, Family Members, Representatives, Care Providers and other Staff. The purpose of this policy is to establish specific procedures to mitigate privacy and security risks associated with the use of Text Messaging for work purposes.

Scope

This policy applies to all Staff, including physicians.

2. Policy

2.1. Use of Text Messaging

Where available, text messages should be sent from VCH-issued mobile Devices only. If Staff must use a personal Device, only the vendor-provided text message service or SMS (Short Message Service) or MMS (Multimedia Messaging Service which enables users to send photographs, audio or video over a mobile phone) must be used. As third-party services such as WhatsApp, Viber, Hangouts, etc. store data outside of Canada, they are not permitted and must not be used for Texting or sending multimedia messages. Requests for use of third-party services for specific projects must be submitted to the Information Privacy Office for review.

Any Staff member using a personal Device for Texting while at work will be expected to ensure their job duties and responsibilities are being given full attention, as set out in the Standards of Conduct policy.

Due to delays which may occur with the transmission of text messages, Text Messaging must not solely be relied on for urgent communications.

To prevent any miscommunication, abbreviations should be avoided.

2.2. Authenticating the Recipient

Texting may be used to communicate Personal and Confidential Information so long as Staff take appropriate measures to authenticate the identity of intended text message recipients.

Ways of authenticating include:

- Sending an initial text to confirm the right Staff member or Client is being contacted i.e. before sending any Personal or Confidential Information; and/or
• When texting with Clients, Family Members or Representatives, asking the recipient to verify, by text or phone, the Client’s birthdate, PHN or other piece of information that only the intended recipient would know.

Authentication must be done on communication with any recipient who has not been previously authenticated. Subsequent Text Messaging communications do not require recipient authentication. Until measures have been taken to authenticate the recipient’s identity, Staff must avoid Texting Personal or Confidential Information.

2.3. Notice Regarding Text Messaging

Staff must communicate to Care Providers, other Staff, Clients, Family Members or a Client’s Representative the common risks associated with Texting. These risks are summarized in the Emailing or Texting your Health Care Provider notice available on VCH’s external Information Privacy Office website. The notice describes that:

• Text messages can include Personal Information, which will be at risk if their Device is compromised.

• There is no guarantee that VCH will receive or be able to respond to text messages in a timely manner; therefore, Texting should not be used in urgent/emergent situations.

Staff can inform recipients of these risks by providing them with a link to the information online, or by printing and distributing the information as a handout.

Transferring the notice onto a device can be done by accessing the information online from the device. Suggested ways of doing this include:

• Visiting the external Information Privacy Office website by going to www.vch.ca, navigating to Contact Us/Information Privacy Office, and clicking on the “Emailing or Texting your Health Care Provider” notice from the device;

• Emailing the full website address, http://www.vch.ca/media/VCH-Emailing-Texting.pdf, or the short website address, www.vch.ca/emailtext, to the notice for access from the device; or

• Manually entering the full or short website addresses as above into a browser on the device.

This information can then be sent to other Staff, Clients, Family Members or a Client’s Representative by copying and pasting the link into a text message.

2.4. Record Keeping

Texts, including multimedia messages that contain photographs, audio or video, should be treated as temporary communications similar to phone calls. Text and multimedia message communications of significance must be documented in the Client’s chart in accordance with usual charting requirements. Once this documentation has been made, the Text and
Multimedia Messaging history and any Personal and Confidential Information must be deleted from the mobile Device.

2.5. Privacy and Policy Considerations

Mobile Devices and personal Devices used for Texting with Clients, Family Members, Representatives, Care Providers and other Staff must be password-protected. Texting 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 VCH technology, including Devices used to communicate text messages, and VCH’s right to monitor and audit use of VCH technology;

- **Information Privacy & Confidentiality** which governs collection, use and disclosure of Personal and Confidential Information; and

- Consent forms governing restrictions and the permissible use and distribution of photography and video recordings.

This policy is also subject to any ensuing Bring Your Own Device (BYOD) policy which governs the use of personal Devices for work-related purposes.

Regarding the involvement of and Client consent for Personal Information to be shared with Family Members, Staff can refer to the **Information Privacy & Confidentiality** and **Family Involvement with Mental Health & Addiction Services** policies for guidance.

Staff are permitted to save Client contact information on their Device e.g. Client name and/or ID number. However, no Client information shall be stored on cloud-based services e.g. iCloud, Google Drive, OneDrive, Dropbox, etc. Automatic backup to the cloud must be turned off for text messages, multimedia messages and contact lists (if these contain Client information).

Staff or their Manager must report all actual or potential Privacy Breaches or breaches of this policy as a result of Text Messaging to the Information Privacy Office. Staff will cooperate with the Information Privacy Office in responding to any Privacy Breaches associated with Text Messaging as per the **Reporting and Management of Information Privacy Breaches** policy.

2.6. Permitted and Prohibited Text Messaging Communications

The following outlines types of Text Messaging communications which are permitted and prohibited.

2.6.1. Permitted Text Messaging Communications

- Scheduling, confirming or cancelling appointments.
- Providing reminders for appointments, tests, etc.
- Replying to location or hours of operation requests.
• Sharing useful resources e.g. general program information, websites, contact information.
• Checking on Client (i.e. how are you doing? Do you need anything?).
• Providing an invitation to a health promotion event.
• Responding to Client’s, Family Member’s or Representative’s requests for services.
• Communicating a Client’s location with Staff.
• Requesting a consultation or assessment by another Care Provider.
• Providing medical escort and/or patient travel instructions.

2.6.2. **Prohibited Text Messaging Communications**

- Sending prescription refills.
- Informing a Client or Family Member or Representative of the Client’s diagnosis.
- Communicating Financial Identifying Information e.g. credit card numbers, etc.
- Engaging Client in lengthy clinical discussions or counseling.

The Texting of certain medication or treatment orders may be restricted by some professional practice standards. Staff and physicians are advised to check with their College or other professional association for further information regarding this.

### 2.7. Responsibilities

#### 2.7.1. Staff

Staff will:

- Comply with this policy and its related policies.
- Notify Clients, Family Members or Representatives, Care Providers and other Staff to not use Text Messaging for urgent or emergent situations and of the risks to Personal Information should their Device be compromised.
- Ensure that the Devices used for Texting with Clients, Family Members, Representatives, Care Providers and other Staff contain security safeguards, such as a password.
- Contact the Information Privacy Office to report all actual or potential Privacy Breaches and cooperate with the Information Privacy Office in responding to any Privacy Breaches associated with Text Messaging.
• Consult the Information Privacy Office if considering creating further guidelines relating to this policy.

2.7.2. Management

Management will:

• Ensure that Staff members are aware of and abide by this policy.
• Review the policy with Staff from time to time to make sure best practices are followed.
• Review the policy with new hires.
• Cooperate with the Information Privacy Office in responding to any Privacy Breaches associated with Text Messaging.

2.7.3. BC Clinical and Support Services (BCCSS) Society/Information Management Information Technology Services (IMITS)

BCCSS/IMITS will:

• Provide guidance to update this and relevant policies to address changes in technology and risks.

2.8. Compliance

The Information Privacy Office will:

• Have primary responsibility for the administration and maintenance of this policy.
• Receive, review and provide privacy guidance for requests regarding the use of third-party services for specific projects.
• Respond to Staff questions about compliance with this policy.

Failure by Staff to comply with this policy may result in disciplinary action up to and including termination of employment, services or privileges.

3. References

Tools, Forms and Guidelines

• Consent for Photography, Audio-Visual Recording and Interviews
• Emailing or Texting your Health Care Provider
• Media Consent i.e. use of name, image, photograph, voice, statements
• Texting Policy: Frequently Asked Questions (FAQ)
Related Policies

- Acceptable Use of Information Technology
- Cellular Phone and Blackberry Devices
- Emailing
- Family Involvement with Mental Health and Addiction Services
- Information Privacy and Confidentiality
- Information Security
- Reporting and Management of Information Privacy Breaches
- Records Retention
- Social Media, Websites and Online Communication
- Standards of Conduct
- Video, Electronic and Other Forms of Surveillance
- Use of Telecommunication Services and Devices

Keywords

cell, cell phone, device, mobile, mobile device, mobile phone, personal information, privacy, SMS, text, texting, text messaging

Definitions

“Care Provider” means any person employed by VCH, or any other health authority, to offer any service related to the Client’s physical or mental well-being.

“Client” means anyone receiving care or services from VCH and includes patients and residents.

“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 or through 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.

“Family” or “Family Member” means a person who has been identified by the Client, the Client’s Representative or the Client’s Care Provider as being in a relationship of importance to the Client and who provides support or care for the Client on a regular basis.

“Financial Identifying Information” means credit card, social insurance, or bank account numbers.
“Multimedia Messaging” or “MMS (Multimedia Messaging Service)” refers to messages sent or received on a mobile phone using a cellular network that include multimedia content, such as photographs, audio or video. Similar to SMS messages, MMS messages do not require an internet data plan or access to Wi-Fi to be sent or received.

“Personal Information” means any information about an identifiable individual, but does not include business contact information (e.g. individual’s title, business telephone number, business address, business email or facsimile number).

“Privacy Breach” or “Breach” occurs when there is unauthorized access to or collection, use, disclosure or disposal of Personal Information. Such activity is “unauthorized” if it occurs in contravention of Part 3 of the *Freedom of Information and Protection of Privacy Act*¹.

“Representative” means a person who has been verified by Staff to provide assistance to the Client outside of VCH. 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 nurses), residents, fellows and trainees, health care professionals, students, volunteers, contractors, researchers and other service providers engaged by VCH.

“Text Messaging”, “Texting” or “SMS (Short Message Service)” refers to short text messages either sent or received on a mobile phone using a cellular network which does not require an internet data plan or access to Wi-Fi.

**Questions**

Contact: Information Privacy Office at privacy@vch.ca

---