

Wyoming Telehealth Network Zoom License Policies

Effective Date: July 1, 2026

Last Updated June 30, 2026

Introduction

The Wyoming Telehealth Network (WyTN) supports direct service providers with a free, HIPAA compliant Zoom license that enables their use of telehealth services. As the host of nearly 2,000 Zoom licenses, our goal is to ensure our expanding state-wide network has consistent access to secure and reliable services. Given the ever-changing technological landscape, in order to meet this goal, we must work together to practice good cyber-hygiene, and data keeping practices. This updated policy document reflects changes that will help our network remain HIPAA compliant, secure, and ensure WyTN's records are current and accurate. By agreeing to join the WyTN Zoom account, you agree to these policies and procedures.

HIPAA Compliance

Each provider/entity must establish telehealth-specific internal policies and procedures to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA). Below is list of HIPAA compliance best practices for providers:

1. Ensure you are in a secure private location during all telehealth visits.
2. Verify your patient's identity at the start of your telehealth encounter.
 - a. Can use traditional methods (DOB, Last 4 SSN) or new techniques provided through secure systems.
3. Use encrypted, HIPAA compliant messaging services to communicate and share information with your patient.
 - a. SMS/MMS messages are not HIPAA compliant.
4. If your patient is not in a private location, confirm they are aware of the risk of sharing personal health information (PHI) and obtain verbal consent.
5. If you are using an artificial intelligence (AI) note-taking device/tool – ensure it is HIPAA compliant.
 - a. Obtain consent to use the HIPAA compliant tool from the patient.
 - b. The HIPAA complaint AI tool should be disabled at the patient's request, even if consent was provided previously.

6. If your patient wishes to use an AI note-taking device/tool, ensure they are aware of the risk of PHI breach when using a non-HIPAA compliant AI program.

Below are links to trusted resources regarding HIPAA compliance best practices.

United States Department of Health and Human Services

- [HIPAA and Telehealth](#)
- [Resource for Health Care Providers on Educating Patients about Privacy and Security Risks](#)

The HIPAA Journal

- [HIPAA Guidelines on Telemedicine](#)

Telehealth.org

- [Mastering AI Documentation in Telehealth: 5 Must-Know Tips for Clinicians](#)

Security Best Practices

Good cyber-hygiene is essential to ensure your Zoom account stays secure, and your telehealth services remain uninterrupted. These policies go hand-in-hand with good HIPAA compliance practices, and should be treated with the same level of diligence.

1. Your Zoom account should have a unique password that is between 12 and 16 characters long. Include:
 - a. Upper and lowercase letters, numbers, and characters.
 - b. Aim for randomness over complexity. Instead of “P@s\$W0rD”, use unrelated words and numbers: “Cat7waterbottle flipflop87”
 - c. Avoid personal info.
 - d. Never reuse passwords.
2. Your Zoom account should have two-factor authentication (2FA) turned on. 2FA is a security method that requires two distinct forms of authentication (password + email or SMS code) before you can access your account.
 - a. Currently, WyTN requires 2FA if you are logging into a new computer or accessing your Zoom account for the first time in several days.
3. Log out of your Zoom account at the end of each day.
4. If there is a device logged into your account that you do not recognize, connect WyTN at wytn@uwyo.edu and change your password.
 - a. If you share your Zoom password with other accounts, change the password to those accounts as well.

5. Do not block or report the wytn@uwyo.edu email. This is the primary way WyTN will contact you, so blocking or 'spamming' our email will restrict you from receiving important communications from us.
 - a. If you do not wish to receive communications such as the newsletter or announcements, please click the unsubscribe link located at the bottom of our communications.
 - b. If you do not wish to receive meeting reminders, please respond to the email and let us know directly.

Changes In Account

The WyTN is excited to support providers throughout their careers – which could mean changes to information such as email address, organization, last names, specialty, location etc. If any of this information changes, please send us an email at wytn@uwyo.edu. We will send you a code that will allow you to quickly update your records. Maintaining an accurate record of providers who use our network allows us to develop relevant learning materials, conduct usage analyses, and importantly – provide accurate reporting to our grantors. Keeping your information up to date will allow us to continue providing you with the best experience with your WyTN Zoom account.

If you no longer want/need your WyTN Zoom account, please let WyTN know at wytn@uwyo.edu. WyTN is only able to support limited number of Zoom licenses. Letting us know when you are no longer planning on using or wanting your Zoom licenses gives us the opportunity to provide other providers with Zoom accounts.

Zoom Meetings

When creating Zoom meetings on your WyTN Zoom account, please follow the below considerations to ensure secure meeting initiation and accurate date reporting.

1. Never share or initiate a telehealth session through your personal meeting ID.
 - a. The personal meeting ID can be easily saved and accessed at any time.
2. When sending a calendar invitation, under 'Primary Purpose of Meeting' indicate what type of meeting you are hosting, using the drop-down menu.
 - a. Accurate selection of the meeting type supports WyTN data reporting.
3. Do not post Zoom meetings to the public without adding a passcode or waiting room.
 - a. All meetings should have a passcode and/or waiting room.
 - b. If you are hosting a general group information meeting, where not all members of the group will be know, advise members at the initiation of the meeting to refrain from sharing PHI.
4. Never share your clients' email addresses, phone numbers, physical addresses with one another.

- a. If you need to email the group, be sure to put email addresses in the BCC address line.

Conclusion

Thank you for taking the time to review these updated policies. We are hopeful that through their successful implementation, our network will be stronger, and more secure. If you have any questions or concerns related to the above changes, please reach out to the Wyoming Telehealth Network through email at wytn@uwyo.edu, or via phone at 307-766-2944 . Thank you for your continued support, and happy Zooming.