DATA MANAGEMENT PLAN FOR ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE

The purpose of a Data Management Plan is to outline the protocols for data storage, access, sharing, and destruction. Use the following sections to describe your Data Management Plan. You may include attachments where necessary. Cleary identify the attachment in the corresponding section. The Arkansas Center for Health Improvement will post your Data Management Plan on the Arkansas All-Payer Claims Database website with your Data Request Form. Requesters should place proprietary information in an attachment and not on this document. Attachments will not be available to view on the website.

Organization Information

Requesting Organization	Click or tap here to enter text.
Project Title	Click or tap here to enter text.
Date	Click or tap to enter a date.
Organization	Click or tap here to enter text.
Phone Number	Click or tap here to enter text.
Mailing Address	Click or tap here to enter text.
Email	Click or tap here to enter text.

Data Custodian Information

Data Custodian	Click or tap here to enter text.
Responsibilities	Click or tap here to enter text.
Office Address	Click or tap here to enter text.
Email	Click or tap to enter a date.
Phone Number	Click or tap here to enter text.
Secondary Point of Contact	Click or tap here to enter text.
Email	Click or tap here to enter text.
Phone Number	Click or tap here to enter text.

I. Physical and Environmental Security

1. Physical Access Controls

#	Instruction
1.1	Describe the physical access controls at the facility where data are stored, including security measures such as key card and biometric systems to prevent unauthorized access.
	Click or tap here to enter text.
1.2	Outline procedures for monitoring and logging access to secure areas to ensure security protocols are adhered to.
	Click or tap here to enter text.

2. Environmental Controls

#	Instruction
2.1	Does your organization have an environmental policy in place that includes comprehensive measures such as power supply and backup systems, fire protection, and temperature control to ensure continuous operation and data integrity?
	Click or tap here to enter text.

II. Data Management and Storage

1. Storage Systems

#	Instruction
1.1	Detail the types of storage media used for data (e.g., SSDs, hard drives, cloud storage) and the security measures in place for each.
	Click or tap here to enter text.
1.2	Describe the security measures and processes for handling removable media and securely disposing of or repurposing storage media. Include specifics on encryption standards for data at rest and in transit, backup procedures, and data redundancy measures.
	Click or tap here to enter text.

2. Data Location and Access

#	Instruction
2.1	Provide details of the computing environment where data will be processed and stored, including whether it is onsite, cloud-based, or a hybrid model. If applicable, describe any offsite backup locations and the security protocols governing these sites.
	Click or tap here to enter text.
2.2	Explain how data access is controlled and monitored, detailing the process for granting, reviewing, and revoking access permissions.
	Click or tap here to enter text.

III. Access Control Policies

1. Access Control

#	Instruction
1.1	Describe your organization's access control policy, including its purpose, scope, and responsibility. How does it ensure compliance with the data use agreement for Initiative Data?
	Click or tap here to enter text.
1.2	How does your organization's account management system ensure unique user accounts and periodically review user accounts? Describe the process.
	Click or tap here to enter text.
1.3	How does your organization control information flow within the system and any interconnected systems? Describe the information flow from source to destination.
	Click or tap here to enter text.

2. Specific Control Measures

#	Instruction
2.1	Discuss the implementation of multi-factor authentication and the encryption standards used for securing user credentials.
	Click or tap here to enter text.
2.2	What logical access controls (e.g., roles, groups, file permissions) does your organization use to restrict access to information?
	Click or tap here to enter text.
2.3	How does your organization's information system manage failed login attempts and account lockouts? Describe the process.
	Click or tap here to enter text.

IV. Data Sharing, Electronic Transmission, and Distribution

#	Instruction
1.1	Outline the organization’s policies on data sharing and transmission.
	Click or tap here to enter text.
1.2	Describe measures in place for secure data transfer and external access, including encryption methods.
	Click or tap here to enter text.
1.3	Indicate if any additional organizations are involved in analyzing HTI data. If so, describe how these organizations will access the data files (e.g., VPN connection, travel to physical location, or request a copy of the data files to be housed at a second location).
	Click or tap here to enter text.

V. Auditing and Accountability

#	Instruction
1.1	Describe the auditing processes in place to ensure accountability and tracking of data access and alterations.
	Click or tap here to enter text.

VI. Awareness and Training

#	Instruction
1.1	How does your organization ensure that users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems?
	Click or tap here to enter text.
1.2	Describe your organization's training programs that are used to educate staff on data protection.
	Click or tap here to enter text.

VII. Incident Response

1. Roles and Responsibilities

#	Instruction
1.1	Define roles and responsibilities for monitoring, detecting, and reporting security incidents and breaches. Detail the methods and tools employed for detection, such as intrusion detection systems and regular security audits.
	Click or tap here to enter text.

2. Incident Management

#	Instruction
2.1	Outline procedures for immediate response to detected incidents, including classification based on severity and impact. Provide step-by-step actions for containment, investigation, and mitigation, tailored to the type of incident or breach.
	Click or tap here to enter text.
2.2	Describe the internal communication strategy during an incident, including escalation paths and how information is shared within the organization.
	Click or tap here to enter text.

3. Post-Incident Handling

#	Instruction
3.1	Explain the process for system and data recovery, highlighting the use of backups and redundancy to restore operations. Detail actions taken to prevent future incidents, based on insights gained from past breaches. Describe regular reviews and updates to the incident response plan.
	Click or tap here to enter text.
3.2	Discuss how incidents are documented for compliance and auditing purposes, including maintaining logs and evidence. Outline the monitoring of compliance with both internal policies and external regulations.
	Click or tap here to enter text.

VIII. Completion of Research Tasks and Data Destruction

Your organization must ensure that it has policies and procedures in place to destroy Initiative Data upon completion of the project and that you have safeguards to ensure the data are protected when members terminate their participation in the project.

#	Instruction
1.1	Describe the policies and procedures in place to destroy the Data Files upon completion of the project.
	Click or tap here to enter text.

IX. Assurances

Please attest to the ACHI cell suppression policy of not publishing or presenting tables with cell sizes with fewer than 11 observations to anyone who is not an authorized user of the Data.

☐ **I agree.** Initial here

Data Recipients must notify ACHI, as soon as practicable, of any unauthorized use or disclosure of Initiative Data.

The undersigned agrees that the Requester and any collaborating organizations will adhere to the Data Management Plan described herein and will notify ACHI of any material changes in data management pertaining to the approved project.

Signature of Duly Authorized Representative:

- **Printed Name:**
- **Title:**
- **Original Submission Date:**
- **Revision Data Management Plan Submission Date:**