**Telecounseling and HIPAA**

Protected Health Information (PHI) subject to the restrictions of HIPAA Privacy Rule include:

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

*Limit PHI to what is therapeutically necessary*

*Consult with administrators and technical support specialists*

*Confirm client identity and location at the beginning of every session*

**Devices**

* Computer
	+ Laptop or desktop
	+ Should be password-protected
	+ Hard drive should be encrypted (if storing any PHI on the computer itself)
	+ Avoid networking to other computers and sharing devices as much as possible
	+ Ensure updated and active virus protection
* Telephone/tablet
	+ Must be encrypted; apple products are already encrypted
	+ Enable 6-digit password instead of a 4-digit password (even if you use face or fingerprint ID)
	+ Landlines are secure (ensure it is not a digital phone marketed as a landline)

**Communication**

* Encrypted email
	+ HIPAA Standard: 256-bit end-to-end encryption
	+ Automatic reply that indicates:
		- Will respond within 8 business hours
		- Contact 911 (or other designated resource) for emergencies
* Telephone
	+ Do not need BAA due to conduit exception
	+ Use business phone number (no personal phone numbers)
	+ Confirm client identity (code word)
	+ Do not confirm a student/client is in services if someone reaches out to you
	+ Leave minimum necessary information via voicemail
* No texting
	+ Will return a text message with a phone call or email
* Mail
	+ Try to avoid indicating it is from a mental health professional
	+ Make your return address just your last name and the street address
* Secure Messaging
	+ Electronic Health Record (EHR) Platform with a Business Associate Agreement (BAA)
	+ HIPAA-compliant apps

**Telecounseling Platform**

* Audio
	+ Password-protected, encrypted cellphone
	+ Landline (not digital)
	+ BAA not needed due to conduit exception
* Video
	+ HIPAA-compliant Platform (e.g., SimplePractice, Doxy.me, Spruce)
	+ Business Associate Agreement (BAA) required
* Internet Access
	+ Cellular data is secure
	+ Ethernet cable is secure
	+ Wifi from a personal, password-protected router
	+ Use VPN on public wireless networks (e.g., hotels, fast food)
		- Purchase from internet provider
		- Purchase online
	+ BAA not needed for internet provider due to conduit exception

**Storage**

* BAA for cloud storage and EHR platforms
* External hard drive/jump drive should be password-protected and encrypted
* Lock external hard drive/jump drive in cabinet or lock box
* Lock paper files in cabinet or lock box
* Paper files should not leave the field placement site
* Keep secure backup copies of data

**Client Responsibilities**

* Password protect computers/phones/tablets; do not share passwords or devices
* Encrypt phones and tablets and any device where PHI is stored
* Encrypt email
* Use Ethernet cable, personal password-protected wifi, cellular data, or a VPN