Cybersecurity and privacy: 8 tips for working from home

With a significant portion of the U.S. workforce working from home over the coming weeks, it is incredibly important to ensure as an organization we maintain good cyber hygiene. Malicious actors will attempt to exploit this shift in how the workforce is connecting. Below are tips to remain vigilant while working from home.

These are Advocate Aurora Health's remote work policies. Click on the title to access the full policy.

- Remote Access Security
- Alternative Work Options
- Acceptable Use of Information Resources
- Safeguards & Incidental Uses and Disclosures of PHI
- Disposal of PHI and Other Restricted Information

1. Lock your computer.
It can seem silly, but you should practice locking your computer when you are away from – it even at home. You have access to confidential information (and potentially regulated data such as ePHI, PII, and PCI, and therefore you are required by regulations to ensure no one else can access or look at this data. You should also practice the clean desk principle at home, ensuring nothing you've printed is left out for someone in your household to see or use.

2. Keep work data on work computers.
It can be very tempting to use your personal computer if your work computer is in a different room at home or you forgot your charger at the office, or even if you want to multi-task. This is a risk for you and for Advocate Aurora Health. Do not use your personal device for anything work-related, and conversely, it's also critical you only use your work devices only for work. Do not allow others in your household to use your AAH devices.

3. Secure your devices.
This may seem silly, but make sure you are locking your doors at home. If your home office has windows, make sure your devices are not within the sightline of passersby. If you are traveling with your computer, take it with you, do not leave it in your vehicle. If that is not feasible, lock the computer in your trunk. **Report missing or stolen devices to AAH IT Service Desk and Security Services immediately.**

4. Avoid public wi-fi and only use AAH-authorized remote access solutions.
Public wi-fi puts Advocate Aurora Health - and you – at risk. If at all possible, only use your trusted home network, and ensure your home network has a strong password. Make sure you are using DUO multi-factor authentication, and AAH-authorized remote access solutions, so your work is secure.

Created by: E. McKinley Created Date: March 25, 2020 Revised Date: March 26, 2020

5. Watch out for scam emails and phishing attempts.
Malicious actors know that a significant portion of the population is working from home, which creates new opportunity for them to exploit you and your information. **Think before you click.** When you receive an email from an unknown sender, hover over the link if it looks suspicious, report it via the Report Phish button (Outlook) or icon (OWA). Many phishing attempts will have a sense of urgency and they will attempt to exploit the COVID-19 situation. Err on the side of caution with emails you receive.

6. Use Strong Passwords
Make sure the password(s) you are using are strong. Strong passwords will not only protect your devices and systems being accessed, but also they protect Advocate Aurora from hackers if a mobile or laptop is lost or stolen. Do not write your passwords down!

7. Scanning and printing
Avoid printing and scanning documents if at all possible, at home. If a form or signature is needed, AAH has technological options that allow forms to be filled and signed electronically (i.e. Adobe Acrobat, DocuSign). Printing and scanning should be minimized as much as possible. If printing or scanning is necessary and cannot be done electronically, please contact the HIT Service Desk or fill out a ServiceNow ticket for available options. Additionally, leaders need to determine if printing is necessary for their team members. If so, printers with hard drives that retain (store) images cannot be used.

Any printed materials containing PHI or confidential information must be secured to prevent unauthorized access. Once the printed materials are no longer needed, they must be shredded, or kept secured until they can be destroyed by AAH.

8. Approved communication channels
You should only use approved AAH communication technologies for communicating with patients or restricted information. Personal messaging services are **NOT** AAH approved. AAH Zoom is a sanctioned communication method. We may evolve to additional methods of communication and videoconferencing methods as needed. Please contact the HIT Security Risk Management Team or Cybersecurity Team with questions.