Icahn
School of
Medicine at
Mount
Sinai

ISMMS Traveling with Technology Bulletin
Updated: September 23, 2019 Version 1.9

If you're planning to travel on behalf of the Mount Sinai Health System, it is critical to safeguard your data and electronic devices, especially for international travel. There are a number of common risks while traveling with technology. These risks include device and identity theft, WIFI hacking, border seizures, emerging threats such as data ransom, as well as state sponsored espionage. It is important to understand ways to reduce your risks.

1. Before You Travel:

- **Reduce your technology and data footprint.**

  The safest way to protect your data is to avoid traveling with it. Only bring data and devices necessary to get your work done.

- **Secure your devices and accounts.**

  Enable available security features, including encryption (may be active by default). Any device accessing MSHS data (including email) must be encrypted.

  In order to view email while traveling, you will need a Mobile Device Manager (MDM) for any mobile device (smartphone, tablet) and/or VPN and two-factor password authentication for any laptop. Please ensure your devices are properly setup before traveling. To learn how, visit https://ITsecurity.mssm.edu.

  Academic IT Support Center (ASC-IT) is available for setup and support assistance with security tools. ASC-IT is located on the 11th floor of Annenberg, behind the Library's circulation desk. It is also reachable via telephone (212.241.7091) or email (ascit@mssm.edu). ASC-IT support is open Monday - Friday, 8am - 8pm; Saturday, 9am - 5pm; and Sunday, 12pm - 8pm.

2. While You Travel:

- **Avoid public computing terminals and open WIFI.**

  This includes charger kiosks, computers, and WIFI. If using a shared or public computer is unavoidable, use caution. Read before you click, and ensure you do not accidently authorize access to data on your device. Beware of using public

computers that may be tracking your key strokes. If you must use a hotel business center computer, make sure that no information is inadvertently saved for the next user. Use known hotel or airline WIFI and always avoid entering passwords into non-secure “http” websites. (Always ensure “https” appears within the URL.)

- **Never leave your devices unattended.**

  Place devices into hotel safes when not in use, and power them down when possible.

- **Report if your device is stolen or seized.**

  Please report your device theft to the local authorities and return home with a copy of the report. Lost, stolen, or seized devices (at the border) must be reported. To do so, please reach out to ASC-IT (212.241.7091)

3. **<u>International Travel Considerations:</u>**

- **Ensure cellular coverage is available before traveling.**

  The Mount Sinai IT team can ensure that your company issued Verizon mobile device stays connected while you’re traveling and that the appropriate data plan is setup. First review if Verizon provides coverage to the country that you’re traveling to: http://www.verizonwireless.com/b2c/tripplanner/tripplannercontroller If there is coverage, please reach out to ASC-IT at least five business days prior to your departure to ensure that you have active coverage on your Mount Sinai assigned device. Please note that MSHS IT cannot setup personal devices for international cell service.

- **Take precautions crossing international borders.**

  Border authorities around the world, including the US and Canada, are increasingly demanding immediate access to travelers’ devices, seizing them for forensic inspection. Therefore, ask yourself if you would be comfortable with an agent inspecting the content of your laptop, camera, or mobile phone. Border agents may ask you for passwords and other biometric information to access your devices and through a variety of ways can bypass most encryption methods. Ensure that passwords to any MSHS remote resources (cloud storage, etc.) are not saved on your device or browser.

  Leave a secure backup of data in the US in case it is seized or lost. Ensure backups are valid and can be read.

- **Know the risks associated with your specific destination. Some areas of the world including China, Russia, and the Middle East are at increased risk of data breaches and may be monitoring communications.**

If possible, it is recommended that you leave your primary devices at home entirely, and travel with devices that have only the data and applications relevant to your trip. When returning home, these devices should be considered compromised, never synchronized, and erased immediately. If you are bringing your primary device, consider backing it up somewhere, wiping it, bringing only the data you need, and restoring to the last back up when you return. If that is not an option, remove any high-risk data such as personally identifiable information: SS#s, health, financial information of yourself or patients as well as student information. Also remove proprietary content including unpublished research, data sets, and employee information.

Consider using a temporary email account for the duration of the trip. At the very least, create temporary passwords to accounts you will access while traveling (both personal and work-related accounts), and set up alerts to notify you if an account is accessed using an unregistered device.

Limit communications (email and phone) to people aware that the conversations might be monitored, and do not transmit sensitive data.

Some countries continually review social media posts (Facebook and Instagram) from visitors and may investigate individuals who violate local laws or customs based on posted content.

4. <u>When You Return:</u>

- **Wipe and restore your devices.**

  If you have backed up and wiped your device prior to traveling, restore your device to the back up.

- **Request IT to SCAN your devices for viruses.**

  When traveling to high-risk counties, request a scan of your device to search for any viruses or malware. The Academic IT support Team is available to assist.

- **Change your passwords.**

  Change all of your passwords to any account used while traveling.