ZOOM Tip Sheet

- Be wary of links that you receive to join meetings. When possible, ask your host to provide the meeting ID and password instead, which you can input into the Zoom application to find and join your meeting. If you are unsure that a link is legitimate, please reach out to the Firm's IT personnel before clicking on it. Advise the host to use different passwords for each meeting, so that if your meeting is running late, attendees of a later meeting are unable to inadvertently join your meeting. Consider using a different password even for recurring meetings. If this is not possible, the host should be asked not to use that password for any other meetings that he/she may set up using his/her Zoom account.

- Meetings should be password protected. We understand that because of the recent surge in security lapses, Zoom is defaulting to requiring passwords for conferences. A user setting requiring passwords can be turned on or a password may be set up when scheduling specific meetings.

- Meeting details should be sent only to participants. Please advise the host not to email such information to those who are not required to attend a particular meeting or distribute the information using messaging boards that are accessible to non-attendees.

- User settings can be set to carefully control what participants may be able to do. For instance, if there are specific individuals who will be presenters, screen sharing rights should be limited to those individuals and turned off for all other attendees.

- The "Join Before Host" setting should be disabled so that the host can control who is allowed into the meeting from the outset. Turn on the "Waiting Room" option so that participants cannot join without being expressly admitted by the host.

- There are options to delegate certain host capabilities to other uses. This option should be used sparingly, if at all.

- Requests to join the meeting should be reviewed carefully by the host, to avoid unauthorized individuals for joining. The list of participants is visible to all and should be reviewed periodically throughout the meeting.

- Lock a meeting, when possible, after a certain amount of time has elapsed or when the expected attendees have all joined. This will prevent unauthorized people from joining during the meeting. This can be done by using the "Manage Participants" option and using the controls that appear on the right of the meeting window. Manage Participants also allows the host to mute all participants, eject certain participants, or stop select participants from appearing by video.

- When joining a Zoom meeting, consider doing so with your camera and sound turned off. You can turn them on once you have joined the meeting and confirmed that you are in the proper conference and trust the attendees.

- Be aware of everything that's within view of your camera. There may be private information, documents, notes, or other confidential information that should not be viewed by others. Remove these from view of the camera before the meeting starts.

- Review your Zoom screen. If the meeting is being recorded, a red button will appear, usually on the top right corner. If you are unsure, ask the host/participants during the meeting, and make any objection known in advance of the meeting (perhaps by email), at the beginning of the meeting, and again towards the end.

- Close windows that are not essential for the meeting, particularly if you had been working on confidential materials, to avoid inadvertently sharing that material if your screen is shared with attendees.

- If your meeting is compromised, arrange an alternate meeting, such as by Webex or teleconference.

- Be aware of how Zoom encrypts its data. Data encryption translates data into another form, or code, so that only people who are supposed to have access to it can read the data.

  As per Zoom, it does not appear that data is encrypted when joining a meeting through a browser (e.g. by going to the website zoom.us and inputting the meeting ID and password or by calling in using a phone).
  In a meeting where all of the participants are using a Zoom app or Zoom Room, and the meeting is not being recorded, Zoom states that it encrypts all video, audio, screen sharing, and chat content in transit so that Zoom cannot access that data at that time. It is also protected against brute force attacks. The data, however, is not encrypted before or after transit (i.e, at an individual participant's device). Zoom claims that it does not access meetings without authorization, and cannot do so without being reflected in the participants list.

- Zoom products are not all HIPAA-compliant. Accordingly, avoid discussing protected health information during Zoom video conferences.

  If you have any questions regarding the foregoing or any related issues, do not hesitate to contact Anna Mercado Clark (aclark@phillipslytle.com or 212-508-0466).