Security Policies and Procedures

Arkansas Central Cancer Registry
Arkansas Department of Health

December 2017

SECTION 1
ADH Policies and Procedures Regarding Data Security

The Arkansas Department of Health (ADH) has a standard set of general policies and procedures that all ADH employees must follow. These policies can be found in the Administration General Policies and Procedures document. There are references to sections of this document as they relate to the Arkansas Central Cancer Registry's (ACCR) security policies and procedures.

Within this document are many excerpts taken directly from the General Policies and Procedures in an effort to highlight critical efforts that should be taken to keep confidential data secure. If a topic found in the General Policies and Procedures is not found here that does not mean that it is not applicable to ACCR staff. All ACCR employees are to adhere to the General Policies and Procedures. The intent of this document is to list critical policies and provide clarification of the security policies and procedures of the ACCR.

GENERAL SECURITY

Private or mission-critical information stored and processed on computer systems must be protected against unauthorized modification, disclosure, or destruction.

Measures must be employed by users to safeguard credentials with respect to both physical security and access to ADH information systems.
GEN-11

LOGINS AND PASSWORDS

Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but, if recorded, the following rules should be observed:

- Never openly post user credentials, particularly in proximity to the user's PC.
- Store recording of credentials in a secure location.
- Do not identify the recording as a password.
- Do not include user name with password.
- Mix in false characters or scramble the password recording in a manner the user will remember so the written version is different from the real password.
- Never record a password on-line or include a password in an e-mail message.

GEN-11- GEN-12

REMOTE ACCESS

It is the responsibility of remote access users to ensure that connection to ADH information systems is not used by unauthorized persons who may have access to their devices. Users must be made aware that remote access connects from their remote site (e.g., home, facility, travel locations, etc.) to the ADH Network, so that their device becomes an extension of the network and can provide a path to expose ADH's most sensitive information. The user must take every reasonable measure to protect ADH information systems from intrusion and exposure.
GEN-16 – GEN-17

EXTRA HELP AND CONTRACTORS

Volunteers, students, extra help employees, and other individuals are informed of their obligations regarding management of private information, including the HIPAA privacy policies that pertain to their activities at ADH, during orientation. Understanding and agreement are documented using the Confidentiality Agreement (AS-32) before they are allowed to observe in or perform duties for the Agency.

ADH enters into Business Associate Agreements with applicable entities if 1) services provided involve disclosure of PHI, AND 2) functions or activities are performed on behalf of ADH. BAA requests go to the ADH Privacy Officer(s).
GEN-34

CANCER REGISTRY DATA

ACCR data is considered Level C – Very Sensitive

Data classified as being very sensitive is only available to internal authorized users and may be protected by federal and state regulations.

Very sensitive data is intended for use only by individuals who require the information in the course of performing job functions.

Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.
GEN-35 – GEN-37

E-MAIL

E-mail records are subject to ADH policies and statutes pertaining to HIPAA. Users are subject to penalties for violation of HIPAA rules and for violations of related Arkansas laws and ADH policies.

Confidentiality of e-mail cannot be assured. E-mail security should always be assumed to be reactive rather than preventive of potential malicious intrusions. Extreme caution should be exercised in using e-mail for confidential or sensitive matters.

E-mail records are subject to disclosure in response to Freedom of Information Act requests.
GEN-47

EXTERNAL STORAGE MEDIA

ADH data may only be stored on ADH issued media.

ADH data may not be stored on personal non-ADH issued media.

Due to the sensitivity level of ACCR data, any data placed on removable and/or portable storage media must be encrypted with ADH approved encryption technology and use of a complex password.

All removable and/or portable storage media must be secured in locked facilities when not in use or when not being transported.

Employees who have been issued removable and portable storage media are responsible for the security of the device and the data on the device.
GEN-94 – GEN-97

CONFLICTS OF INTEREST

Department of Health employees must perform their duties in an ethical manner. Employees must not use their position or knowledge gained from their position for private or personal advantage. Arkansas Code Annotated (ACA) §21-8-304 lists certain activities that are ethically prohibited activities for state employees and officials. If an employee becomes involved in a situation that could be considered a prohibited activity, the employee should immediately communicate all the facts to his or her immediate supervisor.
GEN-28

SECTION 2
HIPPA

The Health Insurance Portability and Accountability Act of 1996 require that health care organizations (ADH included) standardize patient health, administrative and financial data.

HIPAA allows an individual to request: a copy, an amendment, an accounting of disclosures, confidential communications, restrictions, and to inspect their protected health information. HIPAA requires that we secure any protected health information that we use, create, enter, or manage - including written, oral, and electronic data.

Current ADH HIPPA Privacy Officers:
Reggie Rogers
Warren Bankson

VIOLATION AND PENALTIES

Civil penalties can be imposed for violations:

- $100 per violation with a $25,000 annual cap on violations of any one single requirement

Criminal penalties can be imposed for violations:

- Up to $50,000 in fines and 1 year in prison for knowingly obtaining or disclosing PHI
- Up to $100,000 in fines and 5 years in prison if false pretenses are involved
- Up to $250,000 in fines and 10 years in prison if intending to sell, transfer, or use PHI for personal gain or malicious harm

BUSINESS ASSOCIATE AGREEMENT

ADH may only disclose PHI to a business associate or allow a business associate to collect, receive or use protected health information on the ADH's behalf.

ADH is required to take reasonable steps to correct any known material breach or violation of any Business Associate Agreement.

ADH employees must inform the ADH Privacy Officer/Program Consultant whenever they become aware of a material breach of a current Business Associate Agreement to which ADH is a party.
HIP-2

PROTECTING PRINTED INFORMATION

Keep photocopying of documents containing PHI to a minimum.

Shred or place unneeded copies containing PHI in a security bin.

Place any documents containing PHI with identifying information face down on counters, desks, and other places where visitors might see them. These documents should not be left out on desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas.

Remove items from fax machines, copiers, and printers promptly.

PHYSICAL SECURITY

All persons who are not authorized to have access to PHI should be supervised, escorted or observed when visiting or walking through an area where PHI may be easily viewed or accessed.

A system of controlling the distribution of keys should be used.

Doors should be locked at night, unless authorized personnel need access to the rooms or areas after hours.

Access to areas containing PHI should be monitored and controlled to the extent possible.

CONVERSATIONS

Do not discuss patient or employee information unless it is needed to perform job duties.

Do not use patients' names or the names of patients' family members in public hallways and elevators when persons who are not authorized to receive the information are present.

Make conversations in which PHI is being discussed, over the phone or in person, to the extent possible, in a manner or in a location (or both) where persons who are not intended to be a part of the conversation or who are not authorized to receive the PHI cannot overhear the conversation.

E-MAIL/FAX

Include on all e-mail messages the confidentiality statement contained in the HIPAA Privacy Requirements for E-Mail and Facsimile Services policy.

Encrypt any e-mails which contain PHI.

For messages containing PHI, the subject line must state, in whole or part, “CONTAINS PROTECTED INFORMATION”.

Use a coversheet with the word CONFIDENTIAL appearing in bold letters near the top of the form when sending PHI via fax.

Remove items from fax machines, copiers, and printers promptly.

OFFSITE

ADH employees are responsible for maintaining the privacy and security of all PHI that they may be transporting, storing or accessing off-site. This includes, but is not limited to:

- Computers or mobile devices that contain or access confidential information.
- Storage media such as diskettes, CD-ROMs, DVDs, digital memory cards, and flash drives containing confidential information.
- Printed documents that contain confidential information

SECTION 3
Disclosing ACCR Data to Facilities

You may disclose all data from an archive record back to the originating facility. Disclosure of profile (consolidated) data is not allowed even if the record was originally submitted by the requesting facility.
NOTE: The archive record is the original, unmodified data that was submitted by the facility.

Patient follow-up data such as address, vital status, date at last contact, and cause of death is allowed to be disclosed to a requesting facility if the patient record originated from there.

Information from discharge summaries may be provided to a facility if that specific discharge originated from the requesting facility.

Pathology report information may be disclosed to a requesting facility only if the report was ordered by that facility. Ordering facility should be clearly stated in the pathology report.

Information regarding a facility itself that ACCR has accumulated, including ID number, associated physicians, and file exchanges are allowed to that particular facility (or parent company) but may not be disclosed to another facility.