UMKC
Office of Research Services

21. Research Data Security

21.1. Policy

People who volunteer to participate as subjects in research do so with the understanding that the researcher(s) will protect their identity and the information obtained about them from inadvertent or inappropriate disclosure. The principle that the Institutional Review Board (IRB) upholds in assessing the benefits and risks of the research is expressed in the Belmont report as "beneficence"— to maximize possible benefits and minimize possible harms to human subjects. As benefits and risks may be reflected in protections for privacy and confidentiality, all human subject research protocols must have in place an acceptable and documented procedure for the protection of identifiable and/or confidential information before the protocol will be approved, amended, granted continuing approval, or determined exempt from IRB review.

The purpose of this policy is to delineate the requirements for appropriate data security measures to protect the identity of and/or confidential information obtained about Individuals who participate as subjects in research.

This policy applies to all human subject research reviewed by the UMKC IRB and conducted by or under the auspices of UMKC faculty, graduate students, postdoctoral scholars, other affiliated researchers (investigators) or research conducted using UMKC resources. This policy also applies to research conducted under an Institutional Authorization Agreement (IAA) or Memorandum of Understanding (MOU) for which UMKC is the reviewing IRB. The pertinent information or data containing personally identifiable information may be (or has been) collected or stored in any form such as electronic, digital, paper, audio or video tape. This information or data may be stored within computers or equipment that is privately owned, University-owned or -maintained or reside on removable electronic media, in either case located on University premises or elsewhere.

Information Services (IS), or other centralized campus technology experts, can assist investigators to implement appropriate security measures for their research.

The IRB has a regulatory responsibility to ensure the adequacy of an investigator's provisions to maintain confidentiality of the data in human subjects research.

21.2. Definitions

21.2.1. A ***human research data set*** constitutes a body of informational elements, facts, and statistics about a living Individual obtained for research purposes. This includes information collected by an investigator through intervention/interaction with the Individual or identifiable private information obtained without intervention/interaction with the Individual.

21.2.2. ***Private information*** includes information about behavior that occurs in a context in which an Individual can reasonably expect that no observation or recording is

taking place, and information which has been provided for specific purposes by an Individual and which the Individual can reasonably expect will not be made public (e.g., a medical or school record).

21.2.3. ***Identifiable information*** means information that can be linked to specific Individuals either directly or indirectly through coding systems, or when characteristics of the information are such that by their nature a reasonably knowledgeable and determined person could ascertain the identities of Individuals.

21.2.4. ***Personal identifiers*** are any data elements that singly or in combination could be used to identify an Individual, such as a social security number, name, address, email address, demographic information (e.g., combining gender, race, job, and location), student identification numbers, or other identifiers (e.g. Hospital patient numbers). Other data elements, such as internet IP addresses, have varying degrees of potential for identifying Individuals, depending on context. These elements may also be treated as personal identifiers.

21.2.5. ***A de-identified data set*** refers to data that has been stripped of all elements or combinations of elements (including, but not limited to, personal identifiers and coding systems) that might enable a reasonably knowledgeable and determined person to deduce the identity of the subject. For example, while not directly identifiable, a dataset may include enough information to identify an Individual if elements in the dataset are combined.

21.2.6. ***A coded data set*** refers to data that has been stripped of identifiers and assigned an identity code (typically a randomly generated number) that is associated with and unique to each specific Individual that can be used to link data elements to the identity-only data set. This identity code should not offer any clue as to the identity of an Individual.

21.2.7. ***An identity-only data set*** contains any and all personal identifiers absolutely necessary for future conduct of the research and the key to the identity code that can be used to link or merge personal identifiers with the coded set.

21.2.8. ***Secure location*** refers to a place (room, file cabinet, etc.) for storing a removable medium, device, computer, or equipment wherein data sets with personal identifiers to which reside only the principal (or lead) investigator has access through lock and key (either physical or electronic keys are acceptable). Access may be provided to other parties with a legitimate need in context of the research, consistent with the policies below and as disclosed in the research protocol (see UMKC IS foundation services – storage).

21.2.9. ***Data encryption*** refers to the algorithmic transformation of a data set to an unrecognizable form from which the original data set or any part thereof can be recovered only with knowledge of a secret decryption key of suitable length, and using a suitable algorithm.

21.3. Specific Policies

The level of security necessary is relative to the risk posed to the subject should personally identifiable information be inadvertently disclosed or released as a result of malfeasance. In an effort to ensure best practice, it is always more desirable to have a higher level of security than to risk operating at a minimal standard. The IRB has the authority to decide if the security plan to protect subjects' confidentiality or anonymity appears acceptable in accordance with applicable UMKC Information Security. For data that retains identifiers, the protocol must describe adequate administrative, physical, and technical safeguards. When a study involves greater than minimal risk, investigators are encouraged to consult with appropriate information technology and security experts such as their system administrators to develop appropriate data security plans when working with personally identifiable data.

Collect the minimum identity data needed. Identifiers should only be collected if they serve a legitimate purpose in the context of the research.

De-identify data as soon as possible after collection and/or separate data elements into a coded data set and an identity-only data set. Coded data and identity-only data should always be stored separately in a secure location.

Data encryption must be used according to the University of Missouri System Information Security Data Classification System.

All transfer of electronic communications must be via SFTP or SSL (Secure Sockets Layer) protocol with encrypted usernames and passwords.

Limit access to personally identifiable information. The opportunity for human error should be reduced through: a) limiting the number of people (both users and administrators) with access to the data and ensuring their expertise and trustworthiness; and/or b) using automatic (embedded) security measures (such as storing data on non-volatile medium only in secure data-encrypted form) that are professionally installed and administered. If this computer is connected to the campus network or to the public internet, the professional administrator of the computer shall ensure that it complies with all minimum standards for network and data security listed below.

When identifiable information is stored in a personal or University-owned or -maintained computer, investigators are strongly encouraged to ensure that this computer be professionally administered and managed. If this is not possible, investigators should disclose such, and provide the IRB with a plan for how the sensitive data will otherwise be secured.

21.4. Applicable Regulations

The Office for Human Research Protections (OHRP) currently does not specify data security protections but instead requires IRBs to determine, when appropriate, that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

21.5. Additional Guidance

21.5.1. Electronic Data

When password-protecting documents and computers, secure passwords should be created. Passwords should contain at least 8 characters, a mix of upper and lower case letters, and combinations of numbers and symbols. To further protect against a possible UMKC HRPP security breach, real names, dates, phone numbers, addresses, or personally identifiable information should not be included as part of a password.

When encrypting data, there are many different encryption software options including bitlocker for windows, filevault for mac and MEO free encryption software for both mac and windows. Investigators should be sure to consult with UMKC IS, or comparable centralized campus technology experts, when determining which encryption software to use.

When collecting data online, investigators should be cautious of stored IP addresses and data that could be accessed by a third party. Investigators should make sure to encrypt identifiable data before it is transferred over a network or over email.

When using an online data collection site (e.g. Amazon Mechanical Turk, Survey Monkey, etc.), investigators should carefully review the site's data security policy. If the site stores identifiable information and/or links survey responses to Individual participants, this must be made clear in the investigator's IRB submission and in the corresponding consent document(s).

A dataset may be stored online (e.g. on a cloud storage system) only if it does not contain identifiable information or has first been encrypted so that, should there be a security breach, the data cannot be linked back to Individual participants. If considering storing data on a cloud, investigators should first consult UMKC is or centralized campus technology experts to determine which cloud computing service to use. Important considerations include:

1) data storage location;
2) backup policy;
3) deletion policy;
4) rights that the cloud provider claims for the data;
5) isolation guarantees that the provider offers.

Investigators may wish to consider using local hosting options.

21.5.2. Physical Data

Investigators should be careful to protect confidential physical records. Confidential paper records should be kept in locked file cabinets when not in use and physical access to any facility that contains confidential information should be restricted. Access control measures include smart card swipes, PIN keypads and locked doors. Investigators should be aware of who has access to keys, and should take this into account when storing data. Confidential information should not be left on copiers, fax machines, or other shared devices.

21.5.3. International Research

As the above specific policies apply, investigators need to make sure they have appropriate security measures in place while in the field, while in transit, and back at their permanent residence.

Depending on a number of factors, including political climate and availability of secure storage locations, investigators may find it difficult to maintain data security while in the field. In such circumstances, investigators are encouraged to upload their data to a cloud storage system.

When traveling across US borders, investigators should be aware that the US government can, at their discretion, take an electronic device, search through all the files, and keep it for further scrutiny. While this current policy is evolving and may change in the near future, investigators should still take special care to encrypt all confidential information on their electronic devices when traveling across US borders. It should be noted that confidential information should always be encrypted when stored on a removable medium, regardless of border crossings.

21.5.4. Mobile Storage

Mobile computing devices are devices such as tablets, smart phones, e-readers, and laptop computers. The very features that make these devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to UMKC when they contain University data. Major features of mobile devices that cause a risk to the user and potentially the University include their small size (they can be easily lost, stolen, or misplaced); weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of interconnectedness.

As mobile devices become more powerful and ubiquitous, they need to be treated with the same or greater care than personal computers. This document explains general end-user security measures that can be taken on mobile devices. Taking action to personally ensure computer security helps protect everyone from data and identity theft, viruses, hackers, and other threats. Every member of the UMKC community who uses a computing device makes UMKC's computing environment more secure by following these best practices.

21.5.4.1. General Security

Keep your mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. Airport lounges, meeting rooms, restaurants, etc.).

Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is enabled. The password used should be as strong a password as your device will support.

Enable a "remote wipe" feature if available. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.

Do not circumvent security features or otherwise "jailbreak" your mobile device.

Standard security protocols should be followed. This includes ensuring your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.

Wipe or securely delete data from your mobile device before you dispose of it.

Lost, stolen, or misplaced mobile devices should be immediately reported to the police. If your mobile device contained UMKC research data, also inform your IT department about a lost, stolen, or misplaced device.

21.5.4.2. Transmission Security

Where possible, data transmissions from mobile devices should be encrypted.

Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.

Bluetooth discovery mode should be disabled when it is not specifically needed.
If available wireless access should be configured to query the user for confirmation before connecting to wireless networks.

- For example, when Bluetooth is on, select the "check with me before connecting" option to prevent automatic connections with other devices.

Be careful when using insecure networks and use the UMKC VPN service to connect to campus resources. Most modern mobile devices are supported with proper configuration.

21.5.4.3. Application and Data Security

Do not install software from unknown sources as they may include software harmful to your device. Research the software you intend to install to make sure it is legitimate.

When installing software, review the application permissions. Modern applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.

Be careful when storing your personal data on your mobile device. If you lose the device, you could lose your data.

Follow the University's "Data Stewardship Policy" with respect to UMKC data stored on your mobile device.

21.5.5. Questions for investigators and Research Staff to Ask Themselves

- Am I collecting or retaining any identifiable data beyond what is absolutely necessary for the study, and have I destroyed identifiers that are no longer needed for my research?
- Have I replaced all personally identifiable information in my research records with a code and kept the key to identifiers separate from the records? For example, the key to identifiers is kept in a separate encrypted file or in a separate locked file cabinet.
- Do I routinely and regularly review and update my data security procedures?
- If I'm collecting sensitive information, have I consulted with information security experts to make sure my research and/or clinical data are secure from both physical and electronic theft?

Approved by: Lawrence Dreyfus, PhD
Name of University Institutional Official

_____
Signature of University Institutional Official Date