# Montclair State University(MSU) IRB Guidance Document

| | |
|---|---|
| **Guidance Document Owner:** Director, Research Compliance and Regulatory Programs and Senior IRB Coordinator<br>**Responsible Office:** IRB<br>**Document Contact:** reviewboard@montclair.edu | **Revision Date:**<br>**1/3/2019** |

**This guidance document was created to provide researchers with current data security considerations for maintaining their research data in accordance with the requirements of MSU policies and of federal, state and local laws. The majority of data is at some point collected, stored or transmitted electronically. Researchers must understand that this document encourages best practices. However, technology will consistently evolve and data security considerations will be evaluated in each protocol in accordance with risk evaluations and current technologies utilized in the research.**

**Data security considerations for research using electronic data collection or storage**

## I. Definition, Terms and Classifications of Data Security at MSU

All Montclair State University information that is stored, processed, or transmitted by any means shall be classified into one of four levels of sensitivity: Public, Internal, Confidential and Private[i]. The sensitivity classification identifies information in terms of what it is, and how that information is accessed, processed, communicated and stored. If more than one sensitivity level could apply to the information, the highest level (most restrictive) will be selected.

**Public** – (least restrictive) Information that has been declared public knowledge by University Counsel in response to a request for records under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1, et. seq. ("OPRA"), or by someone else who is duly authorized by the University to do so, and thus may be freely distributed. The disclosure, unauthorized access, or unauthorized use of Public information would not adversely impact the University, its students or staff, the state, and/or the public. Accordingly, information made public in official University publications or on the publicly available Montclair State University website may be released without special authorization.

Examples of **Public** information include:

- Faculty/staff bios
- Course catalogs
- Press releases and marketing materials
- Email sent to campus wide distribution lists, unless otherwise stated in the email Communication

**Internal** – Information that is available to business units and used for official purposes but would not be released to the public unless requested pursuant to and authorized by applicable law. The

disclosure, unauthorized access, or unauthorized use of internal information would have a limited adverse impact on the University, the State, and/or the public.

Examples of **Internal** information include:

- Financial accounting information
- Department project data such as construction plans that do not impact University security
- Unit budgets
- Purchase Orders
- Admissions metrics and statistics
- Non-public Montclair State policies and policy manuals
- Montclair State internal memos and email, non-public reports, budgets, plans, and
- Student and employee ID numbers (CWIDs) without any other identifying information

**Confidential** – Information of a sensitive nature that is available only to designated personnel. The disclosure, unauthorized access, or unauthorized use of confidential information would have a significant adverse impact on the University, the State and/or the public. Confidential information is information that is not available to the public under all applicable State and Federal laws, including but not limited to OPRA, the Family Educational Right to Privacy Act ("FERPA") and the Health Insurance Portability and Accountability Act ("HIPAA"). Release of confidential information in any way other than what is described in your research protocol must be reported to the IRB immediately as an Adverse Event.

Examples of **Confidential** information include:

- **YOUR research data**
- Certain pedagogical, scholarly and/or academic research records
- Test questions, scoring and other examination data
- Victims records
- Health information, including Protected Health Information (PHI)
- Criminal investigations, Campus Police records and evidentiary materials
- Communications with insurance carriers or risk management officers
- Social security numbers, credit card numbers, unlisted telephone numbers, and driver's license numbers
- Student records, grievance or disciplinary proceedings

**Private** – (most restrictive) All personally identifiable information (PII) pertaining to individuals that is protected by Federal or State law shall be Private. The disclosure, unauthorized access, or unauthorized use of Private information would have a significant adverse effect on the University, the State and the individuals whose information was disclosed. Exposure of certain Private information may require the University to report such exposure to various Federal and State agencies and/or Financial institutions as well as the individuals whose information was exposed. Release of private information in any way other that what is described in your research protocol must be reported to the IRB immediately as an Adverse Event.

Examples of **Private** information include:

- Social security number (SSN)
- Credit card numbers
- Personal financial information, including checking or investment account numbers
- Driver's license numbers
- Health insurance policy ID numbers

- Unlisted telephone numbers
- Student directory information that a student has requested not to be disclosed
- Student and employee ID numbers (CWIDs) combined with full names and/or birth dates
- NetID usernames or other account names combined with unencrypted password string

**II. Minimum data security for protocols involving electronic data**

- All data collection and storage devices must be password protected. See OIT password policy[i] for tips on password protections.
- Non-MSU devices for use in research should have up-to-date antivirus and protection software.
- Identifiers, linking codes or keys should be places in separate, password protected or encrypted files.
- Identifiers should not be stores on mobile devices, flash drives, or other portable devices [excludes laptop]. If the protocol deems use of a portable device as necessary than the data files should be encrypted. The PI is responsible for consulting with their departmental IT liaison to determine the most secure method(s) for portable devices.
- If using email for communication the PI should include statement(s) to the participants that email is not secure.
- No protected health information or highly sensitive information should be transmitted via email.
- PI must plan for regular back-ups of data in an encrypted format.

**III. Additional Required Data Security for Confidential or Private Information**

- The University has a site license for the Qualtrics survey system. This cloud-based tool has been vetted and authorized by the OIT and University Counsel. Other survey tools may be used but it is the responsibility of the PI to understand the "terms of service" and how data may be accessed by the vendor.
- When using Qualtrics (or other survey tools), check the option to anonymize the data collection process and do not collect the IP address. If IP addresses are necessary to the research, include in the consent process that you will be recording this information.
- All data should be transferred onto the PI's MSUfiles location or access controlled department shared drive, and should not be stored permanently on the local hard drives, flash drive devices, portable devices
- Cloud-based services such as MSU Digital Commons, Google drive or DropBox may be used if approved as such in the IRB approved protocol. It is the PI's responsibility to maintain exclusive access to other users approved for data access on the IRB protocol. It is the PI's responsibility to understand the "terms of service" for cloud storage and how data will be used by the vendor or shared with third-parties.
- Use of mobile apps for data collections is permissible. However, it is the PI's responsibility to understand the "terms of service" and how app data will be used by the vendor or shared with third-parties. The PI must relay those terms to the participant and monitor terms for updates.

- The data file used for data analysis should be free of IP addresses or other electronic identifiers. If IP addresses are collected by the survey tool, the addresses should be deleted from the downloaded data file.
- The IRB standard and regulations requires maintaining original data for three years after project completion. However, if the risk to the participant is primarily breach of confidentiality through an identifiable data record then the PI should consider, as part of the protocol, a method of deleting or destroying identifiable information (i.e. video files). Data destruction prior to the regulatory requirement must be approved by the IRB. (See OIT policy[i] on Data Usage for details on destroying files.)
- Standard security measures like encryption and secure socket layer (SSL) must be considered. Additional protections may include certified digital signatures for informed consent, encryption of data transmission, and technical separation of identifiers.
- Sharing Data with 3rd parties must be approved in the protocol and use a Data Transfer and Use Agreement (if applicable).

Related Notes:

i. Montclair Information Technology Policies http://www.montclair.edu/oit/policies/

ii. Researchers working with children online are subject to Children's Online Privacy Protection Act (COPPA – http://www.coppa.org/) in addition to human subjects regulations. Researchers are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable (likely written) parental permission. For minimal risk research written permission may be obtained by via paper mail or fax. If the research is more than minimal risk, parental permission should be obtained in a face-to-face meeting.