UNIVERSITY of MARYLAND BALTIMORE

Research Advisory Task Force (COVID-19)

Committee Topic: Analysis of Electronic and Other Data Sources for Research Studies
Committee Members: J. Magaziner (Chair); C. Fraser; M. Pappas; T. Shaw
Policy Effective Date: March 18, 2020

Final UMB policy based upon the committee report and recommendations

These guidelines address electronic and non-electronic data used for research that may be confidential or sensitive, or subject to legal restrictions. This includes data about research subjects, patients, personnel, students, commercial confidential data or trade secrets, data pertaining to patentable inventions, not-yet published results, work subject to U.S. Export Control and Embargo regulations, and data subject to non-disclosure agreements, confidentiality agreements and data use agreements.

The objective of these guidelines is to ensure as much work as feasible can be performed remotely with minimum necessary limitations which include limitations specified in the UMB Step 2 Policy for working on-site, when appropriate. These recommendations are applicable immediately as well as under more restricted circumstances which may arise.

General Considerations – Ensuring Security of Electronic and Other Forms of Research Data When Used Remotely

An assessment of the security risks and needs of the research project and qualifications of the individual having access or taking custody of the data should be conducted. In instances where it is determined that secure remote access to data cannot be assured (due to system limitations, inadequate computer virus protections, no remote access via VPN or other means, data sensitivity, etc.) then remote data access (any use or transfer from the normal location of University possession) and analysis should not occur. In instances where data access, analyses and operations can be conducted, remotely researchers should perform this work using secure systems, that have up-to-date operating systems and third-party applications (i.e. Adobe, Java, Microsoft Office) that protect information including identities, individually identifiable health and demographic information and other sensitive, confidential and regulated data, and have up-to-date computer virus definitions

Secure systems include computers that are in secure locations (non-public), up to date with all the requisite security patches, up to date up-to-date computer virus definitions, and a connection to the University through a protected network (e.g. dual authentication, password protected secure networks). Remote access should be done using University supported remote connection systems such as VPN or other secure systems approved by School of University IT personnel. Under no circumstances should sensitive data be saved onto a home computer system or be made available to any person, entity, country not authorized to have access to the data under ordinary circumstances. Researchers should note that remote data access may initiate an automatic download of the data which may create a copy that should be deleted from the remote computer in a timely manner.

Special care should be taken to ensure electronic and non-electronic data is not left unattended, e.g., logged-in, unsecured and accessible to family and friends, in a vehicle (including in the trunk of a car), or carried to a location where it may be forgotten, lost or stolen. In the event of loss or unauthorized access to data, the researcher should refer to the appropriate school or campus procedures for responding to loss or breach of data.

Electronic Data

Security

For analyses and operations that can be done electronically, researchers should perform this work remotely using secure systems that protect participants' identities and have adequate computer virus protections. Public Wi-Fi systems should not be used for conducting sensitive research activities, this includes any network of unknown or suspect reliability and networks that can be utilized without a tightly restricted password. Access should be secured using University supported remote connection systems such as VPN or other secure applications.

Use of data by authorized outside vendors may continue as long as the all required security controls and procedures are followed from the site where the vendor's work is being done.

Information Technology Support Personnel

Personnel designated as responsible for maintaining electronic IT systems accessible to the University research community should be designated as essential so that they can enter University buildings when the work they need to do to assure access cannot be done remotely.

All research data users should be provided with phone and email communication protocols for IT support which may typically include appropriate centralized help desk support and other IT service structures which allow communication and service to be managed and tracked in an organized manner, particularly in the event of heavy demand.

Research units should consult with IT support personnel to plan and initiate general continuity of operations protocols, including identifying software/hardware required, installation and user training as needed for successful and efficient research data telework. Such arrangements should be in place prior an event which requires faculty and staff to engage in telework.

Bandwidth

Research units, schools and the University should consult with IT support personnel to plan and test plans, protocols and systems in advance to ensure that there is adequate bandwidth for transmission and analysis of research data from remote telework sites.

Non-Electronic Data

Security

Non-electronic data (such as data on paper forms) may be access and used remotely with permission of the School-designated Principal Investigator as long as all data with participant identifiers are transported securely and stored and used in secure workspaces. If feasible, a copy of non-electronic data should be maintained at the University in the event the data removed from the University is lost or stolen. These data should not be transported by or viewable by anyone that does not have appropriate regulatory (e.g., IRB) clearance to have possession or access to this information.

All data removed from the University should be tracked by a designated person in the research unit/laboratory, Department, Center, Institute or School. It also is recommended, at discretion of University-designated PI or based on standards established by the School or program, that there be adequate back-up documents created prior to removing documents from the University campus.

Personnel

Only those personnel needed to retrieve and return non-electronic forms of data should be authorized with on-campus access for this purpose. It is recommended that for large projects, a small number of people be designated to manage and transport research data that must be retrieved and securely provided to researchers for remote work at off campus locations.

Operational Preparations

(Must be completed no later than March 20, or sooner if remote work will be initiated earlier)

The Dean of each School will ensure compliance with these guidelines and designate personnel to oversee specific continuity of research and data protection efforts.

1. Each Unit (laboratory, Department, Center, Institute, Program, School) should designate a primary IT specialist, along with one or two back-ups, who will be responsible for maintenance of electronic systems to allow for remote data access and development and implementation of research Unit telework policies and procedures.

2. Contact information (phone and e-mail) for designated support personnel should be shared with faculty members and staff of the Unit immediately. Central IT support units of a school or the University may be designated as the appropriate point of contact.

3. Procedures for data access and troubleshooting should be developed and shared with Researchers and staff as promptly as possible to ensure secure and efficient remote data access.

4. Researchers and other personnel of the Unit must test equipment and connections immediately to ensure all those who will be working remotely with research data have access to systems with up-to-date operating systems, security patches, anti-virus, VPN connections or other secure systems.

5. Procedures for the use of University equipment taken off site should be established in consultation with School administration and IT support personnel. It is anticipated some research faculty and staff may not have the necessary equipment at home that to allow for research telework over an extended period of time. In such cases, a formal request to move computers, printers, etc. from campus to home will need to be made to and approved by the designated Unit administrator and tracked by a designated person in the laboratory, Department, Center, Institute or School.

6. In some instances, equipment needed to continue research operations cannot be moved off campus (e.g., due to size of equipment or use of equipment for clinical and research purposes). In these cases, University Phase 2 criteria for working on-site should be followed with the goal of adequately protecting research personnel from unnecessary workplace health and safety risks.

Data Analysis and Teamwork

Research data analysis is typically a team science with data preprocessing, cleaning, and quality control tasks to be undertaken before an analysis is conducted. After analysis teams will generally be involved in interpretation of study findings or design of further analysis. Use of web conferencing software should be considered along use of encrypted data storage, i.e., OneDrive and SharePoint.

During team analysis, appropriate privacy and security protocols must be followed to ensure protection of all data about research subjects, patients, personnel, students, commercial confidential data or trade secrets, data pertaining to patentable inventions, not-yet published results, work subject to U.S. Export Control and Embargo regulations, and data subject to non-disclosure agreements, confidentiality agreements and data use agreements.