Harvard Pilgrim Health Care, Inc.
Harvard Pilgrim Health Care Institute, LLC
Office of Sponsored Programs

Policy and Procedure
International Travel and Foreign Collaborations

This policy applies to all Harvard Pilgrim Health Care, Inc. (HPHC) and Harvard Pilgrim Care Institute, LLC. (HPHCI), (collectively HPHC/I) personnel who are engaged in instruction, education and research and are involved in international travel and foreign collaborations.

BACKGROUND

HPHC encourages HPHCI's global presence in worldwide research, teaching, and learning. As global mobility increases and communications barriers continue to decline, HPHCI faculty/staff are and should be developing international partnerships and pursuing teaching and research opportunities the world over.

HPHC/I's effort to support research work outside the United States (U.S.) follows two principles:
(1) barriers to global work should be low; and
(2) the risks to HPHC/I, faculty/staff that arise in the course of conducting international work should be managed effectively.

HPHC/I's goal is to allow HPHCI faculty/staff to pursue international opportunities, while receiving the support of institutional structures that mitigate risk. Achieving that goal requires recognition that international projects present challenges and risks along with opportunities.

The shaping principle for these rules is that HPHC/I's policies and procedures, and the laws of the United States and the host country, must be followed. In particular, associated Privacy and Security policies include, but are not limited to:

- CSS0022 - Email
- CSS0001 - Use of Computer & Communications

DEFINITIONS

Bribe - Money or some other benefit given to a person in power, especially a public official, in an effort to cause the person to take a particular action.

Remuneration – Payment received for rendering services, can be in cash or in kind. Examples: rent free accommodations, telephone expense reimbursement.

POLICY

All international travel and foreign collaborations require the standard HPHC/I review and approval of the Director of the Office of Sponsored Programs (OSP) and the Institutional Review Board (IRB) where human subjects research is involved.

Faculty/staff wishing to engage in foreign travel in connection with an HPHC/I contractual undertaking, must notify their OSP grants manager for review to flag particular issues that may arise based upon the destination and work to be performed.

When conducting research in other countries, Principle Investigators (PIs) still need to obtain approval from HPHC's IRB when conducting research with humans. Any research conducted outside the U.S., must be in conducted in accordance with the applicable international laws relating to the conduct of human subjects research in that locality. Even unpaid consultations with foreign collaborators who are engaged in human subjects research requires HPHC IRB review if the HPHC/I researcher expects to be an author on any paper that results from the research or receives any information that would identify a human subject. Often it is also necessary to secure the approval of a local foreign IRB or research ethics committee.

Faculty/staff also should note that as part of their human subjects research obligation for studies conducted among populations with Limited English Proficiency ("LEP"), they must assure adequate informed consent from LEP subjects, consistent with the terms of approval from the HPHC IRB and any local IRB.

EXPORT AND FINANCIAL CONTROL

Faculty/staff must comply with foreign legal requirements relating to imports and exports from foreign jurisdictions. Many countries require a license or permit to import items, and a license or permit to export items, such as human and non-human bio-specimens, identified data (i.e., data that identifies individuals), and art and/or antiquities. Faculty/ staff should anticipate restrictions in this regard when planning an international project and seek advice from OSP on complying with relevant host country laws and customs, HPHC/I policies and procedures, and/or U.S. law.

Faculty/staff are also encouraged to seek advice from the foreign collaborating institutions, which may have information on local import and export licensing requirements. Even inadvertent violations of legal requirements can have serious consequences, including criminal prosecution, imperiled ability to use exported materials and objects for research and publication, and damage the reputation of faculty/staff and HPHC/I.

Faculty/staff must also abide by U.S. export control laws and regulations and by sanction programs enforced by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). U.S. law prohibits the export to specific countries of certain items and technologies, including some seemingly ordinary items that could have a military orientation that triggers higher level controls; and also prohibits a broad range of interactions with certain individuals, entities, and countries, including initial export of items from the U.S., re-export of items, sharing non-public information at an international conference, conducting research in a particular country, engaging in an international collaboration, or shipping to another country equipment, materials, or other items necessary for research (often including common items such as laptops, cell phones, personal digital assistants (PDAs) and other mobile electronic devices). All subrecipients and vendors must be vetted through OSP prior to incurring any payment liability. HPHC/I cannot pay directly for goods or services without a proper invoice.

For example, HPHC/I faculty/staff considering the purchase of capital equipment or supplies the value of which exceeds $3,000 need to comply with Federal law which requires that for equipment and supplies that exceed $3,000 in value, there must be a procurement process that secures at least three competing bids from potential vendors.

HPHC/I faculty/staff should not pay local labor in cash, or pay cash for local procurement of supplies or equipment, unless it is unavoidable and has been approved in advance by OSP. Managing large sums of cash when abroad may entail a personal security risk, and may violate U.S. or other national currency regulations.

For example, it is illegal to carry more than $10,000 in cash or cash equivalents (e.g., traveler's checks) across U.S. borders without declaring the funds in a customs declaration.

Federal law governing use of federal funds, as well as good business practices, require that faculty/staff exercise a high degree of diligence in selecting collaborators in research and other projects abroad, whether they are secured through subcontract or

vendor agreements. A casual acquaintance with a potential collaborator, or choosing a collaborator or subcontractor based on reputation alone, is not sufficient to discharge this obligation. OSP will conduct the reviews of subcontractors and vendors required by Federal Subrecipient Monitoring regulations when the work of licensed professionals is called for by a project. OSP will obtain proof of local professional licensure and of the institutional appointments of collaborator and will establish that the administrative and financial infrastructure supporting a collaborator is adequate. For example, a faculty member should not propose as a collaborator a professional who is employed by an institution that, if made a subcontractor, has inadequate resources to track time and effort of project staff, or satisfy financial reporting and procurement requirements.

The U.S. Foreign Corrupt Practices Act (FCPA) forbids payments to government officials for assistance in conducting business. Under no circumstances may HPHC/I and faculty/staff offer bribes, "pay-offs" or "kickbacks" in attempts to influence officials of foreign governments or institutions. Offering or paying bribes or remuneration in any form to an official of another government to influence them to do what they may not otherwise do is in many instances illegal under the laws of the U.S. and other nations.

For example, rent-free accommodations could be considered remuneration.
If approached by an official soliciting a bribe or payment of any kind that is not covered by a HPHC/I approved contractual commitment, HPHC/I faculty/staff should politely decline. If pressed and if, for example, personal safety is at issue, they should exercise good judgment to remain safe and as soon as possible, immediately report to OSP the circumstances of the solicitation and any payment.

Only the Director of OSP is authorized to sign sponsored research agreements, agreements with foreign governments, provincial officials, municipal, or parastatal officials (working with the government in an unofficial capacity) whose company or organization is owned by a country's government, or subcontractors, vendors or landlords on HPHC behalf. No faculty/staff have the authority to sign contracts, agreements or any other documents intended to bind or obligate HPHC.

HPHC/I faculty/staff are discouraged from practicing licensed professions abroad, such as medicine, nursing, pharmacy, laboratory science or law. If HPHC/I faculty/staff intend to practice a profession abroad, they must not do so without first obtaining local licensure or certification. Practicing any profession without local licensure or certification can, in most countries, be grounds for prosecution, and also carries with it a risk of uninsured liability for malpractice.

HPHC/I faculty/staff also should consult the Director of OSP to obtain guidance on obtaining professional malpractice coverage, if it is available. If the planned professional practice involves any direct patient care or other medical interventions with patients or research subjects, or if a HPHC/I project will directly support clinical care of patients that is delivered by a subcontractor or vendor, this must be disclosed to HPHC/I explicitly in project descriptions, grant applications and research protocols, and approved by the HPHC/I OSP.

HPHC/I faculty/staff should enter and remain in foreign jurisdictions only with appropriate visas. A visa is official permission from a country for you to visit. It is usually a stamp in your passport but is sometimes a piece of paper or electronic document that states how long you are allowed to stay in that country. A visa is always required for travel unless the country to be visited offers a "visa waiver" for short-term stays (e.g., U.S. citizens do not need a visa to visit Canada for fewer than 180 days, though they may need one if their purpose is to study or work); visa waiver eligibility depends on the traveler's country of citizenship. Research, studies, conferences, or business meetings may necessitate a business visa (or a more specialized visa such as a research visa) rather than a tourist visa.

Consult with the Embassy or Consulate for guidance on securing a visa before departure from the U.S., and the appropriate visas for these purposes. It is important to consider the visa laws and historical practices of a country in which a project or program is sited, and to do so well in advance of travel to that jurisdiction so that these issues can be anticipated and resolved in non-urgent circumstances.

ELECTRONIC DEVICE SAFETY

While you are in another country, unless you are required to perform a particular job function to support HPHC business, you should avoid taking any HPHC electronic devices, including but not limited to mobile phones, laptops, personal digital assistants (PDAs), thumb drives and other electronic devices (collectively, "electronic devices"). If you do need to take your mobile electronic device, HPHC's Office of Information Security (OIS) has compiled the following information and tips to assist in safe use of your mobile electronic device when traveling abroad.

Additional guidance from the National Counterintelligence and Security Center (NCSC) of the U.S. Office of the Director of National Intelligence is included below for those traveling overseas with electronic devices:

YOU SHOULD KNOW:

- In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.

- All information you send electronically - by fax machine, PDAs, computer, or telephone - can be intercepted. Wireless devices are especially vulnerable.

- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.

- Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.

- Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."

- Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.

- Corporate and government officials are most at risk, but don't assume you're too insignificant to be targeted.

- Foreign security services and criminals are adept at "phishing" - that is, pretending to be someone you trust in order to obtain personal or sensitive information.

- If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device's hard drive has been copied.

BEFORE YOU TRAVEL:

- If you can do without the device, don't take it.

- Don't take information you don't need, including sensitive contact information. Consider the consequences if your information were stolen by a foreign government or competitor.

- Back up all information you take; leave the backed-up data at home.

- If feasible, use a different mobile phone or PDA from your usual one and remove the battery when not in use. In any case, have the device examined by OIS when you return.

- Seek official cyber security alerts from: www.onguardonline.gov and www.us-cert.gov/cas/tips

PREPARE YOUR DEVICE:

- Create a strong password (numbers, upper and lower case letters, special characters - at least 8 characters long). Never store passwords, phone numbers, or sign-on sequences on any device or in its case.

- Change passwords at regular intervals (and as soon as you return).

- Download current, up-to-date antivirus protection, spyware protection, OS security patches, and a personal firewall.

- Encrypt all sensitive information on the device. (But be warned: In some countries, customs officials may not permit you to enter with encrypted information.)

- Update your web browser with strict security settings.

- Disable infrared ports and features you don't need.

WHILE YOU'RE AWAY;

- Avoid transporting devices in checked baggage.

- Use digital signature and encryption capabilities when possible.

- Don't leave electronic devices unattended. If you have to stow them, remove the battery and SIM card and keep them with you.

- Don't use thumb drives given to you - they may be compromised. Don't use your own thumb drive in a foreign computer for the same reason. If you're required to do it anyway, assume you've been compromised; have your device cleaned as soon as you can.

- Shield passwords from view. Don't use the "remember me" feature on many websites; re-type the password every time.

- Be aware of who's looking at your screen, especially in public areas.

- Terminate connections when you're not using them.

- Clear your browser after each use: delete history files, caches, cookies, URL, and temporary internet files.

- Don't open emails or attachments from unknown sources. Don't click on links in emails. Empty your "trash" and "recent" folders after every use.

- Avoid Wi-Fi networks if you can. In some countries they're controlled by security services; in all cases they're insecure.

- If your device or information is stolen, report it immediately to the local U.S. Embassy or Consulate and as soon as possible to OIS and the OSP grants manager.

WHEN YOU RETURN

- Change your password.

- Have OIS examine the device for the presence of malicious software.

Reference Documents:

Uniform Guidance Part 200—Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (http://www.ecfr.gov/cgi-bin/text-idx?node=2:1.1.2.2.1)

HPHC/I Policy & Procedure: Export Controls and Restricted Party Screening in Procurement and Payment

For general travel alerts and information, see:
http://travel.state.gov/content/passports/en/alertswarnings.html