**NC State Research Project – IRB Information**

**Data Access and Security Plan**

This is intended to be used in accordance with the IRB [Data Management and Security Guidance](https://docs.google.com/document/d/1ttm68MoFa3hJPtB0LXfbnhqGAe_DKMfy/edit?usp=share_link&ouid=111628324854172758765&rtpof=true&sd=true)

**Faculty point-of-contact name: Justin Post**

**Additional personnel name(s): Matthew Ferrell**

**eIRB study number: 26585**

**Study title: Oral Exams at Large Scale: Lessons Learned**

**IT professional assisting with plan:** Terry Byron

*\*\* When a draft of this form is completed, submit the draft with a request through the* [***IT Service Portal***](https://ncsu.service-now.com/sp?id=sc_cat_item&sys_id=eb9cb46f1bb5d91039f40ed6624bcb8c&sysparm_category=f88bd0171bcd60d04d506288bd4bcbc2)*. You must complete this form to the best of your ability and submit it with the request. We highly suggest working with your* [*local department IT*](https://oit.ncsu.edu/help-support/#collegesupport)*.*

**Description of the data/specimens collected for this project:**

The data being collected in this study come from meeting recordings, surveys, and potentially audio recorded interviews.

**Access levels:** What are the varying access levels for this project? What can be accessed, who can access it, and why do they need to access it? You do not have to have 5 levels but they should increase in security. You should provide a clear rationale for each security level. *For example, level one may be “all research team members have access to \_\_\_” and level five may be “only the lead researcher has access to \_\_\_\_”*

* Level 1 access includes: Having access to the study design, the literature, the ongoing paper, and extracted and de identified data elements
  + Who can access this and why? All Research team members can access this, since no identifying information is included and would be sufficient for them to assist in writing and editing the study.
* Level 2 access includes: Having direct access to the data
  + Who can access this and why? The PI and the main student researcher (analyst) can because they will be engaged in analyzing it and extracting information from it to be used by the larger team

**Tracking access and verifying activities:** Describe the process of tracking how the data is accessed.

* Digital data will be stored in Google Drive
  + This storage is accessed through: an online browser
  + Access to data will be tracked as follows: by looking at the activity on google drive for each document
* The access logs for this project will be reconciled every year
  + The following person(s) will reconcile the logs Justin Post
* Describe annual data security review plan including how all equipment including hardware, software, and peripherals will be maintained with up-to-date technology and techniques: devices, computers, accessories, and peripherals: As the yearly data security training is taken, we’ll take note of best practices in the storage and securing of data. In addition, we will continue to keep our computers and google drive up to date as upgrades become available.

**Data sharing: receipt of and transfer of data:** Describe how data is from this project will be shared or transferred.

* Digital data
  + will be shared under the following circumstances: When new data is collected and needs to be shared with the analyst(s)
  + will be received through the following means: through being shared in a folder on google drive
  + will be transferred through the following means: through google drive
* Data Use Agreements or Material Transfer Agreements

☐ A Data Use Agreement IS required Describe where this is at in process

☐ A Data Use Agreement IS NOT required Detail who provided this answer

☐ An “NIH Data Management Plan” is associated with this IRB Data Access and Security Plan

☐ A Material Transfer Agreement IS required  Describe where this is at in process

☐ A Material Transfer Agreement IS NOT required Detail who provided this answer

☐ Another type of agreement is required: Detail information about this agreement

**Disposition and destruction of data:** Discuss how the data will be securely deleted.

* State how and when the data will be deleted:
  + Digital data deletion Data will be kept for 3 years, after which the project folders holding the data on google drive will be deleted manually
* State how the data will be securely deleted and destroyed from all devices, computers, accessories, printers, scanners, other peripherals, and hardcopy files: Since all data will be in google drive, in principle deleting it manually from there will be sufficient. However, we will check to see if any data has been taken off of drive. If that is the case, we will ask for it to be deleted and for proof, potentially over a zoom session.

**Data comprised of information will be securely maintained through:**

* For digital data, discuss the use of some or all personally managed devices, computers, accessories, and peripherals: Google drive with an NCSU account on personal computers
* For digital data, discuss the use of only NC State managed devices, computers, accessories, and peripherals: Google drive with an NCSU account
* Select the following digital data protection methods and describe how and when they are used for this project:

☐ Password Protection (files, folders, drives, computers etc): Passwords are used on all the personal computers, as well as when accessing google drive through an NCSU account

☐ Firewall: Click or tap here to enter text.

☐ Non-Networked devices, computers, accessories, and peripherals: Click or tap here to enter text.

☐ Use of VPN: VPN will be used while accessing identifiable data

☐ Use of 2-Factor Authentication: Accessing google drive through an NCSU account requires DFA

☐ Use of Encryption (files, folders, drives, computers etc): Click or tap here to enter text.

☐ Other: Click or tap here to enter text.

* The data will be securely maintained through the following physical means:

☐ Locked building: This space is accessed by the student researcher, and it is locked using a gate. It is secured 24/7.

☐ Locked office: This space is accessed by the PI, and is locked using a standard door lock. It is secured when not in use.

☐ Locked cabinet/drawer: How is it locked, who has access to this space, when is it secured?

☐ During transport: How is it locked, who has access to this space, when is it secured?

**Informed consent from participants**:

☐ I am seeking a waiver of informed consent for the access, storage, maintenance, use, and sharing of any data.

☐ I will get consent form participants for the storage, maintenance, use, and sharing of DE-IDENTIFIED data.

☐ I will maintain a DE-IDENTIFIED dataset that is not re-identifiable to anyone including the research team.

☐ I will maintain a DE-IDENTIFIED dataset that is re-identifiable to the research team through a master list.

☐ I understand that unless I get broad consent, I can only share de-identified data with others and

☐ I will get consent from participants for the storage, maintenance, and sharing of IDENTIFIABLE data.

☐ I understand that if I use this data for another project that is out of the scope of this project, AND that if I do not seek broad consent, that as an NC State stakeholder I will need additional IRB approval including getting additional informed consent from participants (if I do not qualify for a waiver of consent for the proposed project). This includes applying to the IRB for the use of IDENTIFIABLE secondary data and that the protocol will be reviewed via mid-level review (expedited procedures)

[**Broad consent**](https://drive.google.com/open?id=1R0fkGq4KUCydAe0y9Wft_6YGup1qAfSB) **from participants:**

☐ I will NOT seek broad consent for the storage, maintenance, use, and sharing of IDENTIFIABLE data.

☐ I will seek broad consent from participants for the storage, maintenance, use, and sharing of IDENTIFIABLE data.

☐ I will store, maintain, use, and share a DIRECTLY IDENTIFIABLE dataset for other research endeavors.

☐ I will store, maintain, use, and share a DE-IDENTIFIED dataset that is re-identifiable to the research team through a master list.

☐ I understand that because I sought broad consent at initial collection, that I must keep track of who allowed for the storage maintenance, future use, and sharing of their identifiable data and who did not.

☐ I understand that because I sought broad consent at initial collection, that as an NC State stakeholder, any time I want to access the identifiable data to answer a new research question, that I must apply to the NC State IRB for an exemption. I do not need to re-consent participants for the use of their data.

*Note: If sharing the identifiable data with other researchers, those researchers are responsible for seeking IRB approval with the appropriate IRB. You do not need IRB approval for simply sharing the identifiable data.* *Please also discuss this with your departmental Research Office as you may need a data use agreement.*

**Appendix A**

**Helpful Websites**

* [NC State Endpoint Protection Standard](https://policies.ncsu.edu/rule/rul-08-00-18/)
* [NC State Data Management Framework](https://oit.ncsu.edu/it-security/data-framework/)
* [NC State Data Classification Table with Elements and Categories](https://docs.google.com/spreadsheets/d/1cHJnpD7ObV3a48AIKcCe2AMRZ0MmN4GHkuZMAm1kljg/edit#gid=1639595516)
* [NC State University Data Use Agreements (DUA)](https://research.ncsu.edu/administration/data-use-agreements/)
* [College Level IT](https://oit.ncsu.edu/help-support/#collegesupport) Support (can help in drafting the plan to submit)
* [Secondary Data and the IRB](https://docs.google.com/document/d/1ytvLEFsIgAcZhLtvnFcNNAUyJ72IlJwP/edit?usp=share_link&ouid=111628324854172758765&rtpof=true&sd=true) (reference for IRB considerations)
* [Identifiable Datasets](https://docs.google.com/document/d/1DhQ2xDQs8daep9SKmKqiTFM6bLZFu3Tu/edit) (reference for IRB considerations)

**Ultra-sensitive or Purple Data**  
Ultra-sensitive data includes data where unauthorized disclosure or loss poses the highest risk or impact to the human subjects, university, or its affiliates or where specific data categories require special privileged access management.  Examples include social security numbers, passwords, encryption keys, and biometrics (such as fingerprints and iris scans), admitted behavior that could be considered a felony. Other examples of qualitative data that should be treated as “purple” data include data that will likely lead to arrest, detention, incarceration, deportation, physical injury, or death of both primary and third party participants. Additional access and handling requirements are required for Ultra-sensitive data because it may be impossible to repair damage caused by its unauthorized disclosure. Data Access and Security Plan required to be submitted to the IRB for review and approval.

**Highly Sensitive or Red Data**  
Highly sensitive data includes data where unauthorized disclosure or loss poses a high risk or impact to the university, or its affiliates. Examples include driver’s license, mother’s maiden name, passport, and immigration number, admitted unlawful behavior that is not considered purple. Other examples of qualitative data that should be treated as “red” data include information that could lead to persecution, harassment or retaliation, information that may or likely will irreparably harm relationships, information that will likely lead to stigmatization where physical or psychological harm may occur as a result of both primary and third party participants, or any data where unauthorized disclosure or loss poses a high risk or impact to all human subjects. Data Access and Security Plan required to be submitted to the IRB for review and approval.

**Moderately Sensitive or Yellow Data**  
Moderately sensitive data includes data where unauthorized disclosure or loss poses a moderate to low risk or impact to the university or its affiliates. Examples include date of birth, race, gender, and transcripts. Data that is created or collected within the university’s data environment without having been classified by the data stewards must be controlled at a minimum as moderately sensitive/yellow until final classification is assigned. A Data Access and Security Plan may be required to be submitted to the IRB for review and approval, IRB staff will let you know of this requirement during the review process.

**Not Sensitive or Green Data**  
Not Sensitive data includes data where unauthorized disclosure or loss poses a low risk or impact to the university or its affiliates. This information may be disclosed to individuals regardless of their university affiliation. Minimal security measures are needed to control the unauthorized modification, use, or destruction of this data. A Data Access and Security Plan may be required to be submitted to the IRB for review and approval, IRB staff will let you know of this requirement during the review process.