Investigator:

eResearch #:

OFFICE OF RESEARCH COMPLIANCE REVIEW
UNIVERSITY OF MICHIGAN

Post-IRB Approval
Electronic Data Security Questions for Investigators

Background
This document is designed to assist investigators in assessing the adequacy of data protection mechanisms in place for a given study. Each department, or school, at the university has a Security Unit Liaison (SUL) that may be able to assist investigators with this guidance. *A list of SUL's by department is available at:* safecomputing.IT Unit Security Liaison List (this link requires a U-M log-in).
If you have any questions or concerns regarding data protection mechanisms, please contact your IT Unit Security Liaison.

Data Security/Confidentiality Screening Questions
The following questions are designed to help investigators compare their study practices with best practices. Additional questions identify security issues and institutional policy requirements or recommendations. *ORCR reviews study precautions with the IRB approved data security and confidentiality precautions in Section 11 of eResearch.*

Term	Definition
Device	Per SPG 601.33, a *device* is defined as an object with the ability to engage in computational operations, including the accessing or storing of electronic data.
Sensitive Data	Per SPG 601.33, *Sensitive data* is information whose unauthorized disclosure may have serious adverse effect on the University's reputation, resources, services, or individuals. It includes information protected under federal or state regulations or subject to proprietary, ethical, or privacy considerations. (SPG) 601.33, Security of Personally Owned Devices That Access or Maintain Sensitive
Protected Health Information (PHI)	Per Michigan Medicine Policy 01-04-300, *PHI* is individually identifiable information about a patient that: 1. is created or received by a health care provider; 2. relates to the past, present, or future physical or mental health of the patient; the provision of health care to the patient; or payment for the provision of health care to the patient; and 3. identifies the patient or with respect to which there is a reasonable basis to believe it could be used to identify the patient.
Personally Owned Devices	Per SPG 601.33, *personally owned* includes devices for which a user receives a university subsidy or stipend as well as those wholly owned by the employee

Data Collection		
Question	**Answer**	**Policy/Guidance**
1. Is sensitive data collected for the purposes of this study? Sensitive data includes PHI.	Yes ◯ No ◯	• Safe Computing: Examples of Sensitive Data by Classification Level
2. If research involves PHI access or collection, how is PHI obtained?	Direct MiChart access ◯ Through Data Office ◯ Other, please specify: ◯	
3. If sensitive data is collected, what type of information is being collected?		• Safe Computing: Commonly Used Data Types in Research
4. Does the research data identify subjects "directly" (subject identifiers stored on research data), "indirectly" (stored with a code or key that links identifiers with research data), or is research data anonymized (all direct or indirect identifiers, or codes, have been destroyed before dataset received by study team)?	Direct identification ◯ Indirect identification ◯ Anonymized ◯ Other ◯	• It is a best practice to separate identifiable information from the research data. • If research data will be maintained separately, the key or code should be stored separately from both the identifiable information and the research data.
5. Is data captured electronically from subjects directly, with no hard copy data collection? For example, a subject entering survey responses on a monitor screen.	Yes ◯ No ◯ If Yes, indicate the service and device used to capture data electronically:	

Data Storage		
Question	**Answer**	**Policy/Guidance**
1. Are research data stored on password-protected servers maintained by U-M?	Yes ◯ No ◯ If no, please describe how your server is maintained:	• Refer to the Sensitive Data Guide to ensure data is stored appropriately.
2. Have, or will, data be stored on University owned devices?	Yes ◯ No ◯ If Yes, is your University owned device managed by: MiWorkspace ◯ Department IT ◯ Michigan Medicine IT ◯ Other ◯	• Safe Computing: Manage Your Workstation
3. Have or will data be stored on removable media* such as thumb drives or other portable devices*? *Portable electronic devices include laptop or other portable computers, smartphones, PDAs, mobile phones, media players, and similar electronic devices. *Removable media include USB flash drives, external disk drives, memory cards, CDs, DVDs, and other electronic, magnetic, or optical storage media that can be readily transferred from one electronic device to another.	Yes ◯ No ◯	

4. If data will be stored on portable devices or removable media, is it encrypted?	Yes ◯ No ◯	Policies: • Michigan Medicine Policy 01-04-50 requires all devices that store sensitive data to be encrypted. How to encrypt: • U-M Safe Computing: Encrypt Your Data • File encryption with USB Drives
5. Is data stored on personally owned devices, such as laptops, thumb drives or other mobile devices?	Yes ◯ No ◯ If yes, describe what procedures are in place to ensure compliance with University policies and procedures on the management of sensitive data:	Policies: • Michigan Medicine Policy 01-04-502: Security of Portable Electronic Devices and Removable Media • Michigan Medicine Policy 01-04-507: Mobile Device Security • SPG 601.33 requires workforce to secure sensitive data by properly self-managing the privacy and security settings on their personally owned device. How to secure your personal devices: • Safe Computing: Secure Your Personal Computer • Safe Computing: Sensitive U-M Data on Personal Devices • Safe Computing: Secure Your Mobile Device • Office of Chief Information Officer: Sensitive and Regulated Data - Permitted and Restricted Uses
6. Is research data backed up on a regular basis?	Yes ◯ No ◯	

Data Access		
Question	**Answer**	**Policy/Guidance**
1. Who currently has access to subject identifiers and research data? Please list name and role on research project.		Access to data and files should be restricted to members of the study team.

2. How is on-boarding and off-boarding handled when study team members are either added to the study or leave the study for any reason (e.g. terminate University employment, graduate, etc.)? **On-boarding and off-boarding checklists and other research compliance resources are available on the Compliance and Integrity webpage.**		
Transferring files and/or exchanging study files (and emailing subjects)		
Question	**Answer**	**Policy/Guidance**
1. How are data and/or files shared with collaborators?		Policies: • Michigan Medicine Policy 01-04-357: Email Communications Containing Protected Health Information (PHI) • SPG.601.07. Proper Use of Information Resources, Information Technology, and Networks • SPG 601.12: Institutional Data Resource Management Policy Guidance: • MiShare: Secure transfer of files that contain sensitive data, including those that contain (PHI) • UMHS Compliance Office: HIPAA FAQ-Email, Fax, Text Messaging, and Web
2. Do you have a policy or standard operating procedure (SOP) to cover a breach in computer security?	Yes ◯ No ◯ NOTE: You are not required to have unit-specific policies or SOPs on computer security. See links that can assist you in	Policies: • SPG 601.25. Information security incident reporting policy • Michigan Medicine Policy 01-04-385: Receiving and Resolving Privacy Complaints Guidance: • Report an IT Security Incident

	understanding institutional policies on reporting concerns.	• Michigan Medicine Report a Concern to the Compliance office • IAA Security Liaison Directory
Third Party Vendor		
1. Does this study utilize third party vendor services for collecting, managing, communicating with subjects, or storing data?	Yes ◯ No ◯ If yes, describe how this service was evaluated for security and compliance.	Guidance: • Safe computing: Third Party Vendor Security and Compliance • CIO Standard: Third Party Security and Compliance • Safe computing: Cloud Computing and Information Security

Additional Comments and/or Questions:

Completed By: Date: