ADHS use only: HSRB #

# ARIZONA DEPARTMENT OF HEALTH SERVICES HUMAN SUBJECTS REVIEW BOARD SUBMISSION FORM

Thank you for preparing a submission for the Arizona Department of Health Services (ADHS) Human Subjects Review Board (HSRB). Our preferred submission method is our web-form, however, this form may be used if the web-form is inaccessible. Please reference the ADHS HSRB website for detailed submission instructions.

---

## PRINCIPAL INVESTIGATOR INFORMATION

Name of Principal Investigator: Date:

Organization: Type of Organization:

Organization Address:

Email Address: Telephone Number:

**STUDY TITLE/PROTOCOL NUMBER:**

**PURPOSE OR OBJECTIVE:**

Time Period of Project/Study: Does your study involve Human Subjects? Y: ☐ N: ☐

## TYPE OF SUBMISSION

☐ New Submission

☐ Five-Year Renewal HSRB Number, if known:

☐ Protocol Modification HSRB Number, if known:

For renewals and modifications, please select all that apply

☐ Change in protocol or data requested ☐ Change in data security protocols

☐ Change in Principal Investigator ☐ Other:

☐ Other:

## DATA REQUESTED (if applicable)

☐ Birth Records

☐ Death Records

☐ Hospital Discharge Database

☐ Arizona Cancer Registry

☐ Immunization Records

☐ Medical Electronic Disease Surveillance Intelligence System (MEDSIS)

☐ Other:

---

Signature of Principal Investigator Date of Submission

**Please continue to the next page,**

ADHS use only: HSRB #

# SECURITY CHECKLIST

In Arizona and nationwide, there is a growing concern about identity theft and other fraudulent use of birth and death records or other individually identifiable information.

As part of the ADHS heightened security awareness for research use of Arizona's vital records, registry data, and other confidential information collected by ADHS, the ADHS requires you to address security considerations in your research protocol or request for ADHS-maintained data. **Complete the entire following checklist to satisfy this requirement and to ensure that your paperwork has all the correct documentation.**

---

Study Title/Protocol Number:

Name of Principal Investigator:

Signature of Principal Investigator:

Today's Date:

## ACCESS CONTROLS

| | |
|---|---|
| ◯ Y ◯ N | I have identified all individuals who will be granted direct access to the data requested and their role in the project/study. I further understand that if I add such an individual to this project/study I will need to submit an additional signed confidentiality statement for that individual to the HSRB. |
| ◯ Y ◯ N | Do those individuals receive privacy/security training, and are they required to sign a confidentiality agreement with your institution or their organization's institution? |
| ◯ Y ◯ N | Will anyone else have access to the area (physical or virtual) where ADHS data will be stored (*e.g.*, non-project/study personnel, students, custodians)? |
| | Where in your protocol do you specify the controls you have in place to prevent unauthorized access to the ADHS data? (e.g., Document title and page number) |

## PHYSICAL SECURITY

For ADHS data maintained in hard copy format, please address the following security issues.

| | |
|---|---|
| ◯ Y ◯ N | Will you be maintaining any ADHS data in a **hard copy format** (*e.g.*, paper records, physical copies)? If no, please mark "No" and proceed to the ***ELECTRONIC DATA SECURITY*** section. |
| ◯ Y ◯ N | Have you established restricted access procedures for record storage areas (*e.g.*, key code devices, locked cabinets, shelving or storage rooms, etc.)? |
| ◯ Y ◯ N | Does your institution have a monitored alarm system or physical security guards to detect unauthorized entry after hours? |
| ◯ Y ◯ N | Does your institution require hard copy records containing confidential information to remain on-site? If not, please describe in your protocol/submission the procedures used to ensure the protection of hard copy records transported and used at off-site locations. |
| | Where in your protocol do you describe the procedures used to ensure the protection of hard copy data? (e.g., Document title and page number) |

**ELECTRONIC DATA SECURITY**

For ADHS data maintained in electronic format, please address the following security issues:

| | |
|---|---|
| ○ Y ○ N | Will you be maintaining any ADHS data in an **electronic copy format** (e.g. excel files, cloud-based storage, secure drive storage)? |
| | How will you be electronically maintaining the ADHS data? (Check all that apply)<br>☐ On premise server ☐ Cloud based storage ☐ SaaS platform ☐ Other: |
| ○ Y ◉ N | Will you be using a third-party vendor or service provider to host the ADHS data? |
| | If so, please name all vendors and service providers utilized to host the ADHS data: |
| ○ Y ◉ N | Do you have a written confidentiality agreement in place with the vendor and service provider(s) that prevents them from using or disclosing the hosted data for any purpose other than the hosting service? |
| ○ Y ◉ N | Are devices on which project/study personnel can access the data located in a secure area? (This includes remote access from other institutions, home, etc.) |
| | Where in your protocol do you address secure electronic data access? (e.g., Document title, page number.) |
| ○ Y ○ N | Are electronic data containing confidential information taken off-site or accessed from off-site? |
| | Where in your protocol do you describe the procedures used to ensure the protection of electronic data transported to or used from off-site locations? (Address in your protocol, as applicable, connectivity or use of a web-based system; use of privacy/security agreements; storage on laptops or devices such as flash drives or smartphones; and storage procedures at the off-site location.) (e.g., Document title and page number) |
| ○ Y ○ N | Will the system(s) and server(s) that stores the ADHS data be encrypted? (encryption at rest) |
| ○ Y ○ N | Is encryption enabled on all devices that may have access to the ADHS data? |
| ○ Y ○ N | Is encryption enabled for all transmission of the ADHS data? (encryption in transit) |
| ○ Y ○ N | Do you have a password policy that applies to all project/study personnel and vendors who may have access to ADHS data that addresses minimum password complexity, scheduled password updates, and prohibits password sharing? |
| ○ Y ○ N | Are there dual or multi-factor authentication methods employed for accessing data? |
| ○ Y ○ N | Are devices on which project/study personnel can access the data part of a network? If so, please explain in your protocol the type of computer network (e.g., VPN, LAN, WAN, etc.) that will house the ADHS data, and how you will ensure protection against unauthorized access. |
| | Where in your protocol do you address encryption, passwords, authentication, and network protection? (e.g., Document title and page number) |

## DE-IDENTIFICATION, DISCLOSURE, and DESTRUCTION

**ADHS standard for de-identification**: Individually identifiable data is any information that identifies an individual either directly or indirectly either alone or in combination with other information. ADHS considers data de-identified only if the data is stripped of all direct and indirect identifiers pursuant to the HIPAA Safe Harbor Method of de-identification (45 CFR 164.514(b)(2)) and the recipient does not have knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. Please note that an aggregated data set that contains HIPAA in-direct identifiers (such as data aggregated at the zip code level or by dates of service) is not de-identified under the HIPAA Safe Harbor Method. If you plan to release aggregated data sets that contain HIPAA in-direct identifiers please let us know.

**Disclosure of Data**: ADHS data may not be re-shared with any other entity. If you believe you have authority to re-disclose ADHS data to another entity for the purposes of this study please describe this clearly in your protocol.

**Destruction of Data**: Any physical or electronic ADHS data can be retained for up to five years from the date of the ADHS HSRB approval. Approval may be extended by requesting a renewal from the HSRB before the end of those 5 years. In the event that renewal is not granted, or upon conclusion of the study, all ADHS data (except for fully de-identified, aggregated study results) must be securely destroyed, and a certificate confirming the destruction should be sent to the HSRB.

| |
|---|
| ◯ Y ◯ N Do you plan to de-identify the ADHS data provided to you?<br>☐ The ADHS data provided to me will be already de-identified |
| What de-identification standard will be used? (Please check all that apply)<br>☐ HIPAA Safe Harbor Method of De-Identification (45 CFR 164.514(b)(2))<br>☐ HIPAA Expert Statistician Method (45 CFR 164.514(b)(1))<br>☐ HIPAA Limited Data Set Standard (45 CFR 164.514(e)(2))<br>☐ N/A |
| Where in your protocol do you address data de-identification? (e.g., Document title and page number) |
| Where in your protocol do you address data disclosures, including the disclosure of aggregated data sets or de-identified data sets as part of a deliverable or to stakeholders, partners, or other third parties? (*e.g.*, Document title and page number). If you plan to use ADHS data received for the study to create data sets or analytics that you will publicly release or share with third parties, please let us know if those data sets or analytics are: (1) fully de-identified or part of a limited data set; and (2) aggregated or patient-level. |
| ◯ Y ◯ N Does your institution destroy the hard copy records containing individually identifiable data after data entry is completed? ☐ N/A |
| ◯ Y ◯ N Are electronic records containing individually identifiable data destroyed after transfer to statistical analysis programs? ☐ N/A |
| ◯ Y ◯ N Do you agree to provide ADHS prompt proof of the complete destruction of the original data and any copies or derivative data sets that are developed from the original data upon expiration of HSRB approval or upon written request by ADHS? |
| Where in your protocol do you address data destruction? (e.g., Document title and page number) |
| Where in your protocol do you address data retention? (e.g., Document title and page number) |

## SUBMISSION REQUIREMENTS

Include the names of each file to aid in review of your application. Failure to complete may result in processing delays.

| File Name | *Required application document* |
|---|---|
| | Confidentiality statement signed and dated by the principal investigator and all researchers involved in the project |
| | Protocol for research project/study |
| | A document or spreadsheet listing the specific requested data elements |
| | Original IRB approval and the most current IRB renewals |
| | CVs for principal investigator and co-investigator(s) |
| **If applicable, include the following documents. Otherwise specify N/A.** | |
| | Copies of Consent Forms, Assent Forms |
| | Survey questionnaires |
| | |
| | |
| | |
| | |

I, _____, attest under penalty of perjury that the information stated in this form is true, accurate and complete to the best of my knowledge.

**Submit this PDF and all files above to HSRB_Protocols@azdhs.gov**