Sinai Health

Privacy tips for working from home

1. Be Privacy Proactive
    - If you are just transitioning to working remotely – make sure you have what you need before you start – speak with your manager about your job requirements and what you will need to have in place to work effectively.
    - If you have been working remotely for a while, review your set-up, current practices, and any confidential information that you have taken or accessed off-site (in paper or electronically) and make adjustments as needed.

2. Secure Information in Transit and at Home
    - Limit the information you access or take off-site to only that which is needed. Get approval from your manager before taking any Sinai Health records or devices offsite.
    - Secure paper and electronic media when in transit (e.g. sealed envelope; hidden and locked in your vehicle trunk if temporarily parked on the way home).
    - Keep work-related information secure and not accessible to others in your home.
    - Do a routine clean-up of all confidential information – return documents that you no longer need to the hospital or securely destroy them (cross-cut shred, pulverize, pulp or incinerate – to pieces no bigger than 5 mm x1 mm).

    Remember: Confidential information and patient PHI can take many forms – patient records and other "official" documents, meeting notes, notes made on a sticky note or scrap piece of paper, and even to-do lists.

3. Remote Access
    - Do your work within Sinai Health's secure electronic environment(s) as much as possible. Use Citrix to remotely access work related applications from the "For Staff" page seen on our web site.
    - Use hospital-issued devices (i.e. laptops, mobile devices, USB keys) to remotely access Sinai Health systems, and make sure they have up-to-date security patches.
    - Do not open or save work-related documents or information on your personal devices. Delete any work related documents from personal devices (including from "downloads").
    - Be careful to not allow others to view your screen(s). Use your dedicated work space to prevent shoulder surfing and eavesdropping.

4. Phone Calls
    - Use your Sinai-issued cell phone or a Sinai-approved audio or web-conferencing service. If your work requires the use of a Sinai Health phone or conferencing account but you do not have one, speak to your manager.
    - Avoid using your personal phone to make calls on behalf of the hospital. If you must call a patient using your personal phone due to extenuating circumstances, delete the phone number immediately after the call. To maintain your own privacy, block your personal number by using your service provider's "Call Block" function (e.g. *67).
    - Do not have phone or video conversations in places where others can hear/see (keep in mind – even one-sided conversations can be a breach of privacy).

5. Email
    - Use your hospital-issued email address for all work-related email. Your hospital-issued email can be accessed through our corporate webmail, via the “For Staff” page on our web site.
    - Make sure that you are complying with Sinai Health’s expectations for secure email communication seen in our Appropriate Use of Information Technology policy.

6. Apps
    - Use only Sinai Health-approved applications and accounts to access, process, store or communicate patient or business information (you can contact Helpdesk for guidance)
    - Using personal versions of applications (such as a personal Zoom account) is not permitted.

7. Privacy Incidents
    - Protecting the privacy of our patients is fundamental to maintaining trust in our hospital and ensuring person-centered care. We all play a role in supporting the safety and wellbeing of our patients.
    - If you become aware of any privacy incident or privacy concerns, promptly notify your immediate supervisor and file a SAFER Report.
    - Privacy incidents (that occur in any setting) are managed according to the Privacy Incident Protocol.

Additional Resources

Privacy-related questions or concerns can be directed to the Privacy office at 416-586-4800 x.2101 or privacyoffice@sinaihealth.ca

Information Technology and Security questions or concerns can be directed to the Helpdesk (MSH – x. 4357 or helpdesk.msh@sinaihealth.ca Bridgepoint x. 5000 or helpdesk.bh@sinaihealth.ca

Owner: Privacy and Information Security
Updated: January 26, 2021