CPN0900: Texting Policy

Approved Date:	November 30, 2016
Reviewed/Revised Date:	

1.0 Introduction

1.1 Description

This policy describes how Providence Health Care (PHC) Staff can use Text Messaging, or Texting, as a method of communicating with Patients, Residents, Clients, Family Members 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.

1.2 Scope

This policy applies to all Staff, including all Medical Staff. It is expected that program areas that routinely use Texting as a form of communication will develop program-specific procedures consistent with this policy to accommodate the varying degree of sensitivity of the information being communicated.

2.0 Policy

2.1 Use of Text Messaging

PHC supports the use of Texting as a method of communication when appropriate.

Text messages will be sent from PHC-issued devices, when Staff has a PHC device.

Use only the vendor-provided Short Message Service (SMS) or Multimedia Messaging Service (MMS). This refers to the “normal” Text Messaging service provided by the standard enterprise or consumer telecommunications service providers i.e. Bell, Rogers, Telus, etc.

Third party applications, such as Whatsapp, Facebook, Hangouts or iMessage store data outside Canada and therefore cannot be used for Texting or sending multimedia messages. Requests for the use of third-party services for specific projects must be forwarded to the PHC Information Access and Privacy Office for review.

Any staff member using a mobile device for Texting must comply with their own professional and ethical standards, as well as CPL1400: Standards of Conduct and the policies referenced therein.

Due to delays which may occur during the transmission of text messages, Text Messaging should not be solely relied upon for urgent communications.

If deemed necessary that Personal Health or other Confidential Information be communicated through Text Messaging, only the minimum amount of information necessary to support the purpose should be included. If photos need to be sent via Texting (e.g. wounds, ECG tracings), they should not include any identifiable information (e.g. faces, names, DOB).

2.2 Authenticating the Recipient

Text Messaging may be used to communicate Personal and Confidential Information as long as Staff takes appropriate measures to authenticate the identity of the intended recipient prior to communicating the confidential information. Once a recipient has been authenticated for an encounter/event, subsequent Text Messaging communications do not require recipient authentication for that same encounter.

Ways to authenticate include:

- Sending an initial text to confirm you have connected with the right Staff member or Patient, Resident, Client or Family Member.
- Providing your contact information to the Patient, Resident, Client or Family Member and asking them to send the first message, ideally with one piece of information that only the individual would know.
- Ask the recipient to verify, by text or phone, information that only the intended recipient would know (e.g. month/year of birth, last 4 digits of PHN, reference number, date of last clinic visit, or other previously agreed upon information).

2.3 Notice Regarding Text Messaging

It is the responsibility of Staff to communicate the common risks of Texting to other Staff, Patients, Residents, Clients or Family Members. These risks include, but are not limited to:

- Text messages can include Personal Information, which will be at risk if their Device is compromised
- There is no guarantee that PHC will receive or be able to respond to Text Messages in a timely manner; therefore texting should not be used in urgent or emergent situations
- Text messages may be stored in backup servers by telecommunications service providers, even if manually deleted from the Device itself

Staff can inform recipients of the risks by providing them with a copy of the information which is provided in Appendix A.

2.4 Record Keeping

Text Messages, including multimedia messages that contain video, audio, or images, should be treated as a temporary communication, similar to a phone call. Text and multimedia messages of clinical significance must be documented in the Patient, Resident or Client's chart. Once documentation is made and the specific encounter has ended (e.g. patient has been discharged), the messaging history and any Personal and Confidential Information must be deleted from the mobile Device.

2.5 Privacy and Policy Considerations

Any device used for communicating with Patients, Residents, Clients, Family Members or other Staff Members must be password protected. Texting must also be done in compliance with other relevant PHC policies (see 3.0 References).

This policy is also subject to:

- Any consent forms governing restrictions and the permissible use and distribution of photography, videos or audio
- Any guidelines or policies governing the use of personal devices for work-related purposes

Staff may store minimal Patient, Resident, Client or Family Member contact information on their Devices (e.g. name and/or ID number and phone number). Automatic back-up to the Cloud (e.g. iCloud, Google Drive, OneDrive, Dropbox) must be disabled for Text Messages, multimedia messages and contact lists (if applicable).

2.6 Reporting Privacy Breaches

Staff or their Manager must report any and all actual or potential privacy breaches associated with Texting to the Information Access and Privacy Office, as per CPF1600: Managing Privacy Breaches Policy with CPF1500: Safe Reporting in consideration as well.

2.7 Permitted and Prohibited Text Messaging Communications

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

Permitted Text Messaging Communications:

<u>Administrative Purposes:</u>

- Scheduling, confirming or cancelling appointments
- Providing reminders, such as for appointments or tests
- Requests to contact a program/department
- Replying to location or hours of operations requests
- Providing medical escort and/or Patient/Resident/Client travel instructions

<u>Health Education & Promotion Purposes</u>

- Providing an invitation to a health promotion event
- Sharing resources that may be of interest to the client e.g. general program information, websites, contact information

<u>Patient/Resident/Client Continuity of Care Purposes</u>

- Checking on a client (How are you doing? Do you need anything?)
- Responding to Patient, Resident, Client or Family Member’s requests for services

<u>Communicating between Care Providers/Staff</u>

- Communicating a Patient, Resident or Client’s location with staff

- Requesting a consultation or assessment by another Care Provider

Prohibited Text Messaging Communications:

- Sending prescription refills
- Informing a Patient, Resident, Client or Family Member of a Patient, Resident or Client's diagnosis
- Communicating Financial Identifying Information e.g. credit card numbers
- Engaging Patient, Resident or 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 associations.

2.8 Responsibilities

2.8.1 Staff will:

- Comply with this policy, related PHC policies and guidelines and program-specific procedures.
- Notify Patients, Residents, Clients, Family Members and other Staff Members not to use Text Messaging for urgent or emergent situations
- Notify Patients, Residents, Clients, Family Members and other Staff Members of the risk to Personal or Confidential information should their Device be compromised
- Ensure that the devices used for texting with Patients, Residents, Clients, Family Members, Care Providers and other Staff contains appropriate security safeguards including turning off Cloud storage and using a password
- Contact the Information Access and Privacy Office to report all actual or potential privacy breaches and cooperate with the Information Access and Privacy Office in responding to any breaches associated with text messaging
- Ensure device is wiped or erased when retiring the device
- Consult the Information Access and Privacy Office if creating further guidelines relating to this policy

2.8.2 Management will:

- Ensure that Staff Members are aware of and abide by this policy
- Review the policy with their Staff on a regular basis to ensure best practices are followed
- Review the policy with new hires, where applicable
- Cooperate with the Information Access and Privacy Office in responding to any privacy breaches associated with Texting

2.9 Compliance

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

3.0 References

3.1 Tools, Forms and Guidelines

- Consent for Photography and Audiovisual Recording

3.2 Related Policies

- CPL1400 - Standards of Conduct
- CPF0300 - Information Privacy and Confidentiality
- CPF0900 - Record Retention/Destruction: Clinical Records
- CPF1500 - Safe Reporting
- CPT3100 - Family Presence (Visitation) Policy
- CPF1600 - Managing Privacy Breaches
- CPN0405 - Cellular Phones and Blackberry Devices
- CPN0802 - Information Security
- CPN1240 - IT Asset Security Policy
- CPN1301 - Acceptable Use of Information Technology

3.3 Definitions

Client means anyone, other than Patients or Residents receiving care or services from PHC including youths at a PHC youth clinic.

Confidential Information means all information, other than Personal Health Information, that is specifically identified as confidential or reasonably understood to be of a confidential nature, that Staff receive or have access to through PHC 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** (as defined in PHC's Corporate Policy CPT3100: Family Presence (Visitation): *Family 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. Family members are encouraged to be involved and supportive of the patient/resident and are integral to the overall well-being of the patient/resident.*

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.

Patients and Residents mean all people receiving services from PHC. For ease of language, Assisted Living tenants are not specifically named but are implied in any reference to patient/resident.

Personal Health Information means identifying information about the individual in oral or recorded form, if the information relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual; relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance; the individual's health number; or identifies an individual's substitute decision-maker.

Personal Information means any information about an identifiable individual but does not include business contact information, such as a person's title, business telephone number, business address, email or fax number.

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 PHC.

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.

3.4 Keywords

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

Questions:
Contact: Information Access and Privacy Office at privacy@providencehealth.bc.ca

Appendix A: Notice

Emailing or Texting your Health Care Provider

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:

Clinical discussions, counseling or crisis-related support will not be provided by 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 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 emergent situations.

If you send an email or text to a 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.

Email and text are not secure, private or confidential modes of communication. Text messages may be stored in backup servers by telecommunications service providers, even if manually deleted from a phone. Electronic communications may also be re-routed or stored outside of Canada.

Contact the Information Access and Privacy Office

We welcome your comments and questions regarding emailing and texting between patients and PHC care providers. If you have questions, please contact our Information Access & Privacy Office:
Email: privacy@providencehealth.bc.ca