IRB Recommendations for

RESEARCH DATA STORAGE AND SECURITY

The IRB recommends that you always use UWM-contracted data collection and storage services. Use Qualtrics for online surveys, rather than other platforms such as Google Forms or SurveyMonkey. If your data needs to be shared among multiple team members, use a UWM shared drive that is accessible only to approved research personnel. For cloud storage, use Sharepoint, UWM's OneDrive, or Teams. In addition to providing high levels of data security, our contracts require these vendors to notify us in the event of a breach, which allows us to take immediate action to ensure the confidentiality of data.

The following pages outline the IRB's specific recommendations for data storage, based on the type of data.

Data Storage and Security

The specific level and type of data security needed for any given study depends on two things: the sensitivity and identifiability of the data. Here are some general recommendations for minimum security requirements. However, you can always store the data *more* securely than suggested.

	Anonymous or de-identified	**Coded***	**Identifiable**
Not sensitive *Examples: library usage, study habits, opinions on public transportation*	No specific requirements	Computer secured with ID/password, locked file cabinet	Computer secured with ID/password, locked file cabinet
Mildly sensitive *Examples: medications taken, income levels, attitudes toward somewhat controversial topics*	Computer secured with ID/password, locked file cabinet	Computer secured with ID/password, locked file cabinet	Secure, encrypted storage; limited access, locked file cabinet UWM-contracted services/providers only for data collection and storage. Requests to use other services/providers will require approval of UWM Information Security and UWM Purchasing.
Moderately sensitive *Examples: mental illness diagnoses, attitudes of employees towards their employers, attitudes toward very controversial topics*	Computer secured with ID/password, locked file cabinet	Secure, encrypted storage; access limited to the minimum study team members necessary. Store code key in a different location from data UWM-contracted services/providers only for data collection and storage. Requests to use other services/providers will require approval of UWM Information Security and UWM Purchasing.	Secure, encrypted storage; access limited to the minimum study team members necessary. Give participants option to have their data de-identified or coded instead, and de-identify as soon as feasible. UWM-contracted services/providers only for data collection and storage. Requests to use other services/providers will require approval of UWM Information Security and UWM Purchasing.

	Anonymous or de-identified	Coded*	Identifiable
Extremely sensitive *Examples: participation in illegal activities, data from undocumented immigrants, specific details about traumatic experiences*	Secure, encrypted storage; limited access; delete recordings as soon as they are transcribed UWM-contracted services/providers only for data collection and storage. Requests to use other services/providers will require approval of UWM Information Security and UWM Purchasing.	Secure, encrypted storage; access limited to the minimum study team members necessary; delete recordings as soon as they are transcribed. Store on a non-networked computer whenever possible. Store code key in a secure, separate location from data. Encrypt electronic code keys and destroy as soon as no longer needed. Consider obtaining a Certificate of Confidentiality. UWM-contracted services/providers only for data collection and storage. Requests to use other services/providers will require approval of UWM Information Security and UWM Purchasing.	Not recommended

*"Coded" means identifiers are removed and replaced with a code. A link exists so the data can be re-identified.

Note: If you're storing data that is covered under HIPAA, work with data security / UITS to determine the appropriate storage and security.