Arizona Medical Information Exchange Proof Of Concept

Privacy & Security Policy Manual

version 1.0

September 29, 2008

Chapter 100 – Introduction

101: Purpose and Background

This Manual describes the AHCCCS Policies that have been implemented to maintain the privacy and security of Electronic Protected Health Information (EPHI) that will be accessed by Participants using the AHCCCS Health Information Exchange (HIE) application, know as the Arizona Medical Information Exchange (AMIE).

This Manual presents policies that are applicable to AHCCCS staff, and/or Data Partners, Health Care Providers, and Authorized Users, as minimal standards.

The AHCCCS HIE is operated by AHCCCS through a Federal Medicaid Transformation Grant that includes a statewide, web-based, secure health information exchange utility.

As a Proof-of-Concept (POC), the AMIE is focused on the development and use of a statewide health information superhighway upon which AHCCCS and other statewide HIE's will be built. The POC will be piloted with a limited number of Health Care Providers in Maricopa County, be limited to the exchange and web-based display of three key medical record types for the purpose of Treatment. The initial medical record types include: hospital discharge summaries, medication history, and laboratory test results.

Specific procedures that may be required to fulfill policy objectives are found in a separate document titled "AMIE Procedures and Standards Manual." Many of these security procedures are being defined as part of an on-going process which includes participation from other local, state, and national organizations engaged in health information exchange and electronic health record initiatives.

All policy sections will be denoted as applying to AHCCCS, Data Partners, Participants, or any combination of these three.

102: Definitions (AHCCCS and External)

All definitions below are intended to comply with definitions found in 45 CFR Parts 160 and 164. Additional terms and expanded definitions used by the AHCCCS HIE Utility are included here.

AHCCCS HIE (or Utility) means the AHCCCS Health Information Exchange Utility, which is the project that is implementing the Arizona Medical Information Exchange Proof Of Concept application.

AMIE (or "Exchange") means the Arizona Medical Information Exchange Proof Of Concept application that uses a Record Locator Service to provide access to electronic health Data by use of the Viewer web application found at www.azhealthyrecord.gov

Authorized User (or User) means an individual authorized by AHCCCS HIE under a Participation Agreement to use the Exchange to access Data for a Permitted Use.

Breach, **"**Breach of the security of the system", "Breach of the security system" or "security Breach" means an unauthorized acquisition of and access to unencrypted or unredacted computerized Data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further willful unauthorized disclosure. (Arizona Revised Statutes, ARS §44-7501).

Computer Incident Response Team (CIRT) is a team of individuals trained in information security incident handling and appointed by AHCCCS management to investigate computer incidents and potential Data Breaches.

Data means protected health information provided to the Exchange by Data Suppliers. Protected Health Information is defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

Data Exchange means electronically providing or accessing Data through the AMIE.

Data Supplier means an organization, such as a hospital, clinical laboratory, pharmacy claims aggregation company, or otherwise that makes Data available for access through the AMIE and has entered into a Participation Agreement. A Data Supplier also may be a Health Care Provider.

Electronic Protected Health Information (EPHI) means Protected Health Information that is created, received, maintained or transmitted in electronic format, as defined in the HIPAA Security rule, 45 C.F.R. Part 160 and Part 164.

Health Care Provider means a physician, group practice, hospital or health system, or other health care organization or professional that provides Treatment to Patients, has been assigned an AHCCCS provider number, and has entered into a Participation Agreement with the AHCCCS HIE. A Health Care Provider also may be a Data Supplier as well as an Authorized User.

Health Information Exchange (HIE) means a multi-stakeholder entity that enables the movement of health-related Data within state, regional, or non-jurisdictional participant groups.

Participant means a Health Care Provider (HCP), or an employee of a HCP who is an AHCCCS registered Provider, and/or a Data Supplier that has entered into a Participation Agreement with AHCCCS HIE.

Participation Agreement means the agreement between a Participant and the AHCCCS HIE Utility for the purpose of a HCP's use of the AMIE, or a Data Supplier's transmission of Data through the AMIE and the submission or use of such Data.

Patient means an individual receiving medical Treatment or health care services from a Health Care Provider.

Permitted Use means the reason or reasons Participants and Authorized Users may access Data in the Exchange and use the Data included in the Exchange. For the purpose of the POC, the sole "Permitted Use" is a Health Care Provider or Authorized User's access to the Exchange to obtain Data for Treatment of Health Care Provider's Patients. If a Health Care Provider includes Data in its Medical Record, Health Care Provider and Authorized Users may use the Data only for those purposes permitted by law.

Policy means the AMIE Privacy & Security Policy Manual and the AMIE Procedures and Standards Manual.

Protected Health Information (PHI) is defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

Record Locator Service (RLS) means an information service that locates patient records across systems given a set of criteria, such as patient demographics or ID numbers.

Role Based Access Principles means providing permission to access particular Data and system functions based upon assigned User job roles.

Secure Sockets Layer (SSL) means a commonly-used protocol for managing the security of Data transmission on the Internet.

Security incident (or Incident) means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, as defined by the HIPAA Security rule, 45 C.F.R. § 164.304.

Treatment means the provision, coordination or management of health care services by one or more health care providers, as defined the HIPAA Privacy rule, 45 C.F.R. § 164.501.

Viewer means the AMIE web-browser based application designed to allow Users to search for specific patient related Data, and view a single non-aggregate record through the Exchange.

103: Privacy Officer and Privacy Contact Office (AHCCCS)

AHCCCS HIE's Privacy Officer is the AHCCCS Assistant Director (AD) for the Office of Administrative Legal Services (OALS), or Agency Privacy Officer. The Agency Privacy Officer is responsible for the development and approval of the Administration's privacy policies and procedures. This includes Agency-level as well as division-level policies and procedures. The OALS telephone number is (602) 417-4825.

104: Security Officer and Security Contact Office (AHCCCS)

AHCCCS HIE's Security Officer is the AHCCCS Assistant Director (AD) for the Information Systems Division (ISD), or Agency Information Security Officer. The Agency Information Security Officer is responsible for the development/approval of the Administration's security policies and procedures. This includes Agency-level as well as division-level policies and procedures. The Security Officer's telephone number is (602) 417-4311.

Chapter 200 - Patient Notification, Confidentiality and Privacy

201: Provision of Information to Patients (AHCCCS)

Purpose

The AHCCCS HIE Utility allows participating Health Care Providers to electronically obtain Patient Data and Protected Health Information (PHI) through a secure Record Locator Service known as the Arizona Medical Information Exchange Proof Of Concept (AMIE). This Policy describes when and how AHCCCS will provide information to Patients about the secure use of their PHI via the Exchange by Health Care Providers for the purpose of Treatment during the POC. This Policy will be revisited, and may be changed, if the AMIE expands to include additional Data, additional Health Care Providers or uses other than Treatment.

Background

Related Policies

- AHCCCS Health Information Privacy Notice (English and Spanish)

Policy

During the POC, AHCCCS HIE will use reasonable efforts to give information to all Patients about how their Protected Health Information will be included in the Exchange and how their PHI may be securely used by or disclosed to Health Care Providers for purposes of Treatment.

202: Privacy and Confidentiality (Data Partners)

Participants will maintain sufficient safeguards and procedures to maintain the privacy, security, confidentiality, and accuracy of Data. This Policy requires:

a. 128 bit SSL encryption and authentication, using certificates approved by AHCCCS HIE
b. Participant implementation of message-level security using Web Services Security (WS-Security) or other security technology acceptable to AHCCCS HIE.
c. Participant implementation of firewalls and appropriate infrastructure security safeguards per National Institute of Standards and Technology (NIST) standards.
d. Participant implementation of other safeguards to protect servers based on information security best practices per NIST standards.
e. Encrypted Data transmission between AHCCCS HIE and Participants for any Data to be used for development or testing purposes.

203: Patient Requests for HIE Access Reports (AHCCCS)

AHCCCS HIE will provide a Patient with a report detailing access to the Patient's information (as described in this Manual in section 501: Audit Logging) from the Exchange upon the Patient making a formal request of the AHCCCS Privacy Office, if the AHCCCS Privacy Office deems the disclosure is appropriate. AHCCCS HIE will also accommodate any reasonable confidential communication request made by the Patient.

204: Permitted Purpose of Access (AHCCCS, Data Partners, Participants)

An Authorized User may access Data on the Exchange for the sole purpose of Treatment of a Participant's Patients. Therefore,

a. Data Suppliers that are not Health Care Providers will not access Data through the Exchange.
b. Authorized Users may access Data based upon their role in the Treatment of Participant's Patients. Authorized Users may only access Data needed for the Treatment of Patient. This Policy is meant to restrict what Data an Authorized Users selectively accesses for purposes other than Treatment.
c. AHCCCS HIE may use or disclose Data for the following reasons:
    i. Use
        (1) Operation of the Exchange
        (2) Development and testing
        (3) Performance verification
        (4) Incident or Breach investigations
        (5) Actions relating to compliance
    ii. Disclosure
        (1) As provided for in Participation Agreement
        (2) As required by law

205: Participant Records (Participants)

The Participant may maintain a record of the Data its Authorized Users access from the Exchange used to provide Treatment to a Patient. The Participant may determine in which form to maintain its record of Data access (e.g. print out and add to permanent paper medical record, document Exchange information used to make a Treatment decision in the progress notes). When Data is incorporated into Participant's records, Participant may use and provide access to that Data as permitted by law and will protect the privacy and security of the Data as required by law.

206: Data for Development and Testing (AHCCCS)

AHCCCS HIE may use minimal datasets of EPHI for development, testing, quality assurance (QA), and any other non-production use.

a. EPHI may be manually sanitized, but must be certified as such by a knowledgeable member of the AMIE Security team.
b. If EPHI is only partially sanitized, it must be certified as not individually identifiable by a knowledgeable member of the AMIE Security team
c. EPHI may be scrambled by an automated or software process, but the mechanism used for scrambling must be made secure and not disclosed.
d. Dummy data may be created and used in place of EPHI for testing, but must be certified as such by a knowledgeable member of the AMIE Security team.

207: Non-Compliance/Sanctions (AHCCCS, Participants)

Each Participant must implement procedures to discipline and hold Authorized Users or employees of the HCP accountable for violating these Policies or using, disclosing, or requesting a Patient's Data for any reason other than Treatment.

a. Sanctions. The sanction measures must include, but not be limited to, verbal and written warnings, suspension or termination of access to the Exchange. The sanction measures may provide for retraining where appropriate.
    i. AHCCCS employees who violate the Policies contained in this Manual are subject to disciplinary action by AHCCCS, per AHCCCS Privacy and Security Policy Manual section 904: "Penalties and Enforcement", which reads, in part:
    "All AHCCCS employees, consultants and contractors must guard against the improper use or disclosure of a member's PHI. Employees who are uncertain if a disclosure is permitted are advised to consult their supervisor. If a disclosure cannot be resolved at this level, the AHCCCS Privacy Officer should be consulted. All employees are required to be aware of their responsibilities under AHCCCS privacy and security policies".
    ii. Participants who employ or contract Authorized Users must have a sanction policy in place for violations of these Policies.
    iii. An Authorized User who is an independent Participant/Provider or works for a contract physician group will be held accountable as the law permits, may forfeit their status as an AHCCCS Provider, and may be subject to formal discipline by their certifying board.
b. Reporting Non-Compliance.
    i. A Participant must require its Authorized Users or employees of the HCP to report to the Participant any noncompliance with the Participation Agreement, these Policies, or the Participant's policies on Data access, use or disclosure.

ii. A Participant must immediately report to AHCCCS HIE any noncompliance with the Participation Agreement or AMIE's or Participant's policies for Data access, use or disclosure.
iii. Each Participant must have a process for Patients to report to the Participant any noncompliance with the Participation Agreement, these Policies, and any concerns about Data access, use or disclosure.

Chapter 300 – Participant Management and Authentication

301: AMIE Authentication of Participant (AHCCCS)

All Participants must be a registered AHCCCS Provider in active status. AHCCCS HIE will authenticate a Participant using its AHCCCS Provider ID. AHCCCS HIE will cross-check the Provider ID submitted by Participant with the AHCCCS Provider list. AHCCCS HIE will not grant a Participant or its Authorized Users or employees of the HCP access to the Exchange Viewer until the Participant signs the Participation Agreement and the Authorized User or employee of the HCP signs a Viewer Account Management Form (VAM) (see section 303 of this Manual.)

302: Determination of Authorized Users (AHCCCS, Participant)

Upon request, each Participant will provide AHCCCS HIE with the name(s) and contact information of the site HIPAA Privacy and Security Officer(s). Contract physician groups will provide the name(s) and contact information of the person responsible for contracting physicians. A Participant may designate employees and agents as Authorized Users only if they will use the Data in the Exchange for the Treatment of Participant's Patients. This may include employees and agents, direct care providers (e.g. physicians, nurses) and delegates (e.g. administrative support for direct care providers) admissions personnel, and other categories of personnel that the Participant determines are involved in the Treatment of Patients, and have a need-to-know.

303: Training for Authorized Users (AHCCCS, Participant)

AHCCCS HIE will provide training and materials to Participants on appropriate use of the Exchange, which includes a review of these Policies. AHCCCS HIE will provide this training to all Authorized Users before the AHCCCS HIE permits an Authorized User or employee of the HCP any access to the Exchange. Each Authorized User must sign the attestation on the Viewer Account Management Form (VAM) signifying they have read and understand the Policies and have completed the training. Authorized Users must comply with the terms of the Participation Agreement, as well as AMIE Policies, and applicable laws.

304: Account Management of Authorized Users (AHCCCS)

After an Authorized User completes training and signs the VAM and applicable agreements, AHCCCS HIE will use the VAM Form to create an account for each Authorized User. AHCCCS HIE will issue an identifier (UserID) and temporary password for the Authorized User. All Authorized Users accessing the Exchange will only use this unique individual UserID. Under no circumstances will an Authorized User share their UserID or password. AHCCCS HIE will securely

communicate the UserID and temporary password to each Authorized User at the time of User training.

a. The UserID must point unambiguously and uniquely to the identity of a specific Authorized User.
b. AHCCCS HIE may not re-issue the same identifier to other Authorized Users, even after termination of the first Authorized User.
c. An additional authentication factor may be added in the future to complete the authentication process.

305: Authentication of Authorized Users (AHCCCS, Participants)

The AMIE will authenticate an Authorized User by means of a unique UserID and strong password. Participant may implement authentication of each Authorized User at the point of access and may implement local password policies.

306: Termination of Account or Authorization (AHCCCS, Participants)

a. Termination of Participant or Authorized User Access. AHCCCS HIE will terminate the Participant's, employee of the HCP, or Authorized User's access to the Exchange upon one of the following events:
   i. The Participant, employee of the HCP, or Authorized User fails to comply with the terms and conditions of the Participation Agreement, AMIE Policies, or applicable laws.
   ii. The Participant ceases to be a Health Care Provider.
   iii. The Participant's Participation Agreement ends for any reason.
   iv. The Authorized User, who is an employee of the HCP or part of a contracted hospital, physician group or other healthcare entity, is no longer employed or contracted by the physician group, or the individual no longer requires access to the Exchange based upon his or her job function.
   v. The Participant's status with AHCCCS changes to inactive.

b. Termination of Authorized User by AHCCCS HIE. If the action causing termination is related to the act or omission of an Authorized User or employee of the HCP rather than the Participant, AHCCCS HIE, in its sole discretion, may terminate the Authorized User directly.

c. Reasons for Termination of Authorized User. AHCCCS HIE will terminate an Authorized User's access to the Exchange upon the following:
   i. The Authorized User ceases to be an employee or agent of Participant; or,
   ii. The Authorized User fails to comply with the terms and conditions for the Participant Agreement, AMIE Policies, or applicable laws; or,
   iii. The Participant determines that the Authorized User or employee of the HCP no longer has a need to access the Exchange relating to provide Treatment to Participant's Patients; or,
   iv. AHCCCS or AHCCCS HIE requests that Authorized User's access be terminated for any reason.

d. Notice to AHCCCS HIE. A Participant will notify AHCCCS HIE immediately when the Participant determines an Authorized User or employee of the HCP's access to the Exchange is no longer required. Upon notice of termination, AHCCCS HIE will remove the Authorized User from Exchange access.
   i. Participant will notify the AMIE Operations Team immediately when an Authorized User or employee of the HCP has terminated employment, changed duties, or is otherwise no longer authorized access to the Exchange
   ii. Participants who employee Authorized Users will review its list of Authorized Users quarterly to determine if each Authorized User continues to require access to the Exchange based upon his or her job function.

Chapter 400 – Data Submission

401: Data Accuracy (Data Partners)

Data Partners will not provide the Exchange with Data that they know is inaccurate.

402: Amending Data (Data Partners)

Each Data Partner must comply with applicable federal, state and local laws and regulations regarding Patient rights to request amendment of Protected Health Information. The Data Partner must make the amended Data available to the Exchange, but is not required to affirmatively report any amendments to AHCCCS HIE or other Participants.

403: Minimum Necessary (AHCCCS)

AHCCCS HIE staff will comply with AHCCCS Privacy and Security Policy Manual section 603: "Minimum Necessary Information" in taking reasonable efforts to use or disclose or request only the minimum amount of Protected Health Information required to achieve the purpose of a particular use or disclosure. Section 603 reads, in part:
"AHCCCS will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all the information in the medical record to the requestor. Any requestor of the entire medical record should always be questioned to ensure that only the minimum necessary information is disclosed".

404: Limiting Data upon Patient Request (Data Partners)

If a Data Partner agrees to a Patient's request for restrictions on the use or disclosure of a Patient's Data, the Data Partner must comply with these restrictions when providing Data to the Exchange. If Data Partner does not have a mechanism for restricting specific Data elements, Data Partner must notify AHCCCS HIE of the limitation and work together to flag or filter the Data. If Data subject to restriction is not flagged or filtered and made available in the Exchange, the Data Partner must remove the Data or correct the record. Specific capabilities and requirements for Data Partner and AHCCCS HIE to flag, filter, or otherwise restrict Data use or disclosure, are listed in the Participation Agreement, Exhibit D (if applicable).

405: Prohibited Data (Data Partners)

Data Partner may not provide to the Exchange, Data that are subject to special protection under federal or state laws and regulations, or other requirements listed in Exhibit D of the Participation Agreement. This includes the following:

a. Substance abuse treatment information held by federally-assisted substance abuse treatment programs; and
b. Psychotherapy notes as defined by the HIPAA Privacy Standards.

Chapter 500 – Auditing and Compliance

501: Audit Logging (AHCCCS)

AHCCCS HIE will maintain audit logs documenting Authorized User access to the Viewer. The logs will include date, time, User identification, Data Provider name, and Data pointer elements (internal indexing pointing to source of record) which are transferred upon accessing the Data.

AHCCCS HIE will also maintain audit logs documenting use of the Viewer Administration Tool, which details activity by Patient, Authorized User, and Data Provider. Logs will be provided to Participants in electronic format upon request. Logs will be retained as required by HIPAA regulations.

502: Other AMIE Logging (AHCCCS)

AHCCCS HIE will maintain minimal transaction logging at all times, and verbose transaction logging on an as-needed basis. Verbose debug logging will be used to troubleshoot errors that are unresolved after reviewing transaction logs. Encryption must be used to secure any Viewer audit, transaction, or debug logging results that contain EPHI and are stored. The information gathered and stored in these logs will include:

a. System to system logging
b. Display requests from a source device and the destination device, from the perspective of the Viewer
c. Activities by each gateway, emulator, the Exchange website, and the Exchange SQL database

503: Audit Log Custody and Retention (AHCCCS)

AHCCCS is the custodian of all logs created as part of the Exchange. Audit logs and transaction log are to be retained for 7 years. Verbose transaction logs and debug logs are to be retained for no longer than 30 days.

504: Review of Audit Logs (AHCCCS)

AHCCCS HIE will develop an operational process to regularly perform manual and/or automated reviews and verification of audit logs as part of on-going operational monitoring and security practices, as defined in the HIPAA Security rule, 45 C.F.R. § 164.308(a)(1). Summary reports of access to EPHI through the Exchange, including User identification information, will be reviewed by the AMIE Operations Team. AMIE Operations will review summary reports illustrating significant events gleaned from the monitoring process. Exceptions to this policy must be documented and approved by the Agency Information Security Officer and reviewed on an annual basis.

505: Incident Reporting (AHCCCS, Data Partners, Participants)

All Incidents will be reported to the AMIE Computer Incident Response Team (CIRT) by contacting the AMIE Operations Customer Support. Procedures will be put into place to define the type of Incidents that may occur and to direct the CIRT to the appropriate steps to take to respond to the Incident. Participants will work with AHCCCS HIE and other Participants, if necessary, to detect, contain, and correct the Breach to prevent future occurrences. (See AMIE Procedures and Standards Manual, section 605.)

506: Notification of Breach (AHCCCS, Data Partners, Participants)

AMIE will report security Breaches to ISD Data Security via ISD Customer Support. ISD Data Security will comply with statewide reporting requirement, based upon the type of Breach. If applicable, AMIE Operations will report any Breaches and/or Security Incidents to the Data Provider whose Data was improperly used, accessed or disclosed within 24 hours of the discovery of the incident. Each Participant will inform AHCCCS HIE of any such Incidents within 24 hours of the discovery of the Incident. Individual patient or public notices of any Breach will be disclosed by the AHCCCS Privacy Office.

507: Mitigating Effects of Non-Compliance (AHCCCS, Data Partners, Participants)

Each Participant must implement a process to mitigate, and must take appropriate remedial action to the extent practicable, any harmful effect that is known to the Participant of improper access, use or disclosure of Data through the Exchange in violation of applicable laws, regulations and these Policies by the Participant, Authorized Users or other persons or entities. Mitigation could include Patient notification and Participant's request to the receiving Authorized User or employee of the HCP to return or destroy the impermissibly disclosed Data. AHCCCS HIE will perform a risk analysis of the non-compliance and produce an action plan for Participant remediation, which will be tracked weekly by the AMIE Security team.

508: Complaints/Investigation/ Resolution (AHCCCS, Data Partners, Participants)

AHCCCS HIE, Participants, and Data Providers each must investigate and resolve complaints they appropriately received from Patients, other Participants, or employees or contractors.

a. Patient complaints – per AHCCCS Privacy and Security Policy Manual section 315, the AHCCCS HIPAA Privacy Office is responsible for processing all HIPAA-related complaints received from AHCCCS Members, providers or employees. Section 315 reads, in part: "If a member thinks that his or her health information was disclosed to a third party inappropriately, the member may file a complaint with AHCCCS or DHHSOCR. Complaints may be filed

with AHCCCS by submitting a complaint to the Privacy Officer's office in writing".

b. Participant or AHCCCS HIE routine operational complaints - If a Participant or AHCCCS HIE staff person has a complaint about the Exchange, they should direct their complaint to the AMIE Operations Team.
c. Participant or AHCCCS HIE Privacy or Security complaints - If a Participant or AHCCCS HIE staff person has a complaint about Privacy or Security matters, they should direct their complaint to the AHCCCS Privacy or Security Office. (See sections 103 and 104 of this Manual)
d. Whistleblowers - refer to AHCCCS Privacy and Security Policy Manual section 906: Disclosure by Whistleblowers and Workforce Crime Victims, which reads, in part:
   An AHCCCS employee or business associate may disclose a member's PHI if: The AHCCCS employee or business associate believes, in good faith, that AHCCCS has engaged in conduct that is unlawful or that otherwise violates professional standards or AHCCCS policy. Disclosure may also be made if the individual believes that the care, services or conditions provided by AHCCCS could endanger AHCCCS employees, members or the public; and The disclosure is made to:
   * An oversight agency or public authority authorized by law to investigate or otherwise oversee the conduct of or conditions at AHCCCS;
   * An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by AHCCCS; or
   * An attorney retained by or on behalf of the AHCCCS employee or business associate for the purpose of determining legal options with regard to this policy.
e. Retaliation - refer to AHCCCS Privacy and Security Policy Manual section 905: Retaliatory Actions, which reads, in part:
   Neither AHCCCS nor any of its employees may intimidate, threaten, coerce, discriminate against or take any other form of retaliatory action against:
   * Any individual for exercising any right established under AHCCCS privacy and security policies, or for participating in any process established under AHCCCS policies, including the filing of a complaint with AHCCCS or DHHS-OCR;
   *Any individual or other person for:
      - Filing a complaint with AHCCCS or DHHS-OCR;
      - Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing relating to enforcement of the privacy rules by DHHS-OCR; or
      - Opposing unlawful acts or practices
f. AHCCCS HIE will notify Participant or Data Provider in writing of AHCCCS HIE concerns by contacting the executive team at the Participant or Data Provider.

Chapter 600 – Security Requirements

601: Information Systems Security (AHCCCS)

The Agency Information Security Officer will guide the creation of an information security program and produce policies and procedures with written documentation to be implemented after approval by the HIE governing body.

The goals of the information security program are:

- **Confidentiality** of information is assured.
- **Integrity** of information is maintained.
- **Availability** to information is preserved.
- **Protection** from unauthorized access is assured
- Regulatory and legislative requirements regarding intellectual property rights, Data protection and privacy of personal information are met.
- Business Continuity plans will be produced, maintained and tested.
- Staff will receive sufficient information security training.

602: Computer Incident Response Team (CIRT) (AHCCCS)

A Computer Incident Response Team (CIRT) will be named by the AMIE Project Director and will include AHCCCS HIE designees assigned as necessary to handle AHCCCS HIE and AMIE Incidents. AMIE Security and AMIE CIRT will work with ISD Data Security to investigate and resolve Data Breaches.

603: Security Risk Management (AHCCCS)

a. A risk analysis of AHCCCS HIE and the Exchange processes and technologies must be performed and documented to ensure compliance, per AHCCCS Privacy and Security Policy Manual section 907: “Risk Mitigation”, which reads:
“Each AHCCCS division, department, program or facility must mitigate, to the extent practical, any harmful effects of unauthorized uses or disclosures of PHI by its employees”.
b. Periodic reassessments of potential risks and vulnerabilities to EPHI must be conducted by AHCCCS HIE, and security measures and safeguards for EPHI must be updated to reflect any changes in the previous risk analysis.

604: Session Termination (AHCCCS)

All browser web application sessions must be configured by AMIE to automatically terminate the session if the User is idle for a period of time.

Version Information

Version 1.0 – dated 9/29/2008

Change Logs

Listed below will be significant changes to this Manual. These changes are to be reflected in the latest version. Minor changes, typographical errors, capitalizations, and other such miscellaneous changes have been made without being recorded.

Date	Section	Comment	Item	Suggested by