Mass General Brigham

FROM: Jigar Kadakia, Chief Information Security and Privacy Officer, Mass General Brigham
DATE: September 2021
RE: Clean Laptop/Phone Program for Travel to China, Russia, and countries deemed high risk by the Department of Commerce

Mass General Brigham (MGB) Information Security and Privacy Office is issuing this Information Security and Privacy Memorandum to notify all impacted individuals and business units that business travel to China, Russia and other high-risk countries, whether for research, clinical or consulting purposes, creates specific information security challenges that must be addressed in order to effectively secure MGB's data and assets. The Clean Laptop/Phone Program has been put in place to address these concerns.

Travel Statement

All MGB workforce members traveling to China, Russia or other countries identified as high risk by the Department of Commerce must take special care to ensure MGB's data and assets are properly secured, due to the fact that personal privacy may not be respected. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio, or other monitoring. Workforce members are advised to assume that anything done on any device, particularly over the Internet, may be intercepted. In some cases, encrypted data may be decrypted. To that end, the following security controls must be followed by any individual conducting MGB business in China, Russia, or other high-risk countries.

Prior to Travel

Access to MGB network resources from these countries is limited to MGB workforce members. Workforce members intending to access MGB resources from these countries must complete the following steps prior to travel:

- When you make your transportation arrangements, register your travel plans (including dates of travel) with the MGB Travel Safe Program.
- Review the Department of Commerce high-risk country list, specifically countries listed as high risk for National Security and Chemical & Biological purposes. If your travel destination appears on this list, contact your hospital Export Control Officer at the link below to determine whether you should take advantage of the clean laptop program while traveling or if there are country-specific export controls requirements that must be addressed prior to traveling. (https://partnershealthcare.sharepoint.com/sites/phrmResources/c/ec)
- Contact your hospital's Information Security Officer (ISO) no less than 10 days prior to departure to request a clean computer and mobile phone. Do not bring or use your regular devices during your trip[1].
    - Clean phone program requires an update to Mass General Brigham's myprofile.partners.org to include the international calling number for multi-factor authentication.
- Change all passwords prior to departure.
- Backup your laptop and/or phone before departure.
- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, employee badge or fobs you would use to access your workplace, or other areas, and any other access control devices you may have at home.

[1] If you bring your smartphone, you will need to install the Okta Verify application to support multi-factor authentication for international access.

- Remove any financial information such as bank account numbers, logins and passwords you may have in your purse or wallet.
- Document the account numbers to anything you do take, so that if lost/stolen, you know what is missing.
- Obtain and use an RF-shielded cover or case for any RFID cards (including U.S. Government Nexus "trusted traveler" cards) that you do plan to take with you.

During Travel

Never use shared computers in cyber cafes, public areas, hotel business centers, and never use devices belonging to other travelers, colleagues, or friends.

- Use Citrix to connect to MGB resources (workspace.partners.org).
- Rigorously apply minimum necessary principles to all information accessed, used or obtained.
- When not in use, completely logout of applications accessed and fully power down devices. Do not allow them to be in "sleep" or "hibernation" mode, make sure they are shutdown.
- Keep device(s) with you at all times during your travel. Do **not** assume they will be safe in your hotel room or in a hotel safe.
- Do not send sensitive messages.
- Disable and fully cover any integrated laptop cameras.
- Physically disconnect any integrated laptop microphones.
- Be aware of your surroundings and shoulder surfing. Position yourself to minimize this opportunity for others.
- Disable all unnecessary network protocols, (e.g., Wi-Fi, Bluetooth, infrared, location services, GPS, etc.)
- Do not plug your phone into charger kiosks. There may be a hostile computer on the other end of that innocent-looking wire.
- Access to services that we take for granted like Gmail and other Google apps, Wikipedia, and Yahoo Web Mail are often blocked altogether or monitored/filtered.
- Do not store any sensitive data on your devices while traveling overseas.
- Do not use or borrow others' USB memory sticks.

Upon Return to United States

Upon return to the United States and prior to re-connecting to any MGB network or technology, MGB workforce members must complete the following.

- Immediately discontinue use of the temporary device(s) you brought with you. The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled prior to being reconnected.
- Delete any data stored on such devices listed above.
- Change all passwords you may have used abroad from an alternate device (other MGB/Institution workstation/Laptop).
- Do not plug in any USB memory sticks that you have obtained/received during travel.
- Return the devices by contacting the IS Service Desk site techs for pickup. Ensure you notify them the devices were on international travel.

Applicability

This advisory is applicable to any Mass General Brigham workforce member who is conducting approved business from China, Russia or other high-risk countries.

For questions regarding whether a country is high risk, contact your hospital's export control officer in https://partnershealthcare.sharepoint.com/sites/phrmResources/c/ec

For all other questions regarding the Clean Laptop/Phone Program, contact your hospital ISO.

Resources

- Information Security Officers
- IS Service Desk
- Phone Registration-International

Okta Verify (Smartphones)


Okta Verify Guide for iOS (3).pdf


Okta Verify Guide for Android.pdf

Mass General Brigham Travel Safe Program