Zoom - HIPAA Changes and FAQ

Issue:
There were recent changes to the implementation of WSU Zoom's HIPAA implementation and I have questions on how I should proceed to conduct HIPAA-compliant Zoom meetings.

FAQ:

Q. What do the new HIPAA measures mean for me? Are all my Zoom meetings now HIPAA compliant?
A. All of WSU's Zoom is now HIPAA compliant for everyone via a BAA (Business Associate Agreement) with Zoom. This means if you are sharing sensitive data and follow proper security guidelines, your meeting is protected.

Q. Can I record to my local machine?
A. Yes, you can record locally for normal meetings. If your meeting will need to be HIPAA compliant, the host of the meeting needs to disable the feature. This, and other HIPAA compliance measures, falls under the Endpoint Security Standards.

Q. If medical and counseling providers can cloud record sessions, where are the recordings stored?
A. The recordings are stored on the Zoom Cloud, however, WSU has sole and complete rights and ownership over any PHI stored there.

Q. How long are the cloud recordings stored?
A. Currently, recordings are stored for 365 days.

Q. Are the recordings encrypted?
A. Data in motion is encrypted at the application layer using Advanced Encryption Standard (AES).

Q. Who has access to the cloud recordings?
A. Access control is paramount for recordings with the Zoom services team. Only the three Zoom services administrators have access to recordings, as well as the host of the meeting themselves and anyone they share the recording with.

Q. What are the recommended settings for recording, chat, and meetings?
A. If you regularly host HIPAA-compliant meetings, to prevent confusion between your normal meetings and HIPPA-compliant meetings it is strongly recommended you have saving chat and local recordings disabled.

Q. Who should I contact if I have concerns or questions about these HIPAA changes?
A. If you have a privacy officer, please reach out to them. Otherwise, please contact Sally Makamson (smakamson@wsu.edu) and copy ciso@wsu.edu.

Features and Settings

Below are Zoom User settings (https://wsu.zoom.us/profile/setting) that provide additional security when conducting HIPAA-compliant Zoom meetings:

Meeting Security Settings:
- Enable Waiting Room: Require participants to wait in a virtual waiting room before joining meetings, allowing the host to vet participants and control access.
- Require Passcode: Enforce passcodes for all meetings to prevent unauthorized access.
- Disable Join Before Host: Prevent participants from joining meetings before the host arrives to maintain control over meeting access.

Data Sharing and Transmission:
- Disable Remote Control: Disable remote control features to prevent participants from taking control of the host’s screen, which could potentially expose PHI.

Participant Management:
• **Restrict Screen Sharing to Host Only**: Limit screen sharing to the host only to prevent unauthorized sharing of PHI.
• **Disable File Transfer**: Disable file transfer during meetings to prevent the exchange of PHI-containing files through the Zoom platform.

- Zoom - HIPAA Changes and FAQ
- Zoom - What does invalid Meeting ID mean?
- Email - How to Add, Manage, and Remove Delegates in Outlook for Mac
- Email - How to Add a New Email Account to Outlook for Windows
- Email - How to Add a New Email Account to Outlook for Mac