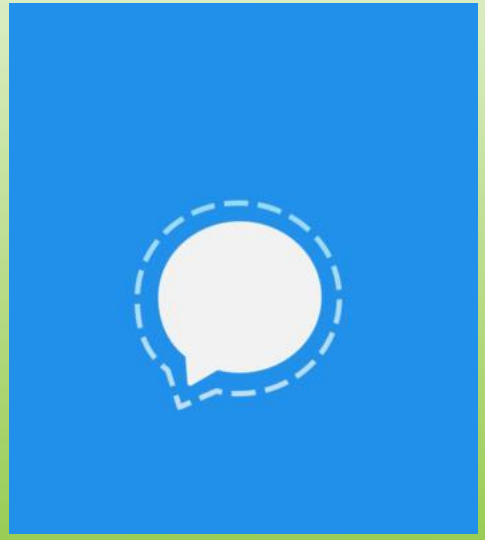
Health PEI
One Island Health System

Secure Text Messaging: Embracing Technology



Module Contents

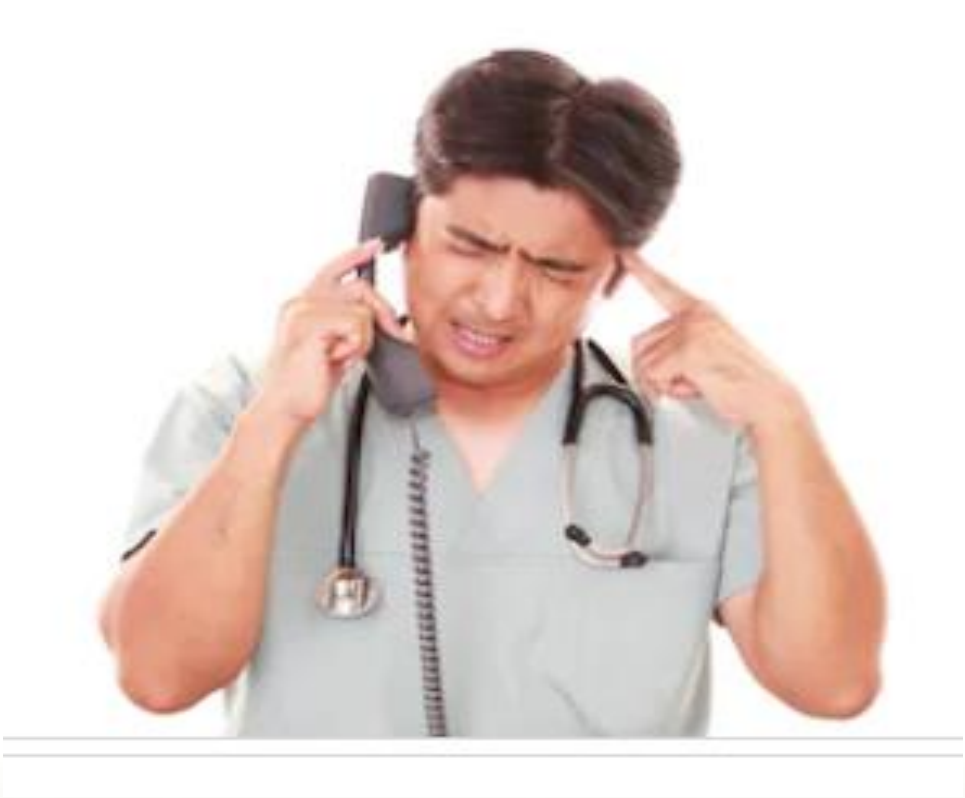
Why Texting?

Privacy, Confidentiality and Security

Step by Step Instructions to Set up on Your Device/Signal App to Take Advantage of the App Options for Top Security

Why do clinicians want to text?

Description vs Picture



Important Definitions

Privacy: The right of an individual to control the collection use disclosure and retention of their personal information

Confidentiality: The obligation of the health care professional to protect the secrecy of personal information

Security: The tools and techniques we use to protect the confidentiality, integrity and availability of personal information

Privacy, Confidentiality and Security

Common questions and answers about secure text messaging with Signal ©

Can I text interesting pictures of patients to my co-workers…for education purposes?

No. PHI and any patient information is to be provided on a need to know basis only.

The purpose of this project is to use secure text messaging for messages between providers who are providing care or, are being consulted to become a part of the provision of care.

Texting is for simple questions, or to engage another physician/health care provider ie. Is this X-Ray a clinic consult or an admission? Can you VPN into this patient's chart and call me to discuss? Can you look at this wound?

Is my patients' information secure when texting?

Your phone is equipped with a texting App that is NOT private. *"SMS texting" is not secure and is easily hacked*

Texting with the Signal App is a secure texting modality. Here's how…

Signal's Terms and Privacy Policy

- Signal© is equipped with open end-to-end encryption, messages are only viewable by the writer and intended recipient
- Signal© cannot decrypt or access the content of messages
- Signal© will queue *encrypted* messages on its servers when devices are temporarily offline

BAD NEWS FBI, EDWARD SNOWDEN'S FAVORITE CHAT APP SIGNAL JUST GOT $50M IN FUNDING

BY **JASON MURDOCK** ON 2/22/18 AT 10:31 AM EST

Former U.S. National Security Agency contractor Edward Snowden appears live via video during a student organized world affairs conference at the Upper Canada College private high school in Toronto, February 2, 2015. Snowden is a known fan of Signal, the chat app.

REUTERS/MARK BLINCH

Should I just write patient initials and not include PHI to protect privacy?

No.

When using *a secure text messaging App*, please include the personal health information. The standard is to provide two identifiers for proper identification of the patient by the receiver (full name, DOB, PHN or MRN)

The approved text messaging app is

Signal©

Can I be sure that my patients' information is not compromised?

The facts

- If you are using a regular phone message App, information is at risk for being intercepted or "hacked"

- The ITSS Chief Security Officer has recommended Signal © as the secure text messaging app of choice

You can help

- Follow the guidelines!

What is my role in privacy and security?

- Physicians/HC Providers sending secure text messages will set disappearing text for 24 hours, enough time for the receiving physician/HC Provider to enter the chart and document the conversation

- You will need to set two technological safeguards:
  - On the phone: set a confidential password to enter the personal device
  - In the App: download the free Signal© App and apply an App biometric or password lock

- Physicians/HC Providers will not store, screen shot or otherwise save or upload patient information directly onto their device. Document your text conversation in a progress note.

- Physicians/HC Providers will ensure that the receiving physician/HC Provider is using the Signal © App and verify the receiver before sending information

- Information is shared on a need to know basis only

Guidelines

Setting Technological Controls on Your Personal Device: Step by Step Instructions

Set up:

1. Your phone
2. Your Signal App Settings
3. 3. Your contact Settings within the Signal App

Step One: Your Personal Device

Make sure there is a **private** password to your personal device

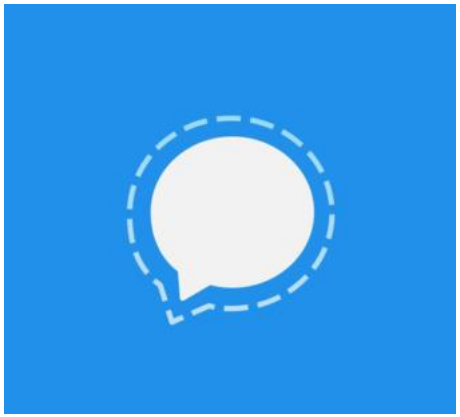
Or

A Biometric passcode, which is preferred (fingerprint, retinal scan)

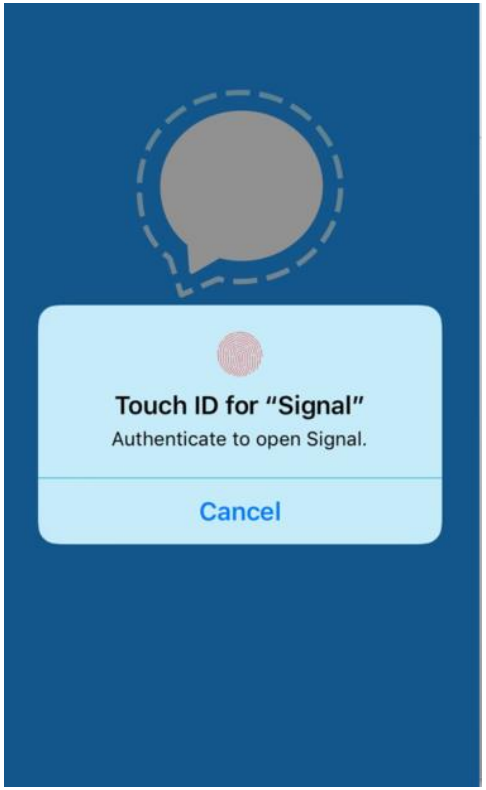
If you use a biometric entry into the device, make sure you are the only user of the phone. Phones will allow more than one biometric scan to open the device for access

ie. *If you share your phone with your family, you can't share PHI or patient information on the device*!

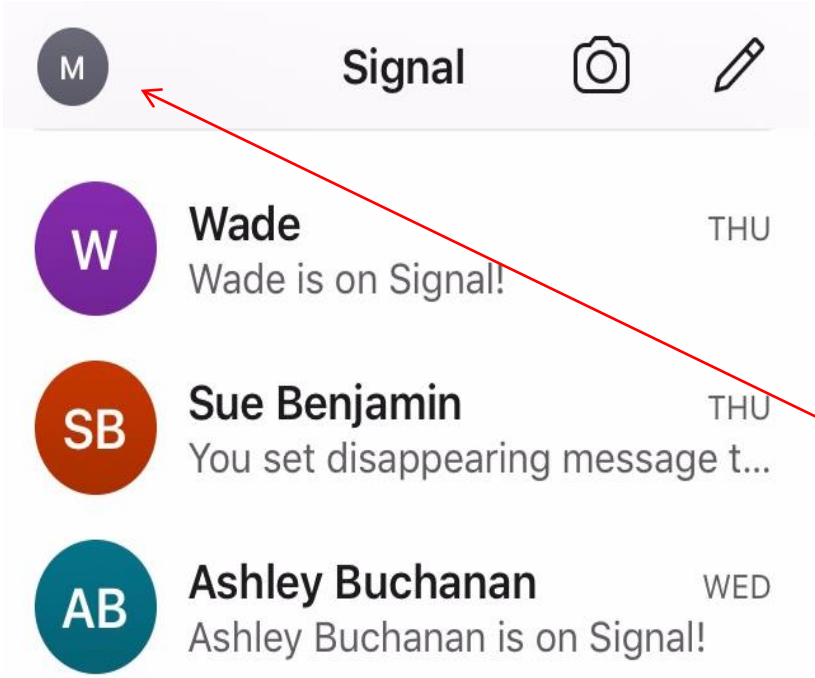
Step Two: Download the Signal App on your iOS or Android



Step Three: Apply Technological Safeguard to enter the Signal App



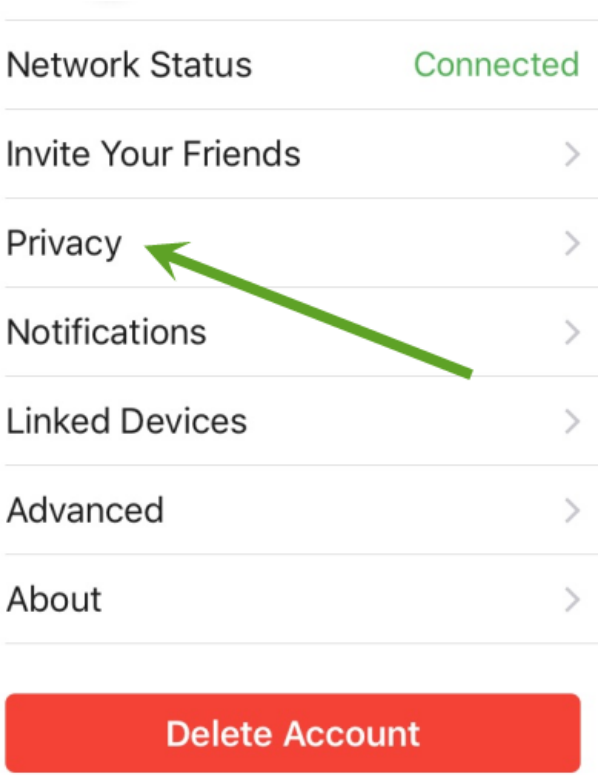
You want to set up your phone/device so that only you can access the app, it adds an extra layer of security



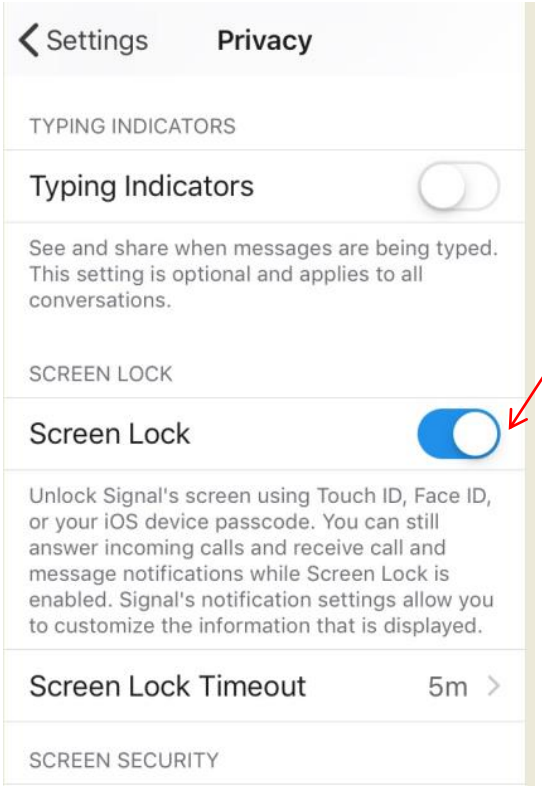
When you open Signal, a list of your conversations will appear once you get started

Above the names is an “M”. Select/touch the M

You are now in Settings



Select Privacy

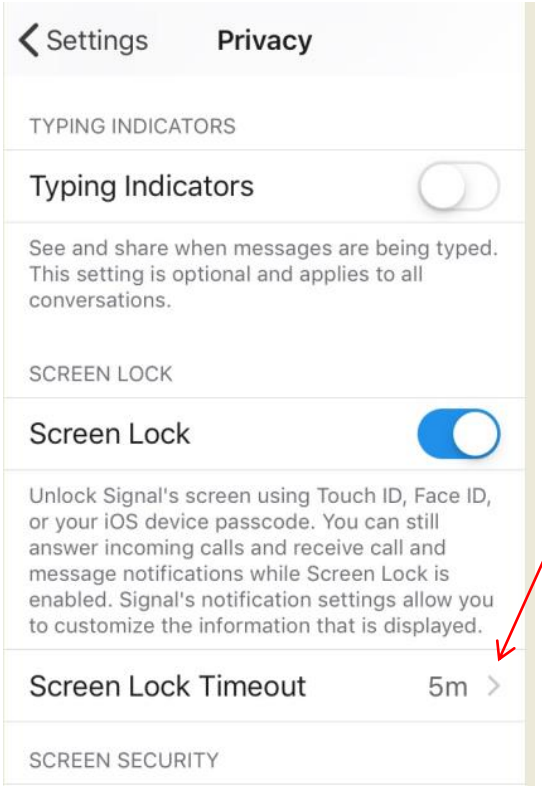


Turn on ”screen lock”

And follow the on screen instructions

If your phone/device allows, biometric locks are safer than password locks

Step Four: Set Screen Lock Out

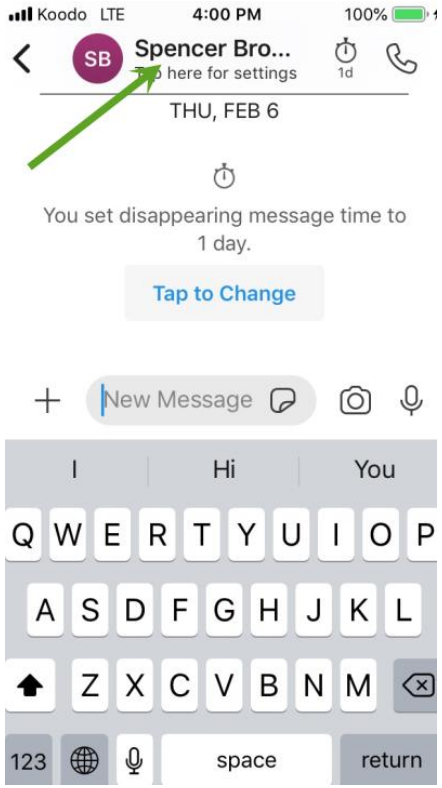


Set your screen lockout to no more than 5 minutes

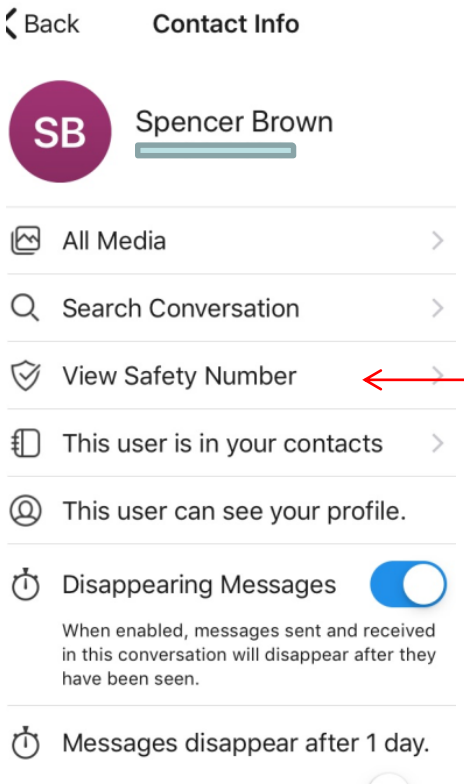
Step Five: Set UP each Contact Within the App: Verify your Contacts

Signal will verify Signal users from your current contact list when you initiate texting

Verify Contacts



- Click on the contacts name in the message window to find the contact settings window

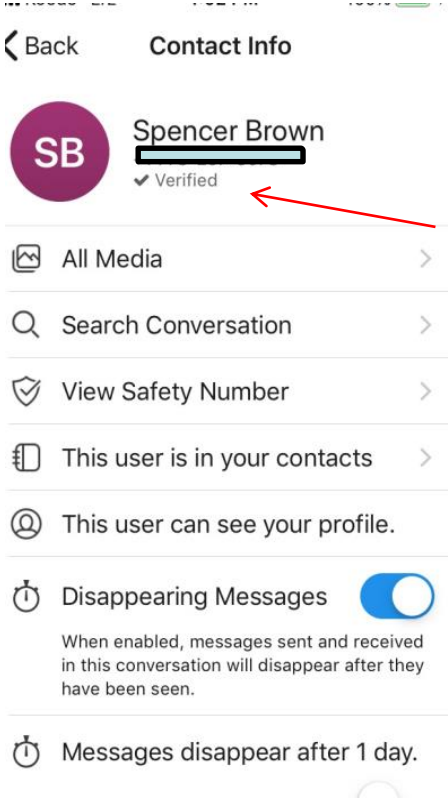


In the list that appears, choose view safety number

Known Contact, Known Signal User

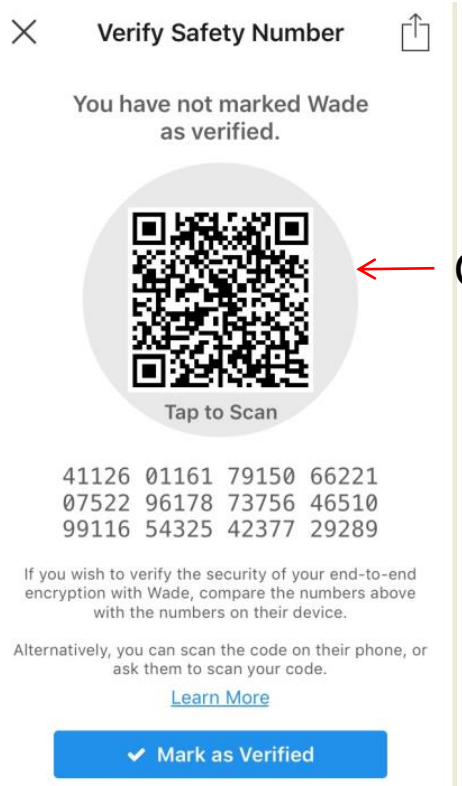
In this case, the user is aware that Dr. Brown has the Signal App. There are multiple texts a month between the users therefore, there is no doubt number that stored is indeed his number

Go ahead and choose ‘mark as verified’



Dr. Brown is now marked as verified

Unknown User or Unsure if Signal Download

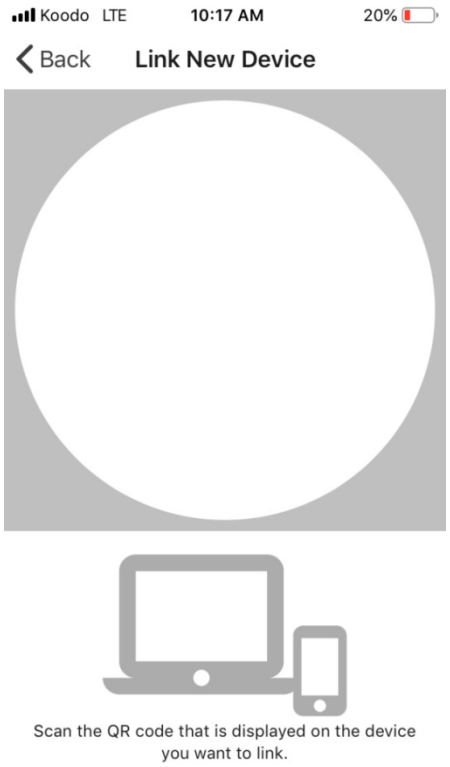


Click Here

Wade is an unverified user and needs to be verified

In the ‘verify safety window’, while Wade has phone open, click/touch the QR Code

After touching the QR code, this will appear



Hold the circle over your new contacts phone and scan the QR code that appears on his phone under your contact name; this is the first way to verify by linking the devices

The second way is to ask your contact to open your contact on his Signal App, touch his QR code and scan the QR code I have open.

This will verify the contacts on both phones

Step Six: Set Disappearing Text for 1 Day (24 hours)

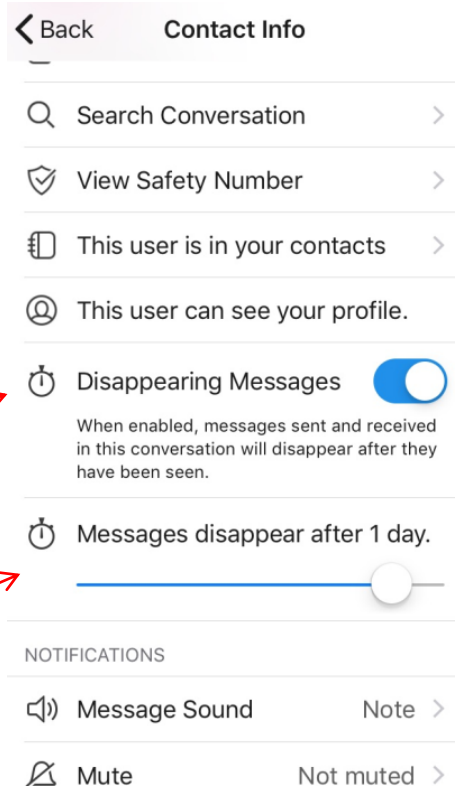
Go to your contact list

Open the message window by touching the ‘pencil’

Touch on the contact’s name at the top of the page to open the person/contact settings page

Turn on disappearing messages

Move the ‘bar’ to one day



Your responsibility

A picture is worth a thousand words, efficiency and convenience make more time for patient contact….

But…

Secure text messaging only, keep your patients' information on a need to know basis, and, communicate your texting discussion by writing a progress note

QUESTIONS?

April Mills, Clinical Informatics Lead
jeamills@ihis.org

Dr. Spencer Brown , Chief Medical Information Officer swbrown@ihis.org