DATA PRIVACY AND CONFIDENTIALITY CASE STUDY INTERVIEW GUIDE

Introduction

Thank you for agreeing to participate in this interview today. My name is [name]. I work for Westat, which is a research organization based in Rockville, MD. [Introduce other staff if on the call.] We are working with the Office of Planning, Research, and Evaluation within the Administration for Children and Families (ACF), U.S. Department of Health and Human Services. The purpose of our project with ACF is to create tools that ACF, states, localities, and tribes can use to encourage data sharing while protecting data privacy and confidentiality. [Entity] has been selected as a case study site for this project. The case study will focus on the data privacy and confidentiality issues that [entity] encountered in establishing its data sharing initiative and how those issues were resolved.

Before we get started, there are a few things I should mention. This is a research project, and your participation is voluntary. We expect that the interview will take [about an hour]. We will use the information we collect through interviews to produce a case study report that will be posted on the ACF website for access by those interested in data sharing, but we will not quote by name any of the specific people interviewed for the case study. We may include those interviewed in the report acknowledgements. If we do, can we include your name and title in the acknowledgements?

[IF PERMISSION TO INCLUDE NAME AND TITLE IN ACKNOWLEDGEMENTS IS NOT GIVEN, ASK IF WE CAN AT LEAST PROVIDE THE OFFICE WHERE THEY ARE LOCATED AND THEIR POSITION TITLE OR DESCRIPTION. IF THEY DO NOT WANT TO INCLUDE EVEN THAT INFORMATION, APOLOGIZE THAT WE WILL NOT BE ABLE TO INTERVIEW THEM.]

With your permission, we would like to record the interview. The recording will be used to help us ensure our notetaking is accurate. The recordings will be accessible only to the project team at Westat, and will not be shared with others. We will destroy the recordings after the study is complete. Are you okay with us recording our interview today?

[IF PERMISSION IS GIVEN TO RECORD, BEGIN RECORDING. IF PERMISSION IS NOT GIVEN, CONTINUE THE INTERVIEW WITH THE STANDBY NOTE TAKER.]

Okay. I'd like to start the audio recording now.

Before we begin, do you have any questions for me?

DATA OWNER/DATA STEWARD (PROVIDER OF DATA)

1) Just to get started, what is your role with [entity]?

Motivation for Data Sharing

2) Why did your organization become part of this initiative to share data with the [entity]?

PROBES:

- What benefits did your organization perceive in becoming part of the data sharing initiative?
- Did your organization have any concerns about participating?
- What were the main reasons for your organization's decision to participate?

Operational Procedures

3) What data does your organization provide to the [entity]?

PROBES:

- Is the data case-level (i.e., does your organization provide data on individual cases with or without PII)?
- How is access provided to your organization's data? Is data transmitted to the [entity] or if the [entity] provided with online access to the data?
- How frequently is data transmitted or online access provided?
- What PII is included in the data your organization provides to the [entity]?
- If no PII is included, how are individual cases linked across time?

4) What are the processes for submitting/providing access to your organization's data?

PROBES:

- How is the data prepared for submission?
- How is data quality ensured?
- How is data transmitted to the warehouse?
- Does your organization provide support for data users?

5) How do your organization's IT systems support these processes in terms of ensuring that privacy and confidentiality is maintained?

Privacy and Confidentiality

6) Before agreeing to participate in [entity], did your organization have any concerns about the protection of the privacy and confidentiality of data contained in [entity]?

PROBES:

- [If yes] How were these concerns addressed or mitigated?
- Did your organization have any data privacy and confidentiality requirements for [entity] as a condition for providing data?

7) What, if any, guidance materials have proved to be most useful in helping your organization protect data from unanticipated disclosure?

8) To what extent (if any) did your organization modify data processes in order to comply with the data privacy and confidentiality required by [entity]?

9) In your organization's experience with [entity], to what extent has organization found the rules and decision-making to be transparent and fair to data owners?

PROBES:

- How have issues of transparency and fairness been addressed?

Best Practices and Lessons Learned

10) What activities related to your organization's involvement with [entity] would you describe as a best practice? (i.e., what would you recommend to others?)

11) In terms of lessons learned: Is there something you would have done differently with regard to this initiative?

PROBES:

- For instance, did your organization start down one path and then realized that it would not work?
- Have there been major changes since the initiative was started? What prompted those changes?

12) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

13) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing conducted by [entity]?

ENTERPRISE ADMINISTRATOR

1) Just to get started, how would you describe your role with [entity]?

Motivation for Data Sharing

2) What gave rise to the decision to develop your organization's data sharing initiative? What problems were stakeholders seeking to solve through this data sharing initiative?

3) Does the project have a mission or vision statement that describes the "value proposition" for your organization's initiative? [If yes] Can we get a copy?

General Description of the Initiative

4) Can you provide a few operational details about [entity]? For instance,
   - How long has [entity] been in operation
   - How many programs are providing data
   - Who are the data users (categories of users? how many users?)

5) Can you give me a general description of your organization's data sharing initiative? How does the data sharing work?

   PROBES:
   For example, can you walk us through an example that explains the lifecycle of the data, from capture to sharing, and mention any special treatments at each step to ensure privacy is protected and data confidentiality is maintained?

Stakeholders

6) Who are your organization's internal partners/external stakeholders?

7) What has been their role in defining policies and procedures for data privacy and confidentiality protection and data security?

Data Privacy and Confidentiality

8) What, if any, data privacy and confidentiality issues were raised by internal partners?

9) How were these issues addressed?

10) What, if any, data privacy and confidentiality issues were raised by external stakeholders?

11) How were the concerns of external stakeholders addressed?

12) What policies and procedures are in place to protect data privacy and confidentiality? Can you provide copies of policy documents?

13) Were there certain laws that drove or motivated the policies and procedures?

14) Where there helpful guides or materials that were useful to your organization when considering policies and procedures to protect privacy?

15) What have been the biggest challenges regarding data privacy and confidentiality?

16) What training has been provided to [entity] staff on data privacy and confidentiality?

PROBES:

- Has additional training been required as new data sources are added to the data warehouse?

Data Analytics

17) Does the data system have a dashboard? [If yes] Who has access to the dashboard?

18) Were there any data confidentiality concerns related to the dashboard during its development?

19) Do staff analysts routinely conduct any data analysis with warehouse data? If yes, please describe.

20) How is data privacy and confidentiality ensured for these analytic tasks? For data reporting?

Monitoring and Sustainability

21) What funding sources support the ongoing development and operation of [entity]?

22) What challenges (funding or otherwise) has your organization faced (or is currently facing) with regard to project sustainability?

23) Can you provide us with any data or statistics on data sharing activities such as the number of requests for data that have been received and the number granted?

24) Have you conducted any analysis or evaluation (qualitative or quantitative) of your organization's data sharing activities? Can you provide us with any reports produced?

Lessons Learned and Best Practices

25) What activities related to the development and ongoing operations of [entity] would you describe as a best practice? (i.e., what would you recommend to others?)

26) In terms of lessons learned: Is there something you would have done differently (or that you are planning to do differently in the future) with regard to the data sharing initiative's development, implementation, or operations?

PROBES:

- For instance, did your organization start down one path and then realized that it would not work?
- Have there been major changes since the initiative was started? What prompted those changes?

27) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

28) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing conducted by [entity]?

HEAD OF GOVERNANCE COMMITTEE

1) Just to get started, what is your role with [entity]?

Organization of Governance Committee

2) Please describe the structure of your Governance Committee.

PROBES:

- How many Committee members are there?
- Who do the Committee members represent?
- Are both internal partners and external stakeholders part of the Governance Committee?
- What is the structure of the Committee – are there sub-committees?
- How are responsibilities divided among Committee members?
- How often does the Committee meet? How long do meetings typically last?
- What methods (other than meetings) are used to communicate Governance Committee decisions to stakeholders?

General Strategy

3) How would you describe [the entities'] general approach to data governance?

PROBE:

- What are the key laws, standards, and guidance materials that impact Governance Committee decisions?

4) What are the Committee's overall goals for data governance?

PROBES:

- What has been achieved
- What is ongoing

5) How does the Governance Committee ensure transparency in decision making?

6) How does the Governance Committee encourage integrity in dealings with internal partners and external stakeholders?

7) Were any key decisions regarding the initiative made outside the Governance Committee? If so, what decisions were these?

Mission with Regard to Data Privacy and Confidentiality

8) Can you describe the data system's policies/procedures for data privacy and confidentiality regarding:

- Data transmission?
- Data storage?
- Data access?

- Data reporting?

9) In setting the data privacy and confidentiality policies and procedures for the above, what concerns/issues were raised by stakeholders?

10) [For each concern/issue noted] How was this issue/concern resolved?

PROBES:

- Who was part of the discussion to resolve the issue?
- Did you obtain information from external sources to help resolve the issue?
- What information resources were used?

11) What risk mitigation strategies have been instituted by the Governance Committee?

PROBES:

- Has the Governance Committee identified and evaluated risks to data privacy?
- Has the Governance Committee instituted data protections such as:
    - Pseudonymization: This is a process that allows an organization to switch the original set of data (for example, data subject's e-mail) with an alias or a pseudonym.
    - Encryption: Preserves the secrecy of both data at rest and data in transit based on mathematical algorithms that transform the original information into a random noise which can only be decrypted back if you have a decryption key.
    - Anonymization: Irreversibly alter data so that the data subject to whom the data is related to can no longer be identified.

12) How are individuals/entities held accountable for maintaining data privacy and confidentiality?

PROBE:

- What training provided for individuals regarding [entity's] data privacy and confidentiality requirements?

<u>Lessons Learned and Best Practices</u>

13) What activities in the development, implementation, or ongoing data governance operations of [entity] would your Governance Committee describe as a best practice? (i.e., what would you recommend to others?)

14) In terms of lessons learned: Is there something the Governance Committee would have done differently (or that you are planning to do differently in the future) with regard to data governance?

PROBES:

- For instance, did the [entity] start down one path and then realized that it would not work?
- Have there been major changes since the initiative was started? What prompted those changes?

15) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

16) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing conducted by [entity]?

IT ADMINISTRATOR

Okay. Also before we start, I'd like to note that the questions we'll be asking refer to the IT connected to the data sharing project and not the entire IT system you may be involved with.

1) Just to get started, how would you describe your role with [entity]?

Organization of the Information Technology team

2) Please describe to me your IT team.

PROBES:

- How many individuals are part of the overall IT team?
- What are their responsibilities?

Database structure

3) How many programs contribute data?

4) How much historical information is included in the database?

5) To what extent are data matched across programs? How is data matching across program accomplished?

6) Are relationships identified between individuals whose records are included in the database? (i.e., mother/child)

7) To what extent is PII used/stored in the data warehouse?

PROBES:

- Is PII treated differently than other data elements?
- How does the IT system support confidentiality of PII?

Data Security

8) What are the [entity's] rules/policies on:

- How data are transmitted
- How data are stored
- Access control
- Risk mitigation
- Data disposal
- Incidence response
- Audits

9) What challenges have you observed in the implementation and maintenance of these rules/policies?

10) What are the available modes of data access (microdata, tables, query tool, download centers, remote access, virtual data center)?

Data Quality

11) What does the [entity] require of data owners with regard to data quality?

12) What are the IT team activities to ensure the quality of the data?

Best Practices and Lessons Learned

13) What IT activities related to privacy and confidentiality (either directly or indirectly) would you describe as a best practice? (i.e., what would you recommend to others?)

14) In terms of lessons learned: Is there an IT activity your team or entity would have done differently (or are planning to do differently in the future) with regard to data confidentiality and privacy?

PROBES:

- Have there been major changes in how IT has handled data confidentiality and privacy since the initiative was started? What prompted those changes?

15) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

16) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing project?

LEGAL COUNSEL

1) Just to get started, what is your role with [entity]?

2) What Federal, State, or local laws were identified as relevant to the security, privacy, and confidentiality concerns of data contained in [entity]?

PROBE:
- Were there any debates over how these laws applied?

3) Were there any non-legal issues related to data security, privacy, and confidentiality that presented barriers to data sharing through [entity]?

4) Please describe any documents that you created or contributed to facilitate data sharing, while supporting the data security, privacy, and confidentiality protections of [entity]. These products may include memorandums of understanding, privacy agreements, or other data sharing documents.

5) [For each document/product developed] Please describe the process of development for these data sharing documents.

PROBES:

- Who was involved in the process (including stakeholders)?
- Did you have a model that you used to base your agreement/notice on? Where did you obtain the model from?
- Were there other information resources that you used?
- What critical issues arose/areas of disagreement?
- How were differences resolved?

6) What continuing activities are you involved in with [entity]?

7) What activities related to the development of data sharing documents would you describe as a best practice? (i.e., what would you recommend to others?)

8) In terms of lessons learned: Is there something your entity would have done differently with regard to the legal issues faced?

PROBES:
- For instance, did your organization start down one path and then realized that it would not work?
- Have there been major changes since the initiative was started? What prompted those changes?

9) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

10) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing conducted by [entity]?

DATA USER

1) Just to get started, what is your role and responsibility in relation to [entity]?

Project Information

[This project was selected in conjunction with the Enterprise administrator. Let the data user know the particular project you are interested in discussing when scheduling the interview.]

2) Can you describe for me the [project] that you worked on, which employed data accessed from [entity]?

PROBES:

- What is the project's purpose?
- What specific data was accessed from [entity]?
- What was the outcome of the project?

Obtaining Data Access

3) What process did your project go through to gain access to data from [ENTITY]?

PROBES:

- Were there forms to complete?
- Who completed these forms and who were they submitted to?
- Was there a back and forth with the data warehouse before permission was granted?
- [If yes] What kind of issues were discussed and resolved?

4) How many days/weeks/months did it take to receive access to data from [entity] after submitting the required forms and other documentation?

5) What (if any) ongoing requirements must your project meet in order to retain access to data from [entity]? For instance, audits of your project's use of the data and required staff trainings pertaining to data requirements.

Data Privacy, Confidentiality, and Security Protections

6) What kinds of assurances (if any) did your project have to make regarding the confidentiality and privacy of the shared data?

PROBES:

- Did your project make assurances regarding who would have access to the data?
    - regarding how the data would be transmitted and stored?
    - regarding the disposition of the data once your project was complete?

7) What was done to accomplish those assurances?

PROBE:

- Has your project implemented IT system procedures to provide these protections?

8) What assurances did your project make regarding the protection of data privacy, confidentiality, and security in reporting data analysis results?

Lessons Learned and Best Practices for Protecting Data

9) Based on your experience as a user of the [entity] data, what data protection procedures in the ongoing administration of [entity] would you describe as a best practice?

10) Based on your experience as a user of the [entity] data, is there any data security, privacy, and confidentiality policies or procedures that you would recommend be handled differently?

11) Are you looking forward to any future changes/enhancements to the data warehouse or its procedures?

12) If you were talking to another group that was about to start a project like [entity], do you have any other advice and/or other recommendations on resources for them?

13) Is there anything else you think it would be good for us to know regarding data confidentiality and privacy as it relates to the data sharing conducted by this project?