Oregon TECH
Integrated Student Health Center

(Mark One) I am enrolled at the:
☐ Klamath Falls Campus
☐ Portland Metro Campus

Telehealth Informed Consent (Video Conferencing)

Introduction of Telehealth: Telehealth is the delivery of mental health support services using video or audio technologies between a provider and a client who are not in the same physical location.

Software Security Protocols: Electronic systems used will incorporate network and software security protocols to protect the privacy and security of health information and imaging data, and will include measures to safeguard the data to ensure its integrity against intentional or unintentional corruption. ISHC is utilizing a HIPAA-compliant license for Zoom (see attached) in order to minimize these risks to the best of their ability.

Technology Backup: In the event of disruption of service, or for routine or administrative reasons, it may be necessary to communicate by other means. If the video technology is not working, my provider will call me on the telephone number that I have provided here: _____

Self-Termination: I may decline any telehealth services at any time without jeopardizing my access to future care, services, or academic standing.

Modification Plan: My provider and I will regularly reassess the appropriateness of continuing to deliver services to me through the use of telehealth and modify our plan as needed.

Provider Communication: My provider may utilize alternative means of communication as follows:

- S/he may send me a secure message through the ISHC Student Health Portal
- I may be contacted by ISHC staff regarding coordination of appointments
- If I have questions or need to contact my provider, I will call 541-885-1800 (Klamath Falls students) or 503-821-1313 (Portland Metro students) and they will act as the liaison.

Confidentiality: It is my responsibility to maintain privacy on the client end of communication. The extent of confidentiality and the exceptions to confidentiality that are outlined in the ISHC Informed Consent still apply to telehealth. Please speak with your provider about questions regarding confidentiality.

Documentation:

- My session with my telehealth provider will not be recorded.
- Documentation (i.e. chart notes) will be stored on the private server of the ISHC electronic medical records software, Point and Click Solutions.

Laws & Standards: The laws and professional standards that apply to in-person behavioral services also apply to telehealth services. This document does not replace other agreements or documentation of informed consent.

Emergencies:
Assessing and evaluating threats and other emergencies can be more difficult when conducting telehealth than in traditional in-person therapy. Should your counselor believe that you are in crisis, they will take steps to establish support for you in your location. By providing the contact information below, you are authorizing ISHC to contact this person in the event of a crisis. If you are in need of immediate and urgent assistance go to your nearest emergency room; you can also call the suicide hotline at 800-273-8255 or text HOME to 741741.

Emergency Contact Name: _____ Relationship to You: _____

Cell Phone Number: _____ Other Phone Number: _____

I have read and understood this information. I hereby give informed consent to use telehealth in my mental health care.

_____ _____
Signature of Client Date

zoom

HIPAA COMPLIANCE GUIDE

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) lays out privacy and security standards that protect the confidentiality of patient health information. In terms of video conferencing, the solution and security architecture must provide end-to-end encryption and meeting access controls so data in transit cannot be intercepted.

The general requirements of HIPAA Security Standards state that covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably-anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably-anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
4. Ensure compliance by its workforce.

How Zoom Enables HIPAA Compliance

We sign the HIPAA Business Associate Agreement (BAA) for our healthcare customers (minimum $200), meaning we are responsible for keeping your patient information secure and reporting security breaches involving personal healthcare information. **We do not have access to identifiable health information** and **we protect and encrypt all audio, video, and screen sharing data.**

The following table demonstrates how Zoom supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).

HIPAA Standard	How Zoom Supports the Standard
Access Control: • Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs. • Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity. • Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency. • Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. • Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	• Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 256-bit key generated and securely distributed to all participants at the start of each session. • Multi-layered access control for owner, admin, and members. • Web and application access are protected by verified email address and password. • Meeting access is password protected. • Meetings are not listed publicly. • Zoom leverages a redundant and distributed architecture to offer a high level of availability and redundancy. In addition, Zoom regularly performs snapshots of our data and can quickly assist the customer with data restoration and access to their data kept in Zoom's cloud. • Meeting host can easily disconnect attendees or terminate sessions in progress. • Host can lock a meeting in progress • Meeting ends automatically with timeouts.
Audit Controls: • Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• Meeting connections traverse Zoom's secured and distributed infrastructure. • Meeting connections are logged for audio and quality-of-service purposes. • Account admins have secured access to meeting management and reports.

Integrity: • Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Multi-layer integrity protection is designed to protect both data and service layers. • Controls are in place and protect data in-motion and at-rest.
Integrity Mechanism: • Mechanism to authenticate electronic protected health information. • Implement methods to corroborate that information has not been destroyed or altered.	• Application executables are digitally signed. • Data transmission is protected using HMAC-SHA-256 message authentication codes.
Person or Entity Authentication: • Verify that the person or entity seeking access is the one claimed.	• Web and application access are protected by verified email and password. • Meeting host must log in to Zoom using a unique email address and account password. • Access to desktop or window for screen sharing is under the host's control.
Transmission Security: • Protect electronic health information that is being transmitted over a network. • Integrity controls: Ensure that protected health information is not improperly modified without detection. • Encryption: Encrypt protected health information.	• End-to-end data security protects against passive and active attacks on confidentiality. • Data transmission is protected using HMAC-SHA-256 message authentication codes. • Meeting data transmitted across the network is protected using a unique Advanced Encryption Standard (AES) with a 256-bit key generated and securely distributed to all participants at the start of each session.

Security and Encryption

Only members invited by account administrators can host Zoom meetings in accounts with multiple members. The host controls meeting attendance through the use of meeting IDs and passwords. Each meeting has only one host unless a co-host is purposefully added by the host. The host can

screen share or lock screen sharing. The host has complete control of the meeting and meeting attendees, with features such as lock meeting, expel attendees, mute/unmute all, lock screen sharing, and end meeting.

Zoom employs industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings. Zoom encryption fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.

Screen Sharing in Healthcare

Medical professionals and authorized healthcare partners can use Zoom to meet with patients and other healthcare professionals to screen-share health records and other resources. Zoom does not distribute the actual patient data. Screen sharing transmits encrypted screen capture along with mouse and keyboard strokes only, not the actual data. Zoom further protects data confidentiality through a combination of encryption, strong access control, and other protection methods.

HIPAA Certification

Currently, the agencies that certify health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Security Rule), nor accredit independent agencies to do HIPAA certifications. Additionally, the HITECH Act only provides for testing and certification of Electronic Health Records (EHR) programs and modules. Thus, as Zoom is not an EHR software or module, our type of technology is not certifiable by these unregulated agencies.

Other Security Certifications

SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.

TRUSTe:

TRUSTe has certified the privacy practices and statements for Zoom and also will act as dispute resolution provider for privacy complaints. Zoom is committed to respecting your privacy. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

EU-US Privacy Shield:

Zoom participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Zoom has committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List https://www.privacyshield.gov/list.