TELEMENTAL HEALTH SERVICES: STUDENT PRIVACY & CONSENT

California Community Colleges HEALTH & WELLNESS

The "Telemental Health Services" series explores the telemental health model, student privacy and consent concerns, technology and set-up, telemental health training options, telemental health in rural communities, and crisis response. Each guide includes practical tips, best practices, and information that is specific to the California Community Colleges setting.

This brief was developed as a series to help California community colleges implement telemental health (TMH) services within the context of COVID-19.

WHAT DO COLLEGES NEED TO KNOW ABOUT INFORMED CONSENT?

It's important to get informed consent from students when providing behavioral health services, and there are specific requirements for TMH. Your college may already have informed consent forms or procedures in place, but be aware that the California Board of Behavioral Sciences (BBS) has outlined required actions that service providers must complete when practicing TMH.

Below are the BBS-required actions as well as recommended or best-practice actions for getting student consent. The California Association of Marriage and Family Therapists created a helpful Checklist that providers can use to ensure that they're following BBS protocols with each client.

BBS-Required One-Time Actions must be done upon initiation of telehealth services. This information can be provided in an informed consent form. For an example, see Appendix A (pgs. 46-47) of College Counseling from a Distance: Deciding Whether and When to Engage in Telemental Health Services. Your college's Risk Management or legal department can review these forms.

- Obtaining consent involves informing the student about the use of telehealth, obtaining their verbal or written consent to receive telehealth services, and documenting their consent in their treatment record. Verbal consent is appropriate and accepted current practice, given the limitations of paperwork signed during the COVID-19 pandemic.
- It is important to disclose risks and limitations of telehealth, such as technical failure, unauthorized access to confidential information, or possibility of other individuals overhearing the session.
- BBS also requires that you provide your license or registration number and type.
- Additionally, it is helpful to provide contact information of resources in the student's area, including emergency services.

Recommended One-Time Actions:

- If by phone: you might explain that you will contact the student if the connection is lost, to avoid a busy signal if both parties attempt to contact each other at the same time.
- It is helpful to establish a safe word the student can use if they need to disconnect from telehealth for safety or privacy reasons without people in their immediate vicinity knowing.
- You might encourage the student to create an environment of uninterrupted privacy; e.g., schedule childcare, place a "do not disturb" sign on the door.

BBS-Required Actions for Each Session:

- It is important to verbally obtain and document the student's full name and the address of their current location. This step helps reduce the risk of impersonation, and it is useful in case of emergency.
- It is also important to assess whether telehealth services are, or continue to be, appropriate for the student's needs.
- Industry best practices can help to maintain student confidentiality and privacy of the communication. Appropriate technology will be covered in more detail in another part of this series.

Recommended Actions for Each Session:

- You might state that you will not record the session and ask that the student not record the session without informing you.
- At the beginning of each session, you might ask where the student is geographically located, as this information is critical to the provision of emergency support services.

- You can confirm a way to reach the student if you are disconnected; an emergency contact for the student; and if anyone else is in the room or house/apartment with the student. These actions can help maintain their privacy as well as their safety in a crisis.
- It may be necessary to explain that you only provide telehealth to clients in California and will refer students to resources in other states as needed if they travel outside of California.

WHAT DO COLLEGES NEED TO KNOW ABOUT STUDENT PRIVACY AND CONFIDENTIALITY?

Colleges are expected to uphold the same standard for protecting students' privacy in TMH service delivery that they have when delivering face-to-face services. Depending on how your college creates, maintains, and transmits patient information, your TMH services may be regulated by federal and/or state laws such as FERPA, HIPAA, HITECH, or the California Confidentiality of Medical Information Act (see Appendix). In general, health services that the college provides to students are usually covered by FERPA rather than HIPAA, but state laws may supersede federal laws where they provide more protections. **You might want to check with your college's legal department about which laws apply to your health or counseling center.**

The technology fact sheet in this series (Part 4) gives more detail about digital tools that protect student privacy and confidentiality. There are many video chat services colleges can use to provide TMH that are HIPAA- and/or FERPA-compliant (e.g., Zoom for Healthcare, Skype for Business). Importantly, the California Community Colleges Chancellor's Office has subscribed all colleges to have access to Cranium Café powered by ConexED, which is FERPA-compliant. During the COVID-19 emergency, the federal government temporarily allowed providers to use some non-HIPAA compliant video chat services that are not public-facing, such as Apple FaceTime or Skype, in good faith provision of telehealth services (learn more). Public-facing services such as TikTok or Facebook Live still may not be used.

APPENDIX: QUICK GLOSSARY[1]

Please note that these descriptions are provided for informational reference only. This is not an exhaustive list, and not all laws may apply to your college. Please confirm with your legal department which law(s) apply to your telehealth services.

FERPA: Family Educational Rights and Privacy Act. FERPA applies to all education agencies and institutions that receive funding from the U.S. Department of Education, which includes most public and private colleges. FERPA defines two types of student records: education records and treatment records. Treatment records are health and medical records (including mental health) that are made, maintained, and used only in connection to student treatment and are disclosed only with providers of that treatment.

HIPAA: Health Information Portability and Accountability Act. HIPAA applies to "covered entities": health plans, health care clearinghouses, and health care providers who transmit PHI in connection with covered transactions (e.g., billing). It's up to the covered entity to ensure that data storage, encryption, and transmission programs are secure and HIPAA-compliant. Many counseling centers do not fall under HIPAA because they do not engage in covered transactions. In addition, even if a school is a HIPAA covered entity, records that are covered by FERPA are specifically excluded from HIPAA.

The ***HITECH (Health Information Technology for Economic Clinical Health) Act*** builds on HIPAA consumer protections around the use of technology. HITECH is designed to encourage the use of electronic health records, and it strengthens HIPAA rules and enforcement related to privacy and security.

California's Confidentiality of Medical Information Act (CMIA) puts in place more stringent regulations and compliance penalties than HIPAA. It extends the definition of health care provider, and creates more prohibitions around how health care providers can use or disclose records without written authorization from the patient.

California's Confidential Health Information Act amends CMIA to provide additional protections for individuals who are not the insurance policy holder, such as young adults covered by a parent's policy. The Confidential Health Information Act is specific to insurers, and it allows individuals to request that communications about "sensitive services" (such as mental health counseling) be kept confidential from the policy holder.

California Community Colleges Health & Wellness | www.cccstudentmentalhealth.org

Publication Date: May 2020. Revised June 2021. CCC Health & Wellness is a program of the California Community Colleges Chancellor's Office (CCCCO).

The "Telemental Health Services" series explores the telemental health model, student privacy and consent concerns, technology and set-up, telemental health training options, telemental health in rural communities, and crisis response. The impetus for these resources was a telehealth discussion through CCC Mental Health and Wellness Association (MHWA) listserv, which CCC Health & Wellness explored and drew from while developing these guides. Each guide includes practical tips, best practices, and information that is specific to the California Community College setting and the COVID-19 context.

[1]For more information, see pages 24-25 of College Counseling from a Distance and the California School-Based Health Alliance's fact sheet, HIPAA, FERPA, Both, or Neither? A Flowchart for Decision-Making.