Data Security Levels

Protecting the rights and welfare of human subjects is a key consideration that should guide the research design process generally and data security procedures specifically. The security levels model addresses matters of data integrity, availability, and confidentiality, and is designed to help researchers identify what type of data security measures are required for their study. All Principal Investigators (PI) are required to prepare a data security plan as part of the Franklin University IRB submission process. PIs must comply with the requirements set forth in their designated level and use their security plan to describe specific measures for data-related activities detailed in the research plan (e.g., managing Zoom interviews, configuring survey settings, etc.).

Assess the risk of your study		**Breach of confidentiality poses what level of risk:**		
		No Risk	Minimal Risk*	Greater than Minimal Risk
Data and/or subjects are:	De-Identified or Anonymous	Level 1	Level 1	Level 2
	Identifiable or Coded	Level 1	Level 2	Level 3

A breach of confidentiality may pose varying levels of risk, depending on the target population. Additionally, there is potential for a breach of confidentiality or accidental disclosure of information whenever the identities of the participants are known to the researchers. Breaches of confidentiality may include the following:

1. The participant being identified as part of the study by someone other than the study team
2. The participant's responses being connected to their identity by someone other than the study team
3. The identity of the group of participants being disclosed despite a plan that the group would not be identified (e.g., a specific group, employees of a particular organization)

Examples Per Risk Level:

- Greater than minimal risk: Health interventions with aging populations.
- Minimal risk*: Interviews and observations of families shopping for food.
- No risk: Surveys of personal opinions about business leadership style.

*The Office for Human Research Protections (OHRP) defines minimal risk as the following:

> ***Minimal risk*** means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. (45 CFR 46.102(j))

LEVEL 1 - GREEN

TYPE OF DATA

Anonymous or de-identified information; identifiable information that a subject has consented to make publicly available; or identifiable information that a subject has been assured would remain confidential, even though no harm would be expected if this information were to be disclosed.

EXAMPLES

No risk/anonymous:

- An online SurveyMonkey survey is sent out to local business managers. The survey asks about their leadership style. Data anonymization is turned on in SurveyMonkey so that no IP addresses are captured.
- An online Qualtrics survey is sent to directors of Job and Family Services offices across Ohio. The survey asks about their opinions regarding healthcare access for lower income families. Data anonymization is turned on in Qualtrics so that no IP addresses are captured.

No risk/identifiable:

- College students in Columbus are asked to participate in a short in-person interview about their experiences enrolling in classes.
- Directors of drug rehabilitation programs are asked to participate in interviews about their opinions regarding counseling practices.
- University managers are asked to play an online game to determine if it is an effective leadership training tool.

Minimal risk/de-identified:

- The researcher is collaborating with the Ohio Department of Education (ODE). ODE will send paper surveys out to math instructors at all Ohio high schools. The survey will request information about what changes they would like their administrators to make regarding curriculum. ODE will remove any identifying information before providing it to the researcher.
- The researcher is collaborating with a local college to see if new students are more likely to continue in school if they earn a 3.0 GPA or higher in their first semester. The college will generate a report and remove any identifying information before providing it to the researcher.

Minimal risk/anonymous:

- An online Qualtrics survey is sent to directors of drug rehabilitation programs. The survey asks about the director's experiences with difficult clients and situations in which they had to change their typical approach to rehabilitation. Data anonymization is turned on in Qualtrics so that no IP addresses are captured.

SECURITY REQUIREMENTS

To comply with Level 1 – Green, you must implement the following:

- Information shared and stored in a manner that provides access only to authorized individuals
- Standard controls if information is stored on a computer:
    - fully patched operating systems and applications
    - current anti-malware protection
    - firewalls
- Use of a password manager with strong and unique passwords
- Encrypted cloud storage
- Data retention plan
- Routine data back-up plan

LEVEL 2 - YELLOW

TYPE OF DATA

Individually identifiable information that, if disclosed, could reasonably be expected to be damaging to a person's reputation or to cause embarrassment.

EXAMPLES

Minimal risk/identifiable:

- The researcher will interview community college employees via Zoom at one institution in Ohio. The questions will gauge their interest in increasing and supporting diversity across campus employees.
- A drug rehabilitation clinic posts a flier in their facilities requesting that clients contact the researcher to participate in an interview. The interview will ask questions about how many times the client has started a rehabilitation program, how many times they have completed programs, and their opinion about different counseling styles that they have experienced.

Greater than minimal risk/anonymous:

- An online SurveyMonkey survey will be sent out to community college instructors across the country. The survey will include questions regarding the barriers that they face in working with their administration to better serve the student body. Data anonymization is turned on in SurveyMonkey so that no IP addresses are captured.
- A drug rehabilitation clinic sends out a Qualtrics survey to previous clients on behalf of the researcher. The survey includes questions about past illegal drug use and private health information. Data anonymization is turned on in Qualtrics so that no IP addresses are captured. The researchers will not have access to names or email addresses of clients, and the only demographic questions asked are age range, gender, and ethnicity.

SECURITY REQUIREMENTS

To comply with Level 2 – Yellow, you must implement the following:

- All Level 1 Controls, namely:
    - Information shared and stored in a manner that provides access only to authorized individuals
    - Standard controls if information is stored on a computer:
        - fully patched operating systems and applications
        - current anti-malware protection
        - firewalls
    - Use of a password manager with strong and unique passwords
    - Encrypted cloud storage
    - Data retention plan
    - Routine data back-up plan
- And the following additional controls:
    - Data is not disclosed to additional parties without prior IRB approval specifically authorizing the disclosure
    - Files containing any identifiable information, including coded identifiers are individually protected with strong encryption. (see the section labeled **Error! Reference source not found.**)

LEVEL 3 - RED

TYPE OF DATA

Information that could cause harm to an individual if disclosed, including, but not limited to, risk of criminal or civil liability, psychological harm or other injury, loss of insurability or employability, or social harm to an individual or group.

EXAMPLES

Greater than minimal risk/identifiable:

- Ohio college instructors will be approached to participate in an in-person interview. The interview will include questions regarding the barriers they face in working with their administration to better serve the student body.
- Flyers are posted in a drug rehabilitation clinic requesting that clients contact the researcher if they are interested in participating in an interview. The interview will include questions about illegal drug use and private health information. The researcher has a certificate of confidentiality from the NIH.

SECURITY REQUIREMENTS

To comply with Level 3 – Red, you must implement the following:

- All Level 1 Controls, namely:
    - Information shared and stored in a manner that provides access only to authorized individuals
    - Standard controls if information is stored on a computer:
        - fully patched operating systems and applications
        - current anti-malware protection
        - firewalls
    - Use of a password manager with strong and unique passwords
    - Encrypted cloud storage
    - Data retention plan
    - Routine data back-up plan
- All Level 2 Controls, namely:
    - Data is not disclosed to additional parties without prior IRB approval specifically authorizing the disclosure
    - Files containing any identifiable information, including coded identifiers are individually protected with strong encryption. (see the section labeled **Error! Reference source not found.**)
- And the following additional controls:
    - Local system of record storage (e.g., local server, approved cloud) whenever possible
    - Encrypted mobile computer systems or portable storage media
    - Coded data with a linked list of codes and identifiers stored separately from all coded data
    - Physical security measures for PCs and other devices that may store data, even if brief

Modified from Oregon State University's Human Research Protection Program (HRPP) and IRB.