HIPAA Compliance

Cell Phones & Computers

1. Both of these must have high security passcode protection, because if someone stole your phone or computer then we need to prove that we tried to our best intentions to protect client information.
2. HIPAA Password Protection: Standard best practice requires at least 8-10 characters, including symbols, numbers, uppercase and lowercase letters.
3. Only use secure Wi-Fi Networks: **Free Public Networks are not secure. Don't access client information at a coffee shop!**

Google Suite emails

1. HIPAA Compliance
    a. G Suite is HIPAA compliant only within G Suite to other colleagues using a Lacamas Counseling email
    b. G Suite is not HIPAA compliant is you send an email outside of G Suite to Lacamas Counseling
2. Add Notice of Confidentiality to your email signatures
    a. *Notice of confidentiality: This email may contain information that is protected by Federal Confidentiality laws (42CFR, Part 2). It is intended only for the individual(s) above-named, and the privileges are not waived by virtue of this having been sent by email. If the reader of the email is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of the communication is strictly prohibited. If you have received this communication in error, please immediately notify the sender by phone and delete this message.*
    b. Notice of Confidentiality does not completely cover HIPAA guidance rules for sending client protected information. It is a step to add additional coverage and offers limited protection in case of accidental breach of information.
3. Google Chat
    a. HIPAA compliant if chatting within Lacamas Counseling G Suite to other colleagues with a Lacamas Counseling email

Simple Practice Secure Messaging –

1. This is secure and HIPAA protected. Email clients through Simple Practice when possible (instead of through your Lacamas Counseling email)
2. Secure Messaging
    a. https://support.simplepractice.com/hc/en-us/articles/115003629583-Getting-started-with-Secure-Messaging
    b. Set up Secure Messaging in Simple Practice
        i. Select Settings
        ii. Select Secure Messaging
        iii. Switch the toggle to On to enable Secure Messaging between you and your Clients
        iv. Activate Secure Messaging with each client

1. Update each individual Client Record
    a. Edit Client Record
    b. Select Client Portal Tab
    c. Check box “Use Secure Messaging
2. Send Secure Message
    a. Select New Message
    b. Search for Client Name
    c. Select “Enable” to activate secure messaging

3. Invoicing
    a. HIPAA compliant through Simple Practice
4. Payments
    a. HIPAA compliant through Simple Practice
    b. Paypal, Venmo, Quick Books – are not HIPAA compliant for payment processing

Log all Record Requests

1. Keep a log of all client record requests including
    a. Date of the request
    b. Date of your response
    c. Nature of your response (e.g. provided three pages of records in paper format).

Computer and Phone Updates - Maintain Recommended Software and System Updates

1. Operating system and browser updates often include security patches, new security features, and privacy measures. If you have a security flaw in your browser or operating system all the data on your computer then all the data you access on the internet is at risk. This includes both files you may have stored on your computer as well as any PHI you access via the internet like an electronic health record (EHR)
2. Use Firefox, Chrome, or Safari browsers
    a. Don’t use Internet Explorer – major websites have stopped supporting this browser