**Travel and Transfer/Sharing of Data**

1. **Guidance**

**Purpose:** This document serves as a reminder of the institutional permissions that are required to properly share or transfer any BMC data outside BMC. This document also provides guidance to researchers with travel planned outside of the country and who are contemplating how to transfer data to their destination outside of BMC. Contact DUA.MTARequest@bmc.org if you have any questions.

**Background:** By way of background, in addition to a focus on biological materials leaving the country, in 2020 the federal government has also begun stopping and searching researchers at airports with regard to any research data in their possession as well. This has sometimes resulted in questioning, seizure of data and/or devices, or making copies of the data in their possession. Follow the guidance here to properly and permissibly share or transfer data to a non-BMC entity.

**Scope:** This guidance for data sharing/transfer in general applies for all transfers of BMC data to any non-BMC entity. Those subject to this guidance include, but are not limited to, BMC employees, researchers, principal investigators, trainees, visiting scientist/researchers, post-docs, collaborators, or other staff members (“BMC Staff”), if they intend to transfer or otherwise share access to BMC data. It also applies to BMC Staff who are planning round-trip travel outside of the country, as well as to any visiting researchers or post-docs who have completed their tenure at BMC and are returning home outside of the country. PIs must ensure their lab members are aware of these requirements and enforce compliance. If unsure whether or not this guidance applies to you, or for questions, contact the Senior Research Compliance Manager at michelle.irick@bmc.org.

**General Rule:** In any case, sharing or transferring data outside of BMC requires that you follow the substantive steps herein and contact the BMC representatives listed here. BMC prefers sharing/transfer via authorized, permissible digital methods (e.g. cloud storage service). Only if that is not possible could travel with data be possible. Be aware that data created at BMC using BMC resources is owned by BMC, not by individual researchers. A copy of data may only be shared or transferred outside BMC with assent from Legal/Research Compliance and IT.

1. **Recipient Institution**. Data may only be transferred outside BMC to a recipient institution. Researchers leaving BMC must have a formal affiliation with an institution in order to transfer data. BMC will not permit transfer of data to unaffiliated individuals.
2. **Authorization from the Principal Investigator or Department Chief.** The Principal Investigator or Department Chief must give you express permission in writing to transfer any BMC data.
3. **Institutional Review Board (IRB).** Contact the IRB at medirb@bu.edu to inform them of your plans related to an IRB protocol. In addition to taking any steps the IRB requests (e.g. IRB amendment for protocol modification etc.) the IRB must either approve or provide a determination indicating your plan may move forward from the IRB perspective. Please consider ahead of time what type of data you plan to share/transfer, how this data relates to BMC research and any potential future research, whether the subjects have provided permission/authorization for transfer of the data, how the data will be stored, and how it will be protected.
4. **Legal/Compliance**: What data are you planning to transfer and for what purpose? Do institutional policies and state and federal law permit this? Contact Legal and Research Compliance to facilitate answering these questions in your situation. Before sharing/transfer of any data or taking a copy of any BMC data with you, you must obtain institutional permission by having the requisite agreements executed outlining the terms and conditions under which you may take any data. Contact DUA.MTARequest@bmc.org for assistance.
5. **Information Technology**: BMC discourages anyone taking data on one’s person or in possession on devices through the airport or customs. Instead BMC Staff or returning researchers/post-docs should first see if a BMC-authorized electronic transfer/sharing or cloud storage method such as Box is possible. IT will determine if this will be possible in your case. Only if this is not feasible is traveling with a copy of data an encrypted electronic device a possibility. In that event, you need (i) sufficient encryption on an (ii) authorized device, (iii) approved by BMC IT. Contact DG-informationsecurity@bmc.org for an IT travel consult and authorization.
6. **Traveling with Data:** If IT determines you may take data on an authorized device and travel with it to your destination institution, then you must have in your possession, on your person, (1) copies of any executed agreements related to the data and (2) a signed copy of the Authorization Letter, complete with contacts.

1. **authorization Letter Instructions**

These instructions are intended to assist in completing the Authorization Letter for Traveling with Electronic Data document.

1. **Identification**: Provide the full name and credentials of the individual who will travel with the BMC Data “Data Holder”.
2. **Role or Position**: Provide the Data Holder’s role at BMC, whether it is post-doc, trainee, medical resident, senior scientist, visiting scientist, etc. in order to inform Customs/Border Control how the Data Holder relates to BMC.
3. **Data Description**: Describe the Data, tying it to the specific BMC-related project and giving data type, so that Customs/Border Control understands clearly what the Data is.
4. **Data Ownership**; **Authorized Possession/Use**: To assure Customs/Border Control or the FBI that the Data Holder is taking an authorized copy of the data, with ownership and secure storage remaining in the United States, the Data Holder should carry with them any agreements relating to the Data. They should have them on hand to present to Customs/Border Control or the FBI as needed. These agreements will serve as backup for the Letter. If there is a different arrangement in place, please describe, and carry those relevant agreements for support.
5. **Authorized Purpose**: Clearly describe the authorized purpose for which the Data Holder has possession of and is travelling with the Data. For example, if BMC has a collaboration agreement in place between BMC and the destination institution in the foreign country the Data Holder is travelling, and the Data Holder is transporting the Data to carry out research authorized via that agreement, describe this.
	1. If the purpose is tied to an agreement between BMC and the destination foreign institution, the Data Holder should also have in their possession a copy of such agreement and any other Data-related agreement to present to Customs/Border Control.
6. **Transfer Method**: The PI should have counseled the Data Holder (if Data Holder is not the PI) to see if the Data could be shared securely in other ways that do not involve physical travel with the Data, and travelling with the Data should be determined to be the only way to achieve the authorized research purpose. The Data must only be located on and transported via secure, BMC-vetted and approved devices for this purpose. These devices shall be as limited as possible, and shall be authorized by BMC Research Information Security (RIS) prior to travel.
7. **Travel Dates**: The Data Holder must have concrete dates of travel planned and provided to the PI for custody of the Data.
8. **Final Plan/Destination**: The PI shall provide a statement regarding the final plan and status of the Data Holder, whether they intend to and will return to BMC under the PI’s supervision, or if they will remain at the foreign institution in a separate role.
9. **Contacts**: If detained by Customs/Border Control or the FBI, the Data Holder may be questioned, in which case the detainers may require additional information before release of the detainee. Provide authorized contacts that Customs/Border Control or the FBI may contact for such purpose.
10. **Final Authorizations**: This Letter authorizing the Data Holder to possess and travel with the BMC Data must be reviewed and signed by the Principal Investigator and also reviewed and signed off on by [Chief Compliance Officer, Research Compliance, or Research Ops]. In order to receive final authorization, please provide the following information along with the request for authorization:
	1. Any agreement(s) associated with the Data
	2. Any associated IRB H#(s)
	3. Description of reasons for travel