Date:  May 1, 2018
To: All VCH Community Directors and Managers
From: Lorraine Blackburn, Executive Director, Clinical Informatics, Professional Practice
CC: Barb Lawrie, Vice President, Professional Practice and Chief Clinical Information Officer
Re: Community Smartphones Update

Where are we at?

Since smartphone deployment started in the fall of 2017, feedback about the phones has been excellent. Many staff members are finding innovative ways to use the devices in their clinical practice, and for communication within their work team.

At the same time, we are hearing from smartphone users and programs that the inability to access apps has been a concern for patient care and communication. The smartphone working group has researched options to support this request and we are now ready to provide some help.

What’s happening next?

Today we are announcing a relaxation in some of the rules restricting the use of VCH issued smartphones. In keeping with our intention to be innovative in our practices, and to respond to your feedback, we want to make sure the rules around smartphone usage help you and your teams to decide how to use your smartphones to benefit staff and clients, and still operate within our privacy and security framework.

As of now, VCH staff members using VCH issued smartphones are permitted to:

1. Use an AppleID to access the iTunes app store on their VCH issued smartphone
2. Download VCH approved apps to their smartphone.

AppleID for app downloads

Before downloading any apps, staff members using a VCH-issued smartphone may create an Apple ID account using their personal email address or a VCH issued email address. No payment method (e.g. credit card) should be associated with an Apple ID that uses a VCH issued email address. This is a change from the previous direction that no Apple ID was permitted on VCH issued smartphones.

Keep a secure record

Each phone user must communicate their Apple ID and password to their Admin support person, who should keep a secured record of at least the: User name, Phone #, Passcode, Apple ID and Apple ID password for each phone under their control. This ensures the phones can be managed if/when they are re-assigned, if they are lost, or if they are shared. We ask that Directors and Managers ensure a secure record keeping process is in place for smartphones used by staff in their area.

Please Note: In the future, all smartphones will come under the “Airwatch” enterprise mobility management program. At that time smartphones may need to be reset. Apps and data on each phone may be lost.
Approved apps for VCH Smartphones

The following is a list of apps approved for use on VCH issued smartphones. Other apps are under review by the VCH/IMITS Working Group and will be added to the list when approved. Staff may now download these apps to their smartphone.

- **Up-to-date** (Clinical Decision Making): [https://www.uptodate.com/home/how-access-uptodate](https://www.uptodate.com/home/how-access-uptodate)
- **Pay-by-Phone** (Parking): Find on iTunes
- **Google Maps** (route maps and navigation): Find on iTunes
- **Chrome Browser** (web browsing): Find on iTunes
- **Facebook** (Social media): Find on iTunes
- **Twitter** (Social media): Find on iTunes
- **Skype for Business** (Messaging): Find on iTunes (See [Skype For Business](https://www.skype.com/usa/business/) user sign in process)
- **SafeNet Token** (Remote access): referred by IMITS when user requests remote access to VCH network.
- **RACE** (Clinical advice) Rapid Access to Clinical Expertise for Physicians and Nurse Practitioners - [http://www.raceconnect.ca/race-app/](http://www.raceconnect.ca/race-app/) and iTunes store
- **Facetime** (Wireless phone to phone call): comes with iPhone.

For more information about apps and Apple IDs, see the Community Smartphone website or email smartphonedeployment@vch.ca.

**Turn off iCloud**

The requirement to turn off iCloud services on VCH issued phones is still in place. iCloud is a function that allows sharing of information (photos, videos, documents, apps, and more) across multiple devices…and it stores information in the US. This presents a privacy risk and is also in violation of BC’s Freedom of Information and Protection of Privacy Act (FIPPA). To help ensure good stewardship of our clients’ personal information, when using an iPhone, staff must:

- Turn OFF (if on) iCloud services by following the Apple's instructions to change iCloud settings.

**Follow smart business practices**

In all cases, VCH Smartphones should only be used for appropriate business activity, including team communication and clinical practice support. Messaging, downloads and data storage should be limited to information necessary for the effective provision of care to clients, or communicating within a distributed work team. Documentation of any clinically significant information should be done in the Client, Patient or Resident’s chart, and not saved on the smartphone. Staff members should report a lost phone to the VCH Service Desk and their Admin support person, and report any actual or potential privacy breaches associated with the phone to the VCH Information Privacy Office at [privacy@vch.ca](mailto:privacy@vch.ca).

**What you can do now**

The Community Smartphone Deployment website has been updated with new instructions about the use of AppleID’s and the list of approved APPs. Please communicate to your teams that these guidelines are changing. View the updated Quick Reference Guide and share it with your staff.
If you have any questions regarding the information in these guidelines, or about using a smartphone contact:

- Smartphone Deployment Project team: smartphonedeployment@vch.ca
- VCH Service Desk: VCHservicedesk@hssbc.ca