PCAP Smart Phone & Electronic Device Security Recommendations

Always superseded by host agency policies

Employee education:

Smart phones and tablets are actually computers, sometimes with more power and storage capacity than many laptops. Because they go with you, they are easy to misplace or steal. It is up to you to protect client information by thinking about four areas: 1) access, 2) storage*,* 3) transmission, and 4) acting responsibly.

1. ACCESS: Device security

Password protect your phone. Use a screen lock that requires a password or code to be entered after being left idle for 2 minutes or more. Use the most rigorous method available to you. It is best to change the default 4-digit passcode to a longer 6- or 8-digit passcode, or use an alphanumeric password. Do not use the default password provided by the phone or voicemail service. Change your password regularly.

When possible use encryption. Encrypting your data makes the information unreadable—in essence, useless—even if a hacker gets through the lock screen. For iPhone (iOS 8 and above) and Android phones using Google's Android 5.0 (Lollipop) and above, encryption is built into the phone and tied to the passcode (you may have to enable encryption on your Android device). For both types of phones, encryption is only as secure as your passcode: the more complex the passcode, the harder the encryption is to crack. Note that the phone's built-in encryption system will only protect files/data stored in the /data partition on the phone; it does not protect files and photos stored on an SD card.

Report loss or theft promptly. Any loss or theft of the phone or mobile device must be reported to your supervisor within 24 hours, sooner if possible. Because your phone or mobile device's data may be wiped (destroyed) by network support in the event of loss or theft, do not store anything on the phone or mobile device that is not duplicated elsewhere.

2. STORAGE: What can, and cannot, be stored on your PCAP phone

Be selective in what content you place on the phone. Smart phones have many useful apps that may enhance work with clients, and safety of advocates. Example: Apps such as "Find my Friends" (Apple) or "Locate my Friends” (Android) with advocate locations turned on can allow supervisors to know where advocates are at all times, and in case of emergency can help locate them. But many other apps may have malware or phishing code built into them designed to strip information from your phone and sent to the developer without your knowledge. Sites should develop lists of approved apps and protocols. Do not download apps that are not approved.

Do not store any personally identifiable client information on your phone. This includes names and addresses. Suggestion: Use a 3-digit code to identify clients. This risk may be ameliorated by a secure encryption method. Always err on the side of protecting client's identity and location information.

Be mindful that the GPS feature stores locations. Locations are automatically stored unless you turn this feature off (some phones don't allow this and on some it doesn't always stay off). Check periodically and remove locations that are stored. (See appendix for instructions.)

3. TRANSMISSION: Secure wireless connections

Connect only to secure private networks that are password protected. Do not access sensitive information from an open network such as that found at Starbucks, McDonalds, etc. Note that if you store sensitive information on your phone and you access an open network, a hacker with the right software can strip the contents of your phone. Be sure that your home network router is password protected and is not using the default password provided by the router manufacturer.

Turn automatic connect off. Switch off the feature that allows your phone to connect to any available WiFi connection automatically so that your phone does not connect with an unsecure network without your knowledge. Check periodically. Doing this will also enhance battery life.

Turn Bluetooth off. Switch this feature off unless in use to protect yourself from hackers. Check periodically.

4. ACT RESPONSIBLY

Do not leave your phone unattended.

Restrict client's use of your phone. At the site's discretion clients may (or may not) be allowed to use the advocate's smart phone. Sites should set policy. For example: client access to the phone should be under the advocate's direct supervision and include phone use only, no checking texts, email or internet. No children should be allowed to use the phone; do not download children's apps.

Do not allow phone to "remember" passwords. If you are using the phone to access any kind of account requiring a log-in, do not store the password: log in every time. Many sites will not allow work email to be accessed from a smart phone, check your agency's policy.

Do not store pictures and videos. Check with your agency's policy, remember that taking pictures of client or client's children may require a signed release. Once sent to clients, pictures should not be stored on phone. Do not store pictures of yourself on phone.

Facetime (on iPhone) or Skype: These apps do not record the video and are much the same as an audio call. (Note: count as electronic, not face contact, on time summary.) Wipe the history of the phone numbers called if you use it.

Recording apps are not secure. Smart phones come with the ability to make audio recordings and then convert them into text. While it may be tempting to dictate a note and then email it to yourself, consider the content of what you are sending into "the cloud" to be transcribed and stored. These apps are not secure.

Perform "security maintenance" routinely. Remove past locations and browser histories, etc. See Appendix.

Do not conduct any personal business on a PCAP phone. Do not shop through the browser, browse your personal Facebook account, access your bank account, etc.

Using your own personal phone or device: Unless authorized by your host agency, no PCAP client data should be on your personal phone or mobile device. This includes email, client contact information, and databases access through applications or web browsers (i.e., DatStat). Do not browse any client related content (e.g., Facebook) from your personal device, especially not from your personal Facebook page.

Do not access DatStat from any smart phone.

Appendix:

To clear location history from the iPhone, go to:

Settings ➔ tap Privacy ➔ tap Location Services ➔ tap System Services ➔ tap Frequent locations

Tap "Clear History..." at bottom of Frequent Locations screen to clear your locations. You can also tap the Frequent Locations switch to move it to the off position and prevent further data logging.

> *More detail:*
>
> The **Location Services** menu details all the apps that currently use GPS and Wi-Fi to establish your location. You can turn permissions on and off for each of the apps here. (Frequent Locations is at the bottom of the first list.)
>
> The **System Services** menu contains all the finer details of location data, and you can toggle the switches (permissions to use Locations) for each of the functions listed as you wish.
>
> The **Frequent Locations** menu will show all your frequent locations listed at the bottom of the screen. If you tap the arrow next to any item on the list you can see it plotted on a map. The map goes into detail, letting you select any location to see how many times you have been there, and for how long, including dates and times. This could allow someone to retrace your steps. It is from here that you clear your history, by clicking on "Clear History..."

To delete previous searches in the Maps app for iPhone and iPad:

1) Launch the Maps app on your iPhone or iPad.
2) Tap in the search field.
3) Tap on Favorites.
4) Tap on Recents in the bottom navigation.
5) Tap on Clear in the upper left hand corner.
6) Tap on Clear All Recents in the popup menu.

To delete Locations on an Android device:

1) Depending on your device, find Google settings in a separate app called Google Settings, or in your main Settings app, scroll down and tap Google.
2) Touch Location > Location History.
3) At the bottom of the screen, touch Delete Location History.

To delete a place from your Maps history on an Android device:

1) Open the Google Maps app and sign in.
2) Tap the side menu > Settings > Maps history.
3) Tap the X next to the entry you want to delete, and then tap Delete.