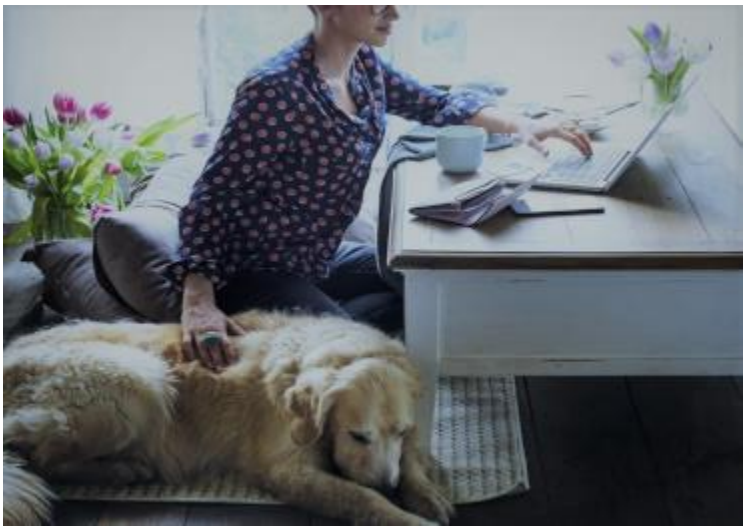
Working from Home: Quick Tips



- ✓ Update (patch) all the software on your computers and devices.
- ✓ Use extra-long passwords and two-factor authentication for remote access to your organization.
- ✓ Protect all mobile devices with passwords/biometrics and never leave them unattended.
- ✓ Diligently follow all company rules related to remote working and re-read all relevant company policies on working remotely.
- ✓ Never use public WiFi to transact sensitive business unless through a Virtual Private Network (VPN) or other secure means.
- ✓ Securely dispose of all sensitive information (including shredding any paper copies) in accordance with company rules.

Use Zoom Securely

Remote workers are using video conferencing apps like Zoom to meet with co-workers. Zoom's popularity is also highlighting some major security vulnerabilities. For example, there have been multiple reports of unauthorized participation in meetings, a practice dubbed "Zoom bombing." These privacy and security concerns caused New York City to instruct its public schools to "move away" from using Zoom.

Take the following steps to securely use Zoom.

- ✓ **Update your Zoom application/software**. Zoom recently updated its software and added meeting passwords by default and disabled the ability to scan for meetings. These features are intended to prevent unauthorized access to the meeting. Zoom is constantly making security fixes so always run the latest version of Zoom.
- ✓ When creating a meeting, ensure it is **password protected**. Password settings are on the "Settings" page in the web portal under the "Meetings" tab.
- ✓ Use the **"waiting room"** feature. This feature prevents participants from joining the call until approved by the host. Confirm this feature is enabled on the "Settings" page in the web portal under the "Meetings" tab.
- ✓ Provide the meeting link directly to specific people. Do not publicly broadcast a meeting link.
- ✓ As the host, control participants in your meeting using the "Manage Participants" button. To prevent participants from sharing screens, click "Host Only" in the Advanced Sharing Options under the "Screen Share" button.
- ✓ Only record the meeting if you must and be careful where the file is stored. The host can control which participants may record the meeting through the "Manage Participants" button and click "Allow Record."

Understand COVID-19 & HIPAA

The U.S. Department of Health & Human Services Office for Civil Rights (OCR) has issued two important Notifications of Enforcement Discretion related to (1) telemedicine and (2) uses and disclosures of Protected Health Information (PHI) by business associates.

Telemedicine

To help slow the spread of coronavirus, particularly at health care provider facilities, telemedicine has been encouraged by health regulators. OCR announced it will not penalize healthcare providers for HIPAA noncompliance related to the good faith use of telehealth during the COVID-19 public health crisis. A covered entity can provide telehealth to patients during the COVID-19 public health emergency using "any non-public facing remote communication product available to communicate with patients." OCR identified the following acceptable popular platforms: Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype. Applications, however, like Facebook Live, Twitch, TikTok, and similar applications are public facing, and should not be used.

Uses and Disclosures of PHI by Business Associates

OCR also announced it will not penalize business associates for uses and disclosures of PHI for public health and health oversight activities during the COVID-19 nationwide public health crisis. Current regulations allow a business associate to use and disclose PHI for public health and health oversight purposes only if expressly permitted in the business associate agreement. During the current COVID-19 health crisis, however, there will be no penalties provided that the business associate:

1. makes a good faith use or disclosure of the PHI for public health activities or health oversight activities; and
2. the business associate informs the covered entity within ten (10) calendar days of the use or disclosure.

Examples of potential PHI disclosure by a business associate include those to the Centers for Disease Control and Prevention (CDC), Centers for Medicare and Medicaid Services (CMS) or similar authorities at the state level.