Securing Your Mobile Device:

Mobile health apps on your phone provide access to confidential information about you and your medical history. While OTN has gone to great lengths to secure access to your data in the cloud, there are several security best practices that you are encouraged to follow when using the Mobile Apps.

Smartphones, tablets and other mobile devices have become common in many home care settings. Due to their small size, portability and "always-on" connectivity, mobile devices are ideal for health monitoring and reporting purposes. However, the same characteristics, that make handheld devices so convenient and easy to use, introduce additional risk concerns. For example, a smartphone can be easily lost or misplaced and end up in the wrong hands. Unless properly secured, the personal information stored on the phone will be available to anyone who comes in contact with the phone.

Here are some tips to keep your mobile device safe and secure:

- **Guard your device as you would a wallet – do not leave it unattended at any time and keep it locked and out of sight when not using it.**

Think of the mobile device and protect it the same way you would your wallet. Leaving it unattended and in plain sight will attract potential thieves and opportunists with a readily available target. Whenever finished using the mobile device keep it in your pocket or otherwise lock it in a drawer or a safe.

- **Create a strong password.**

Although swipe patterns provide a level of security, greasy finger-trails could reveal too much. Similarly, a four-digit PIN can be easily guessed. A strong password is the ideal phone protection. Choose a password that is a mix of letters (both upper and lower case), numbers, and symbols and is at least eight characters in length. Don't use common words, birthdays, kids' or pets' names, or anything else easily guessed.

- **Use your device's auto-lock feature.**

You can set the length of time after which the device will lock itself and require a password to unlock. Five minutes or less is a good estimate, even if it may feel slightly inconvenient.

- **Do not share your device with others.**

Your device stores personal and confidential information that requires privacy protection. As such, you should not share your device with any parties that would not be, otherwise, authorized to view the data.

- **Do not "jailbreak" or "root" your device.**

These are terms for overriding software and security protections on your device. Some users do this to install apps or extensions that are not legally available through the manufacturer. Doing so, leaves the device more vulnerable to attacks and compromises.

- **Use only secure and trusted connections when performing sensitive transactions.**

Avoid using your mobile devices for sensitive transactions unless you are using a secure Wi-Fi connection. Secure connections begin with "https" rather than just "http".

- **Be aware of your surroundings.**

Do not perform sensitive tasks in public areas, such as airports, coffee shops or business lounges where there is opportunity for strangers to see over your shoulder or eavesdrop on the conversations.

- **Delete emails, images, documents and other content when no longer needed.**

In case of a mobile device theft or loss, these items will be potentially accessible to anyone capable of bypassing the device's security mechanism. To prevent unauthorized disclosure of sensitive information, mobile devices should not be used to store personal or private information.

- **Keep your mobile device up to date.**

In order to take advantage of the latest security features, set your phone to automatically update its operating system and security software. Ensure that the updates are received from legitimate and authorized source (e.g. Google Play or iTunes Apple App Store).

- **Check App Permissions.**

Whenever an App is installed it has to ask the user for "permission" to use specific features of the phone. Consider whether you want that app to have access to your information.

- **Be aware of "Phishing" Emails or Texts.**

If you get an email or text message that asks you for private information such as usernames, passwords, address details or credit card information, it is likely a "phishing" attempt. Most reputable companies, including OTN and Vivify Health, will never ask you to disclose personal information via an email or text message.

- **Approach Links in Email Messages with Caution.**

Links in email messages can often take you to fake sites that encourage you to provide personal information or infect your computer when clicked.
Before you click a link, make sure to read the target address by hovering your mouse pointer over the link. If the target is different from the displayed text, DO NOT CLICK ON THE LINK!

Example:

- **Do Not Open Attachments from Unknown or Unexpected Senders.**

Attachments might be malware that downloads to your machine when you open the file. If you don't know who the attachment is from, or if you weren't expecting it, DO NOT OPEN THE FILE!

- **Install/Enable anti-virus software on your device.**

Anti-virus software provides a layer of protection against known threats. Having an up-to-date anti-virus software will protect your device from new and diverse threats that emerge regularly.

- **Download apps only from reputable sources.**

Trojans, viruses, and fraudulent apps all present a risk. To avoid them, download apps only from trusted, authorized app stores like iTunes or Google Play

- **Enable remote wiping.**

If your phone is lost or stolen, you'll be able to wipe all of its data remotely. Deleting the data will prevent strangers from accessing it.

- **Encrypt your device.**

If it's not already the default, consider encrypting the data on your device.

- **Report loss or theft of your mobile device immediately!**

If you have lost your mobile device, report it immediately to your Care Team.