Icahn
School of
Medicine at
Mount
Sinai

ISMMS Traveling with Technology Bulletin
Updated: February 6th, 2018
Version 3

If you're planning to travel either domestically or internationally, it is critical to safeguard your data and electronic devices. There are a number of common risks while traveling with technology. These risks include device and identity theft, WI-FI hacking and emerging threats such as data ransom, border seizures of personal content, as well as state sponsored espionage.

These threats have been widely publicized within the media, and it's critical to understand ways to prevent or reduce their impact. If you are planning on traveling with data, we encourage you to consider the following:

1. Reduce your technology footprint:

The safest way to guard your data while traveling is to avoid traveling with it. Be sure to bring only the data and devices that are necessary for your visit. As reported in the Wall Street Journal and New York Times, border authorities around the world, including the US and Canada, are demanding immediate access to travelers' devices. Therefore, ask yourself if you would be comfortable with an agent inspecting the content of your laptop, camera, or mobile phone.

In some areas of the world including China, Russia, and the Middle East, it is recommended that you leave your primary devices at home entirely. Instead, travel with devices that only have data and applications relevant to your trip. When returning home, these devices should be considered compromised, never synchronized, and erased immediately.

2. Prepare before you leave:

Backup your data and synchronize your mobile devices and enable available security features. Enable encryption if it isn't active by default. Any device accessing MSHS data including email must be encrypted.

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 Also remove proprietary content including unpublished research, data sets, and employee information.

Our account policy requires strong network passwords, changing them on a regular basis and the use of a Mobile Device Manager (MDM) or two-factor password authentication to review email off campus. Please ensure your devices are properly setup BEFORE traveling. To learn how, please visit https://ITsecurity.mssm.edu.

We also recommend you visit the Academic IT Support Center (ASC-IT) 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 during the following times:

- Monday - Friday, 8am - 8pm
- Saturday, 9am - 5pm
- Sunday, 12noon - 8pm

Ensure that passwords for your personal accounts (such as Google/Facebook) use at least 8 characters with upper/lower case letters, numbers, and special characters. Also, set up alerts that notify you if your account is used/accessed using an unregistered device.

3. Ensure secure data and cellular coverage:

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; please check directly with your mobile carrier.

4. Exercise caution while traveling with technology:

Avoid charger kiosks. There might be a computer on the other end capable of copying your information. If use is unavoidable, use caution. Read before you click and ensure you do not accidently authorize access to all your data on your device.

Beware of using public computers and rental kiosks as they could be tracking your key strokes. Avoid logging into anything using these computers. Hotel business center computers should be avoided as one's passwords can be inadvertently saved for the next user.

Never leave your devices unattended. Place devices into hotel safes when not in use, and power them down when possible.

Use known hotel or airline WI-FI and always avoid entering passwords into non-secure "http" websites. Always ensure "https" appears within the URL

5. What to do 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, please reach out to ASC-IT (212.241.7091)