Parent-Child Assistance Program (PCAP)
UNIVERSITY OF WASHINGTON ADDICTION, DRUG & ALCOHOL INSTITUTE
SEATTLE, WASHINGTON (206) 543-7155
http://pcap.psychiatry.uw.edu/

PCAP Client Confidentiality Protocol

CONFIDENTIALITY BASICS

PCAP client confidentiality requirements are outlined in our DBHR contracts (Exhibit A – Confidential Information Security Requirements) and mandated by IRB, 42 CFR Part 2, and HIPAA.

Confidentiality is paramount to the safety of PCAP clients and to the reputation of PCAP in the community. This is why PCAP has security protocols in place, including but not limited to:

- Using ROIs that are 42 CFR Part 2 compliant;
- Using an encrypted, HIPAA-compliant database program for storing PCAP data;
- Having a federal Certificate of Confidentiality to protect research subjects identities;
- Storing the Client Tracing Access Database on an encrypted/password-protected thumb drive that is kept in a secured, locked location when not in use, and only accessible by the supervisor and office assistant;
- Storing client files in locking file cabinets and never removing them from the office; and
- Using secure electronic means of transmitting confidential information (see below).

WORKING IN THE FIELD OR FROM HOME

- PCAP paperwork with Personally Identifiable Information (PII - names, addresses, phone numbers, etc.) or Protected Health Information (PHI – SUD treatment, pregnancy and health history, etc.) should never be removed from the office. PII/PHI must be kept secure by storing it in locking file cabinets in the office with doors locked.
- PCAP work products generated in the field or at home must be taken into the office for secure storage at your earliest convenience.
- While working from home, PCAP paper and electronic work products must be kept secure, never allowing access to others in the home.
- Keep in mind potential risks to client privacy. Skype, Facebook, and FaceTime are not secure or private means of communication. We recommend ensuring any technology platform being used is end-to-end encrypted such as Zoom, Signal, WhatsApp, Viber, and iMessage.

SECURE ELECTRONIC TRANSMISSION OF CONFIDENTIAL INFORMATION

EMAIL. Emailing <u>unencrypted</u> information via email is not secure. PCAP staff should **never** send personally identifiable information (PII) (i.e., names, birthdates, addresses, phone numbers, email addresses) or protected health information (PHI) or about a client via email, either in the body of the email itself or in an attachment, unless the attachment is encrypted (i.e., password-protected). If there is a need to send PHI electronically, always encrypt the document before sending.

Emailing encrypted information as an email attachment is secure*. It is the most secure way to electronically transmit PII/PHI. To read an encrypted email attachment, the email recipient must be given a password that enables them to decrypt it (the password must be given separately from the encrypted attachment). The following websites provide some guidance for encrypting a document and opening an encrypted document:*

- Encrypting WORD documents: https://support.office.com/en-us/article/protect-a-document-with-a-password-05084cc3-300d-4c1a-8416-38d3e37d6826
- Encrypting PDF documents: https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html

When emailing confidential information, PCAP staff should follow these basic instructions:

- **Never send confidential information in the body of an email.**
- Type the confidential information into a document and encrypt it before attaching it to an email.
- Before sending the email and attachment, call the intended recipient with the password or send it to them by text.
- If a client or provider sends an email to a PCAP staff member containing PHI, the PCAP staff member should always remove the confidential information before sending a reply.
- We recommend including the following statement or one like it in your email signature footer:

Because e-mail is not secure, confidentiality cannot be guaranteed. Never include personally identifiable client information in an email or unencrypted attachment.

FAX. Faxing is secure only if the sender is certain they have the correct fax number; before sending, confirm with the recipient that they will be physically present to receive the fax (so that it doesn't fall into the wrong hands).

SECURE TEXTING AND VIDEO CHATS

PCAP staff should maintain a quiet, private environment while video chatting with clients. Always practice professional demeanor and good work-at-home habits that protect clients' confidentiality.

Text or video chat applications**.** Look for and use applications that employ secure, end-to-end encryption. This means the text cannot be read at any point between sender and receiver, especially important when discussing sensitive issues electronically. Apps with end-to-end encryption include Zoom, Signal, WhatsApp, and Viber. If both people have Apple products, iMessage and FaceTime is secure. Note that Facebook messenger does not employ encryption unless one selects the "Secret Message" option.

> ***Note:*** *A 3.17.20 federal DSSH notification stated:* ***"Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth".*** *While PCAP does not provide medical or mental telehealth services, we should still heed this warning.*

SECURE ZOOM MEETINGS

The free version and paid versions of Zoom are both secure and encrypted. Therefore, PCAP staff may use Zoom for supervision, staff meetings, and video conversations with clients and providers.

Always keep your Zoom application up to date. For Zoom information and tutorials: https://support.zoom.us/hc/en-us/articles/206618765-Zoom-Video-Tutorials

Security issues with video conferencing. In using Zoom or other video conferencing, there are the same risks as for any e-communication, or anything going over the internet. Be alert and aware, and if you have concerns about something risky happening on a video conference, close the app and do not proceed. There are hacker risks (more of a concern for businesses), risks of downloading a virus with the app (use reliable app download), and (more important to us) risks that you cannot fully assess "the room" (i.e., may not be able to see who else is there).

Advanced Security controls for Zoom video meetings

- Generate a new, unique Zoom meeting ID for each Zoom meeting (do not use your personal Zoom meeting ID code)
- Set up a password that the meeting participants will need in order to connect to the meeting.
- Enable the 'Waiting Room' function so that the participants cannot enter the meeting without you admitting her.
- Disable the 'Share Screen', 'White Board', and 'Recording' functions.
- Close the app fully when done.