Print Form

ARIZONA DEPARTMENT OF HEALTH SERVICES

Human Subjects Review Board

SECURITY CONSIDERATIONS FOR INVESTIGATORS

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. There can be great temptations for unscrupulous persons (e.g., professional thieves or computer hackers) to obtain and use individually identifiable information unlawfully.

As part of the Arizona Department of Health Services (ADHS) heightened security awareness for research use of Arizona's vital records, registries and other confidential information, the ADHS requires you to address security considerations in your research protocol or request for ADHS-maintained data. **The following checklist may assist you to satisfy this requirement.**

ACCESS CONTROLS

☐ Yes ☐ No Have you identified all individuals who will be granted direct access to the information requested and their role in the study?

☐ Yes ☐ No Have these individuals signed the HSRB confidentiality agreement?

☐ Yes ☐ No Have you provided documentation of who is authorized to directly access confidential study data?

☐ Yes ☐ No Do those staff members receive privacy/security training, and are they required to sign a confidentiality agreement?

☐ Yes ☐ No Will anyone else have access to the area where ADHS information will be stored (e.g., students, custodians)?

☐ Yes ☐ No Are there any controls in place to prevent unauthorized access to the information?

PHYSICAL SECURITY: For ADHS records maintained in hard copy format, please address the following security issues.

☐ Yes ☐ No Have you established restricted access procedures for record storage areas (e.g., key code devices, locked cabinets, shelving or storage rooms, etc.)?

☐ Yes ☐ No Does your institution use a controlled-access vault or safe for the protection of this type of paper or electronic files?

☐ Yes ☐ No Does your institution have a monitored alarm system or physical security guards to detect unauthorized entry after hours?

☐ Yes ☐ No Does your institution destroy the hard copy records containing individually identified data after data entry is completed? If so, please identify in your protocol/submission the method of destruction to be used (e.g., shredding or incineration). If not, please explain in your protocol/submission the rationale for not destroying them.

☐ Yes ☐ No 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.

☐ Yes ☐ No Did you describe in your protocol/submission any other physical or electronic security procedures to protect hard-copy records?

ELECTRONIC DATA SECURITY: For ADHS records maintained in electronic format, please address the following security issues.

☐ Yes ☐ No Are workstations on which study personnel can access the records located in a secure area? If not, please explain in your protocol/submission.

☐ Yes ☐ No Are workstations on which study personnel can access the records part of a network? If so, please explain in your protocol/submission the type of computer network (e.g., VPN, LAN, WAN, etc.) that will house the ADHS records, and how you will ensure protection against unauthorized access (e.g., encryption, firewalls, intrusion detection or other security techniques).

☐ Yes ☐ No Is a method of authentication used to access data (e.g., passwords, passwords plus another level of authentication, etc.)?

☐ Yes ☐ No Are there scheduled updates of passwords and a policy against sharing of passwords?

☐ Yes ☐ No Are electronic records containing confidential information taken off-site or accessed from off-site? If so, describe in your protocol/submission the procedures used to ensure the protection of electronic records transported to or used from off-site locations. (Address, 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 PDAs; and storage procedures at the off-site location.)

☐ Yes ☐ No Are electronic records containing individually identified data from coding or data entry destroyed after transfer to statistical analysis programs? If not, please explain in your protocol/submission the rationale for not destroying them.

☐ Yes ☐ No Are other physical or electronic-security procedures used or planned to be used to protect electronic records?

OTHER INFORMATION PROTECTION AND SECURITY MEASURES

Please provide any additional pertinent information to the Human Subjects Review Board on how you will assure the integrity, privacy, and security of information you've requested, if applicable.