Data Security Plan – Sample 1

The proposed study is a Level 2 risk for data security. In order to ensure unique responses, SurveyMonkey will be recording IP addresses. Although these are linked to the computer used for the survey as opposed to the individual, they are considered identifiable information for data security purposes. The survey also allows the participants to submit an optional email address in order to be provided a copy of the study results.

The following plan is in place to ensure data security in compliance with the Level 2 risk:

- Only authorized individuals will be provided access to the SurveyMonkey account used to create the survey and store the data.
- Data used for analysis will have all identifiable information permanently removed prior to performing analysis. The remaining data will not include any identifiable information and will be stored on the principal investigator's computer.
    - Following the export of the survey results, the IP addresses will be immediately and permanently deleted from the computer used to analyze the results. The IP addresses will be stored electronically on the SurveyMonkey site to ensure data retention compliance but will not be stored on any device or service outside of SurveyMonkey.
    - Following the export of the survey results, the email addresses will be immediately and permanently deleted from the computer used to analyze the results. The email addresses will be stored electronically on the SurveyMonkey site to ensure data retention compliance but will not be stored on any device or service outside of SurveyMonkey.
    - Following the conclusion of the study, the data will be downloaded again, and the email addresses will be captured. These will be used to send emails with the results of the study attached for any participant who requested the results. The results will not include any of the raw data or identifiable information. The emails will be sent individually to each requesting participant from the principal investigator's Franklin University email. After all emails have been sent, the downloaded data including the email addresses will be permanently deleted from the principal investigator's computer. The sent emails will remain in the Sent emails folder of the principal investigator, but will not include any identifiable information or data from the results other than the email address that could be used in the case of a data breach involving the Franklin University email system.
- The limited data set used for the study that has had all identifiable information removed along with the agreement to participate in the study authorizing use of the data will ensure compliance with HIPAA regulations and does not require additional written consent.
- Principal investigator's computer will be fully patched with automatic updates, current malware protection, and firewalls to protect the data. The computer will have a password manager with a strong and unique password at all times.
- The survey results will all be stored for a minimum of three (3) years through SurveyMonkey. SurveyMonkey provides encryption, data security, and data backup on this data to ensure that

all data will be protected. More details about the security measures in place can be found at https://www.surveymonkey.com/mp/legal/security/.

- All data will be retained for a minimum of three (3) years on both the SurveyMonkey site and the principal investigator's computer.
- Data will not be disclosed to any additional party without authorized written consent from the Franklin University IRB.