Policies and Procedures

for the

Privacy and Security of Health Information:

Administrative, Physical and Technical Safeguards

Data Use and Management
# Table of Contents

Purpose ......................................................................................................................................... 5  
Definitions ................................................................................................................................... 5  
Levels of Access to PHI or Other Confidential Data: ................................................................. 7  

Section I. Administrative Standards .......................................................................................... 8  
A. Allowed Use and/or Disclosure of PHI ............................................................................... 8  
   Use of PHI in Research or Other Use/Disclosure .................................................................. 9  
   Data Management and Disclosure Accounting .................................................................... 10  
B. Assigned Security and Privacy Responsibility ...................................................................... 11  
   Security Officer .................................................................................................................... 12  
   Privacy Officer ..................................................................................................................... 12  
C. Workforce Security .............................................................................................................. 13  
   Authorization and Supervision: Establishment and Modification ........................................ 13  
   Termination Procedures ...................................................................................................... 14  
D. Information Access Management .......................................................................................... 15  
   Isolating PHI on ASU Network ............................................................................................. 15  
   Access Authorization and Modification ................................................................................ 15  
E. Security Awareness and Training .......................................................................................... 15  
   Periodic Security Updates and Reminders ............................................................................ 15  
   Protection from Malicious Software ...................................................................................... 15  
   Log-in Monitoring .................................................................................................................. 16  
   Password Management ......................................................................................................... 16  
F. Incident Procedures ............................................................................................................... 17  
   Response ............................................................................................................................... 17  
   Mitigation ............................................................................................................................... 17  
   Reporting ............................................................................................................................... 18  
G. Contingency Procedures ........................................................................................................ 18
Data Backups ...............................................................................................................................18
Disaster/Emergency Recovery and Operations ..............................................................19
Testing and Revision of Contingency Procedures .........................................................20
H. Privacy and Security Management Process .................................................................20
Penalties for Violating Federal Laws ..................................................................................20
Risk Analysis and Evaluation .........................................................................................20
Risk Management .............................................................................................................21
Sanctions .............................................................................................................................21
Information System Activity Review ...............................................................................22
I. Business Associate Contracts and Other Arrangements ..............................................22
J. Amendments to Data ......................................................................................................23
K. Training ..........................................................................................................................23
L. Documentation and Recordkeeping .............................................................................24
M. Working Remotely ........................................................................................................25

Section II. Physical Safeguards ..........................................................................................26

A. Facility Security, Access Control and Validation .........................................................26

Building ...............................................................................................................................26
CHiR Office Suite ..............................................................................................................26
CHiR Office Suite Visitors .................................................................................................27
CHiR Office Suite Special Access ......................................................................................28
CHiR Server .........................................................................................................................28
Contingency Operations ....................................................................................................28
Maintenance Records ........................................................................................................28

B. Workstation Use & Security ........................................................................................29

In-Office Workstations ....................................................................................................29
External/Remote Workstations ...........................................................................................30

C. Device and media controls ..........................................................................................31
Disposal ............................................................................................................................... 31
Media Re-use ...................................................................................................................... 31
Accountability ....................................................................................................................... 31
Data backup and storage ..................................................................................................... 32

Section III. Technical Safeguards ....................................................................................... 33

A. Access Control ................................................................................................................. 33
   Unique User Identification ................................................................................................ 33
   Emergency Procedures .................................................................................................... 33
   Automatic Lockout or Logoff .......................................................................................... 33
   Encryption and Decryption .............................................................................................. 33

B. Audit Controls ................................................................................................................... 33
C. Integrity ............................................................................................................................. 33
D. Person or Entity Authentication .................................................................................... 34
E. Transmission Security ...................................................................................................... 34
Purpose

The policy of the Arizona State University (ASU) Center for Health Information & Research (CHiR) is to implement policies and procedures to regulate the use and disclosure of protected health information, electronic protected health information ("ePHI") and other confidential information received from or created on behalf of Covered Entities in a manner that meets all applicable federal, state, university, or contractual requirements. This document shall inform all CHiR workforce members (i.e., faculty, staff, students, and collaborators) of the center policies concerning privacy and security of data in order to:

1. Ensure the confidentiality, integrity, and availability of all health information that CHiR creates, receives, maintains or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security and integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law.
4. Ensure compliance with these policies by all CHiR workforce members.

Definitions

Access – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative Safeguards – Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the Covered Entity's or business associate's workforce in relation to the protection of that information.

Breach – The acquisition, access, use, or disclosure of protected health information in a manner not permitted under federal regulations, which compromises the security or privacy of the protected health information.

Business Associate – A non-member of a Covered Entity’s workforce who, on behalf of the Covered Entity or other organized health care arrangement, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information for health care operations, including, but not limited to,

\[1 45 \text{ CFR § 164.306(a); 45 \text{ CFR § 164.316(a); 45 \text{ CFR § 164.530(c).}}\]
claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; data aggregation, management, administrative, accreditation, or other services; consulting.

Citrix – An enterprise level software client under which University Technology Office provisions individual accounts that permit access to desktops, applications, servers, and data securely over a network. Authorized CHiR workforce members access PHI and other confidential data on the dedicated server via this client.

Confidentiality – The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity – A health care provider, a health plan, or a health care clearinghouse who transmits any health information in electronic form in connection with certain transactions.

De-identified Data – Data in which the 18 elements declared under HIPAA to be used to identify an individual or an individual’s relatives, employers or household members are removed.

Disclosure – The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Encryption – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Individually Identifiable Health Information – Information that is a subset of health information and 1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or is reasonably believed that the information can be used to identify the individual.

Password – Confidential authentication information composed of a string of characters.

Physical Safeguards – Physical measures, policies, and procedures to protect a Covered Entity’s or business associate’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information or PHI – Individually identifiable health information on individuals, individuals’ relatives, employers or household members that is received from a Covered Entity or created on behalf of Covered Entity by ASU.

Research – A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
Security – All of the administrative, physical, and technical safeguards in an information system.

Security incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical Safeguards – The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

University Technology Office (UTO) – The office who manages information technology throughout ASU and is responsible for network storage hardware and software, including maintenance, administration and system security.

Levels of Access to PHI or Other Confidential Data:

- **Level 1 (Full Access)** – CHiR data management staff who can access all PHI that CHiR creates, receives, maintains or transmits.

- **Level 2 (Restricted Access)** – CHiR workforce members or other researchers who can access specific PHI provided by Level 1 members or other confidential data for business needs, or when contractual or project terms permit (e.g. human resource functions, limited data sets, etc).
  - Certain Level 2 members may be given access to a folder on the CHiR server where specific PHI is provided to them by Level 1 members. Such access shall be determined by CHiR management and the CHiR Security Officer.

- **Level 3 (Low Level Access)** – CHiR workforce members who are permitted to access only de-identified data extracts that are provided by Level 1 members and stored on drives external to the server. This level also includes aggregated data from statistical analyses.

- **Level 4 (No Access)** – CHiR workforce members (i.e., administration only) who are not permitted to access any PHI, de-identified data or other confidential data maintained at CHiR.
Section I. Administrative Standards

A. Allowed Use and/or Disclosure of PHI

1. CHiR may provide the following services to the Covered Entity:
   a. Merge health information received from the Covered Entity and multiple other sources into a repository to produce useful analyses concerning the provision of health care services.
   b. Perform an analysis of the data provided by the Covered Entity in order to provide information to improve their healthcare operations and to identify ways to improve services and reduce costs.
   c. Conduct studies on behalf of the Covered Entity and/or other entities and produce reports on mutually agreed upon topics that can be generated within available resources at CHiR.
   d. Use PHI to perform data aggregation services.

2. The Covered Entity may disclose PHI to CHiR in order to create information that is not individually identifiable health information (de-identified), whether or not the de-identified information is to be used by the Covered Entity.
   a. If such use is granted in writing, then CHiR may use and/or disclose the de-identified information without any further authorization from the Covered Entity.

3. Authorized CHiR workforce members will use or disclose PHI only for those purposes necessary to perform the services above, or as otherwise expressly permitted in this policy or required by law, and will not further use or disclose such PHI.
   a. The use or disclosure of PHI shall make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.
   b. Any PHI created, received, maintained or transmitted by CHiR that has an agreed upon restriction from the original Covered Entity from which it was received shall be used or disclosed in a manner that does not violate that restriction.

---

2 45 CFR § 164.502.
3 45 CFR § 164.504(e)(2)(i)(B).
4 45 CFR § 164.514(d).
4. CHiR may use or disclose PHI for its management and administration, or to carry out legal responsibilities only after providing written notification to the Covered Entity whose data will be accessed and receiving a written response from the Covered Entity approving the use or disclosure.
   a. CHiR may disclose PHI received from the Covered Entity to a third party for such purposes only if: (1) the disclosure is required by law; or (2) CHiR secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) use or disclose the PHI only as required by law or for the purposes for which it was disclosed to the recipient; and (iii) notify CHiR of any other use or disclosure of PHI.  

Use of PHI in Research or Other Use/Disclosure

1. CHiR must notify the Covered Entity who provided the PHI or other confidential data of its intent to conduct research or otherwise use or disclose the data for an activity not requested by the Covered Entity for the purposes of the Covered Entity permitting or denying such use or disclosure of the data.
   a. The notification should be in the form of a formal request and must include the following details:
      i. Purpose of the data use/disclosure
      ii. Organization that will use or receive data or outputs from the data
      iii. Data elements/variables involved
      iv. Data analysis to be conducted
      v. Personnel involved in the activity
      vi. ASU Institutional Review Board (IRB) protocol(s) and approval(s), if required by the Covered Entity and/or stipulated in the terms of the Business Associate Agreement or other written agreement.

2. If the request is denied by the Covered Entity, then the data will not be accessed or utilized for the research project.

3. If the request is approved by the Covered Entity, then CHiR may conduct the activity according to HIPAA regulations and subject to any limitations imposed by the Covered Entity in writing and/or stipulated in the terms of the Business Associate Agreement or other written agreement.

\[\text{5 45 CFR § 164.504(e)(4).}\]
a. CHiR may use PHI for research with individual authorization by the research participant according to 45 CFR § 164.508.

b. CHiR may use PHI for research in compliance with 45 CFR § 164.512(i), which permits the use/disclosure of PHI without individual authorization by obtaining documentation of approval or exemption by the ASU IRB or Privacy Board and the IRB or Privacy Board of the Covered Entity, if required. The documentation of approval must also include board approval of an alteration or waiver of authorization.

c. Specific types of research require the following additional documentation:
   i. Reviews preparatory to research. CHiR must obtain from the researcher appropriate representations that the use/disclosure of PHI is for purposes preparatory to research according to 45 CFR § 164.512(i)(1)(ii).
   ii. Research on decedent’s information. CHiR must obtain from the researcher appropriate representations that the use/disclosure of PHI of decedents meets the criteria of 45 CFR § 164.512(i)(1)(iii).
   iii. Limited data set. CHiR may use or disclose a limited data set by entering into a data use/access agreement with the limited data set recipient in accordance with 45 CFR § 164.514(e).

4. If any PHI is accessed for use/disclosure of data without the need for IRB review (i.e., data request, reviews preparatory to research, etc.) and the data is later incorporated into a research project or used for any conference submission (abstract, poster presentation, oral presentation) or publication, then CHiR must notify the Covered Entity as stated above and obtain approval or exemption from the appropriate IRB(s) or Privacy Board(s) before the data can be used for such purpose.

Data Management and Disclosure Accounting

1. All PHI provided to CHiR must be securely transmitted, stored, and maintained with access granted only to authorized workforce members.
   a. Data must be stored electronically on CHiR’s server dedicated to the processing, analysis and storage of data and which resides in a HIPAA-compliant environment maintained by UTO.
   b. Electronic data submissions at a minimum should utilize 256-bit encryption in transmission to guard against unauthorized access or modification of data; however, CHiR’s recommended level is 1024-bit encryption, which is used by CHiR’s technical staff.
i. The only permitted means of secure transmission of data to and from CHiR are via: Secure File Transfer Protocol (SFTP), encrypted flash drive and encrypted files uploaded to a HIPAA compliant cloud-based system.

2. All PHI and other confidential data received must be logged upon receipt by Level 1 workforce members in the Data Submissions and Data Tracking database.

3. Level 1 personnel load and store the data according to pre-established procedures.

4. Data that is accessed or disclosed for any allowable use above is logged into a database maintained by CHiR management for tracking and accounting purposes.6
   a. CHiR will keep a record of any access or disclosure of data including disclosures made to its agents, subcontractors or other third parties according to the elements specified in federal law.
   b. CHiR will maintain records of such disclosures for six years from the date of disclosure and will provide such records to the Covered Entity within a reasonable time period upon Covered Entity’s request or per the terms of the Business Associate Agreement or other written agreement.
      i. CHiR shall immediately forward any requests received from individuals requesting an accounting of disclosures of their PHI to the Covered Entity for action.

B. Assigned Security and Privacy Responsibility

ASU appoints the university Security Officer and Privacy Officer. ASU requires each of its “covered components” to designate an internal Security Officer7 and a Privacy Officer8.

1. CHiR management will appoint a Security Officer from the data management personnel and a Privacy Officer for a term of one year, generally the university fiscal year.

2. Upon acceptance of the appointment and signing of the appointment letter, CHiR management will:
   b. Provide a copy of the appointment letter to the ASU Security and Privacy Officers for their records.

---

6 45 CFR § 164.528(b); 45 CFR § 164.504(e)(2)(ii)(G).
7 45 CFR § 164.308(a)(2).
8 45 CFR § 164.530(a).
**Security Officer**

The Security Officer has the following responsibilities:

1. The development, implementation and maintenance of policies and procedures necessary for CHiR to comply with the HIPAA Security Rule, including those necessary to establish and maintain administrative, physical, and technical security safeguards and to prevent, detect, contain and correct security violations.
2. Monitoring CHiR workforce members and operations for compliance with the HIPAA Security Rule.
3. Ensuring that all appropriate workforce members are trained concerning requirements of the HIPAA Security Rule.
4. Receiving, investigating, and resolving complaints concerning CHiR’s compliance with the HIPAA Security Rule.
5. Carrying out these responsibilities in accordance with applicable Arizona Board of Regents and ASU policies and procedures and in consultation with the ASU Security Officer.

**Privacy Officer**

The Privacy Officer has the following responsibilities:

1. The development and implementation of policies and procedures necessary for CHiR to comply with the HIPAA Privacy Rule.
2. Surveying and monitoring CHiR’s compliance with the HIPAA Privacy Rule.
3. Ensuring that all appropriate workforce members are trained concerning requirements of the HIPAA Privacy Rule.
4. Receiving, investigating, and resolving complaints concerning CHiR’s compliance with the HIPAA Privacy Rule.
5. Carrying out these responsibilities in accordance with applicable Arizona Board of Regents and ASU policies and procedures and in consultation with the ASU Privacy Officer.
C. Workforce Security

**Authorization and Supervision: Establishment and Modification**

1. It shall be the responsibility of the CHiR Privacy and Security Officers to verify and document that each workforce member has received appropriate training on all policies regarding information security and HIPAA regulations before access to PHI or other confidential data is granted.
   a. Each workforce member accessing PHI or other confidential data must be approved and verified no less frequently than biannually (every six months).
   b. The CHiR Security Officer will review all workforce member access to all electronic applications (i.e., Citrix) and network drives (i.e., Data, Admin, Projects) to determine whether access is appropriate or may have been used inappropriately.
      i. Changes will be made to individual access as needed.
      ii. Further investigations into access that may have been used inappropriately will be conducted according to the Incident Procedures in this policy.
      iii. Results will be documented and filed.

2. The CHiR Security Officer will assign a data access level to each workforce member based on the level of data that is required for their job duties or “need to know” basis. The data access level for each workforce member will be changed as duties change.
   a. The CHiR Security Officer will notify the assigned UTO contact of the appropriate data access level, which the UTO contact will grant on the Citrix application.
      i. Workforce members who will have Level 1 access will require a two-step process of approval and setup between the CHiR Security Officer and UTO before access is granted.
      ii. Workforce members who will have Level 2 access can be approved and setup by the CHiR Security Officer.
   b. Workforce members’ access level is authenticated upon logging into Citrix. After logging into Citrix, Level 2 members will be denied access to any folders on Citrix to which they have not been assigned. Level 3 and Level 4 members will be denied access upon attempts to log into Citrix.

---

9 45 CFR § 164.308(a)(3).
c. The workforce member access level will remain in effect until the CHiR Security Officer authorizes a change in access level or removal of access.
   i. Workforce members with Level 1 access can be changed or removed via a two-step process between the CHiR Security Officer and UTO.
   ii. Workforce members with Level 2 access can be removed by the CHiR Security Officer.

**Termination Procedures**

1. When a workforce member is leaving employment at ASU or as a CHiR workforce member and no longer needs access to PHI or other confidential data, the CHiR Security Officer and Administrator will be notified of the status change by CHiR management.
   a. The CHiR Security Officer will request that UTO remove access to the server for Level 1 and Level 2 members by the date specified, which may also be the same as the date of the request.
   b. CHiR administration will perform the following tasks by the date of termination or earlier, if required: 1) request deactivation of the terminating workforce member’s computer accounts, electronic door access, and building access; 2) request a reset of the workforce member’s voicemail by UTO; 3) remove CHiR calendar access; and 4) notify appropriate customers of the staffing change and provide an interim or permanent contact for business matters.
   c. The terminating workforce member must return all university property for inventory, including sun card, laptop, office keys, and any other equipment to authorized university staff by the date of termination.
   d. The CHiR Security Officer and CHiR administration will conduct a final briefing no later than one week post termination to verify successful completion of all tasks that are performed and resolve any remaining items.

2. When a project ends, the CHiR Security and Privacy Officers shall meet to determine any changes to data access for project team members and security of any data used in the project, which may include the following:
   a. Removal of or redefining access to the server.
   b. Removal of or redefining electronic door access.
   c. Archival of project data or files.
D. Information Access Management

Isolating PHI on ASU Network
1. All electronic data files containing PHI shall be processed, analyzed, and stored only on the secure server allocated to CHiR through Citrix by UTO.
2. The CHiR server shall remain distinct from the rest of the ASU network with no access via general logging into the ASU network or Citrix.

Access Authorization and Modification
1. All workforce members accessing data on the CHiR server must be approved and verified by the CHiR Security Officer at regular intervals, but no less frequently than biannually.
2. Only workforce members who have been approved by the CHiR Security Officer shall be able to log into Citrix and access the CHiR server.
   a. Level 1 members shall have access to all folders on the CHiR server.
   b. Level 2 workforce members can access only the specific data folders on the CHiR server that are assigned to them by the CHiR Security Officer.
   c. Access shall be updated as workforce members with Level 2 access begin or end projects/studies that require such access.

E. Security Awareness and Training

Periodic Security Updates and Reminders
1. Security updates will be communicated to workforce members as implemented by the CHiR Security Officer. Additional training will be provided as needed.
2. Periodic reminders of security procedures will be sent to workforce members by CHiR administration, especially in preparation for special events, building or suite maintenance that will impact security, or office closings due to holidays or shutdowns.

Protection from Malicious Software
1. UTO monitors all network traffic to guard against, detect, or report malicious software trying to access the ASU network. The CHiR Security Officer will work with UTO to

---

10 45 CFR § 164.308(a)(4).
11 45 CFR § 164.308(a)(5).
mitigate any effects to CHiR’s servers or data and will notify CHiR management and other workforce members as appropriate.

2. All workforce members are required to maintain updated anti-virus software on their individual workstations. Computer systems that are owned by the University will utilize University endorsed anti-virus software. Options are available on the ASU website: http://getprotected.asu.edu/.
   a. It is recommended that each user schedule their computer to automatically check for updates daily.

3. It is encouraged that computer systems not owned by the University utilize University endorsed anti-virus to ensure that proper assistance can be obtained should issues regarding the anti-virus arise.
   a. Those computer systems found utilizing the University network without proper anti-virus software will be removed from the network immediately by UTO and required to install the appropriate anti-virus solution before network access is restored.

Log-in Monitoring

1. All Citrix and CHiR server access attempts are logged electronically by UTO.
2. The CHiR Security Officer shall regularly review the logs to determine both appropriate and inappropriate access as well as security incidents.
   a. Upon discovery of inappropriate access, the CHiR Security Officer will implement the procedures under Section C: Authorization and Supervision: Establishment and Modification.
   b. Upon notice of a security incident, the CHiR Security Officer will follow procedures under Section F: Incident Procedures.

Password Management

1. In order to access the ASU network, each workforce member shall maintain a strong, distinct, individual ASURITE password of the following criteria:
   a. Password must contain at least ten characters with at least three of the following: special characters, upper case letters, lower case letters, and numbers.
   b. Password must be secured and not revealed to anyone or stored in any form.
   c. Password must be changed at regular intervals, and password should never be reused or recycled. (NOTE: The ASU password change program will not allow
users to re-use the last 10 passwords, and once the password is changed, users will not be allowed to change it again within the next 10 minutes.

i. Workforce members with Level 1, Level 2 or Level 3 access must change their password every three months. A designated CHiR workforce member will send out a reminder quarterly to these workforce members and require written verification of the change by a defined due date. An electronic file of the quarterly password changes shall be maintained on the CHiR administrative network drive for up to six (6) years.

2. Any additional, individual passwords required to access particular systems within the ASU network should adhere to the above standards or as prescribed for that particular system.

3. Any passwords suspected of being compromised must be reported to the ASU Help Desk and CHiR management immediately and all passwords changed.

F. Incident Procedures\(^\text{12}\)

Response

1. CHiR workforce members and any external person or entity must report a suspected or actual incident affecting the privacy and/or security of PHI immediately upon discovery to the CHiR Privacy or Security Officers and CHiR management.

2. Upon notice of an incident, the CHiR Privacy and/or Security Officers will perform any mitigation procedures that are immediately necessary to secure protected health information or other confidential data and prevent further harm.\(^\text{13}\) Simultaneously, they will open an investigation to determine whether an actual event of unauthorized use or disclosure of data has occurred, including the following:
   a. Interviewing individuals involved.
   b. Gathering supporting documentation.
   c. Reviewing all applicable policies and procedures to determine any violations.
   d. Documenting investigation process and outcome.

Mitigation

Incident mitigation procedures may involve one or more of the following, depending on the need and the outcome(s) of the investigation.

\(^\text{12}\) 45 CFR § 164.308(a)(6).
\(^\text{13}\) 45 CFR § 164.530(f).
1. Close data access portals of systems that have been breached.
2. Maintain or restore data access, as appropriate, for other authorized users to continue business operations.
3. Apply appropriate sanctions to involved workforce members or other authorized researchers (See Section H).
4. Review and update security procedures and processes as needed to prevent future incidents.

**Reporting**

1. Notify CHiR management and keep them informed of the situation and response.
2. Notify other authorities, as appropriate, and as documented on the CHiR Incident Event and Investigation Log and as required in the federal Breach Notification Rule14.
   a. Report in writing to Covered Entity any security incident of which CHiR is aware.15
   b. Cooperate with other authorities who may conduct their own investigations into reported incidents. CHiR will work with non-ASU authorities under the guidance of the ASU HIPAA Officials, including ASU legal counsel.
3. Document all information gathered in the investigation on the CHiR Incident Event and Investigation Log. This log is to be maintained in the HIPAA Investigations electronic file for six years from the date of the incident to support legal proceedings, compliance reviews, and investigations by CHiR internally, ASU officials, Covered Entities and the Secretary of Health and Human Services.16

**G. Contingency Procedures**17

**Data Backups**

1. Snapshots of all data and programs stored on the server shall be regularly backed-up by UTO. Snapshots are generally available for up to four weeks prior to the current date. *(Efforts are in progress to extend the availability of snapshots to three months prior to the current date.)*

---

14 45 CFR § 164.400-414.
15 45 CFR § 164.314(a)(2)(i)(C); 45 CFR § 164.504(e)(2)(ii)(C).
16 45 CFR § 160.310.
17 45 CFR § 164.308(a)(7).
2. In the event of a non-breach loss of data on the CHiR server (i.e., equipment failure, fire, natural disaster, etc.), a server snapshot will be used to restore the CHiR server data.

**Disaster/Emergency Recovery and Operations**

1. It shall be the responsibility of each workforce member to protect and maintain confidentiality of PHI and other confidential data in the event of a technical malfunction or other disaster.

2. In the event of disaster or other emergency (i.e., equipment failure, fire, flood, natural disaster, etc.) involving the CHiR server, the CHiR Security Officer will work with UTO to ensure that no security features on the CHiR server have been compromised and no data has been lost.
   a. If security features for electronic access to the CHiR server are determined to be ineffective or compromised due to the disaster, the CHiR Security Officer will authorize the shut-down of the CHiR server and/or removal of access by all other authorized users until the security of the environment is restored.
   b. If the CHiR server is usable, secure, and accessible, the CHiR Security Officer shall verify all workforce members’ access prior to resuming normal business operations.
      i. If the server denies access due to the inability to verify authorization, affected workforce members shall notify the CHiR Security Officer who will mitigate the issue with UTO. If the problem cannot be resolved within a reasonable time frame, the CHiR Security Officer shall implement an alternative work arrangement.
   c. If any data loss is suffered, the CHiR Security Officer shall implement the Data Backup procedures to restore the lost data.

3. Workforce member workloads shall be evaluated by supervisors, and any non-essential tasks shall be tabled while operating in disaster/emergency mode.

4. UTO maintains a backup operations center, and they will automatically transfer all server operations to the backup system if the main system fails or is unusable (e.g. power failure), so that regular business operations continue with minimal interruption.

5. If workforce members are unable to work in or travel to the office (i.e., pandemic, quarantine, inclement weather, or shut-down of campus facilities), the following alternative work arrangements shall be implemented.
a. CHiR management shall authorize working remotely as appropriate. Affected workforce members shall follow the procedures in Section M: Working Remotely.

6. All workforce members shall monitor their health and report any signs of illness to CHiR management, especially during potential times of pandemics (i.e. flu season, etc.).

   a. Any affected workforce members should not present at work until symptoms have subsided for more than 24 hours.

Testing and Revision of Contingency Procedures

1. The above contingency plan shall be tested within twelve months of the original date of this policy and then annually thereafter.

2. Revisions to the contingency plan shall be documented and implemented as dictated by business needs and to maintain compliance.

H. Privacy and Security Management Process

Penalties for Violating Federal Laws

1. CHiR will implement appropriate privacy and security management processes to ensure compliance with all applicable federal regulations and with the understanding that violations of the administrative simplification rules can result in civil monetary penalties as described in 45 CFR 160 Subpart D.

Risk Analysis and Evaluation

1. CHiR will annually conduct a formal, internal assessment of compliance with the HIPAA Privacy and Security Rule, usually in the fourth quarter of the year.

   a. All privacy and security measures implemented within this policy shall be reviewed and modified as needed to continue provision of reasonable and appropriate protection of PHI.

   b. The assessment will document potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information under CHiR stewardship.

   c. Results of the assessment will be stored in the electronic folder for HIPAA Compliance Audit for six (6) years.

\[18\] 45 CFR § 164.308(a)(1).
2. Periodic technical and nontechnical evaluations may be performed as needed to respond to environmental or operational changes within CHiR or modifications to federal standards implemented under the HIPAA Privacy and Security Rule.¹⁹

**Risk Management**

1. CHiR will implement privacy and security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
   
a. Upon notice by the university audit team or internal discovery of any vulnerability, CHiR management will log the issue on the Vulnerability/Deficiency Log and establish a timetable to correct the deficiency.
   
b. Corrections of all deficiencies shall be documented. Any deficiencies that cannot be corrected shall also be documented. Documentation shall be stored in the electronic folder for HIPAA Compliance Audit.

**Sanctions**²⁰

1. Each CHiR workforce member is subject to and shall be held responsible for following all established security policies and procedures.
   
a. External Authorized Data Users shall have this responsibility and obligation specified through a Data Use Agreement.

2. Access to or disclosure of electronic health information without authorization or beyond one’s level of authorization is strictly prohibited.

3. CHiR will apply one or more appropriate sanctions against workforce members who fail to comply with the policies and procedures contained in this document including the following:²¹
   
a. Temporary or permanent suspension of data access privileges.
   
b. Separate re-training in policies and procedures for data access and handling.
   
c. Monitoring of workforce members for a period of time to be determined by the CHiR Security and Privacy Officers or until satisfactory progress is made in appropriate data access and handling.
   
d. Disciplinary action up to and including discharge or termination of employment contract.
   
e. Legal prosecution.

---

¹⁹ 45 CFR § 164.308(a)(8).

²⁰ 45 CFR § 164.530(e).

²¹ 45 CFR § 164.308(a)(1)(ii)(C).
Sanctions applied to CHiR workforce members will be documented in the *CHiR Incident Event and Investigation Log*.

**Information System Activity Review**

1. UTO routinely logs and monitors the following activities of personnel: 1) use of passwords and accounts accessed; 2) time and duration of network activity; 3) access to network software; 4) volume of data storage and transfers; and 5) server space used for e-mail.
   
   a. In cases of suspected violations of policies, especially unauthorized access to computing systems, CHiR management may authorize additional monitoring through UTO.

2. The CHiR Security Officer shall regularly review the electronic door logs in the CHiR suite to determine both appropriate and inappropriate door access as well as security incidents.
   
   f. The ASU Tempe Lock Services team will be contacted to manually download the logs from each secure door individually and transmit the combined log file to CHiR.

3. UTO logs the attempts to access Citrix and the folders on the secure network drive. The CHiR Security Officer shall regularly review the logs to determine appropriate access and security incidents.

**I. Business Associate Contracts and Other Arrangements**

1. CHiR shall maintain a business associate contract or other arrangement in written form with each Covered Entity who provides PHI or other confidential data to CHiR.
   
   a. The contract shall provide that CHiR will implement reasonable and appropriate administrative, physical and technical safeguards for protection of the data that it receives, creates, maintains or transmits on behalf of the Covered Entity.

   b. The contract shall provide that CHiR will report any security incident of which it becomes aware.

---

22 45 CFR § 164.308(a)(1)(ii)(D).

23 45 CFR § 164.308(b); 45 CFR § 164.314(a)(2); 45 CFR § 164.502(e); 45 CFR § 164.504(e).
c. The contract shall provide appropriate means for returning or destroying the data, or otherwise limiting the further use and disclosure of the data, received from the Covered Entity upon termination of the contract for any reason24.

2. If CHiR provides PHI to a subcontractor or agent to perform services, CHiR shall first enter into a contract, confidentiality agreement, or business associate agreement with such subcontractor or agent that contains similar terms, conditions, and restrictions on the use and disclosure of PHI as contained in the agreement with the Covered Entity.
   a. If any subcontractor or agent performing services for and on behalf of CHiR violates any material term of the contract or agreement, CHiR will terminate the contract or agreement and follow all appropriate mitigation and incident reporting procedures required by law, if applicable.

J. Amendments to Data25

1. Per the terms of the agreement with the Covered Entity or within a reasonable time frame of receiving a request from the Covered Entity to amend an individual’s PHI, CHiR will amend the data and provide proof of amendment to the Covered Entity.

2. CHiR shall forward any requests received from individuals to amend their data to the Covered Entity for action as the Covered Entity maintains control over the use/disclosure of their data.

K. Training26

1. All CHiR workforce members will receive training on the policies and procedures contained within this document and other training required by the university or legal authorities in order to carry out their assigned functions. Such training includes, but is not limited to, Collaborative Institutional Training Institute (CITI) Human Subjects Course for Biomedical Research Investigators, ASU HIPAA Training, and ASU Information Security Training.
   a. CHiR workforce members shall receive all training within one month of hire or affiliation and annually thereafter for ASU HIPAA Training and ASU Information Security Training.

24 45 CFR § 164.504(e)(2)(ii)(I).
26 45 CFR § 164.530(b).
Security Training. Refresher training for the CITI Human Subjects Course for Biomedical Research Investigators shall be completed every four (4) years.

i. An annual training record shall be maintained for workforce members by the CHiR Privacy and Security Officers.

ii. Notice of required training and the period for completion shall be sent to all workforce members.

iii. At the end of the training period, all training will be verified and documented in the training record.

iv. Data access shall be removed by the CHiR Security Officer for workforce members who do not complete the required training.

v. Workforce members whose job function includes access to PHI shall not access any PHI until successful completion and documentation of the above training.

b. All external researchers and/or project leaders who receive or access identifiable datasets (i.e., Limited Data Sets, custom data sets) for use in IRB-approved research studies or publications must complete the CITI Human Subjects Course for Biomedical Research Investigators or an equivalent human subjects training course before receiving or accessing the datasets.

i. The CHiR Privacy Officer or designated personnel will verify that applicable researchers and project leaders have received the required training.

ii. External researchers and/or project leaders who do not complete the required training shall not access any datasets.

L. Documentation and Recordkeeping

1. CHiR shall maintain these policies and procedures in written form for six (6) years from the date of its implementation.

2. This document shall be available to all persons responsible for implementing the procedures referenced in this document.

3. This document shall be reviewed periodically and updates incorporated as needed.

---

27 45 CFR § 164.316(b).
28 45 CFR § 164.532(j).
4. CHiR will keep records and submit compliance reports as required by the Secretary of Health and Human Services.\textsuperscript{29}
   a. CHiR will cooperate with any compliance reviews or investigations of CHiR policies, procedures or practices.

M. Working Remotely

1. Workforce members must have approval from his/her supervisor to work remotely from home or some other location.

2. Each workforce member must have a secure and appropriate environment to work remotely, including the following:
   a. Computer with a secure internet connection.
      i. An unsecured Wi-Fi connection is strictly prohibited.
      ii. Remote work in a public place is strictly prohibited.
      iii. Home networks must be within the same residence and have no file sharing capabilities enabled.
      iv. Workforce members with Level 1 and Level 2 data access are required to use only their office laptop for remote work. A current Off-Campus Use of Equipment Authorization must be on file in the workforce member’s personnel file.
   b. Telephone or mobile phone for conference calls.

3. To prepare for remote work, workforce members must ensure the following:
   a. Take home only material relevant for work. No material containing PHI can be taken out of the office. PHI can only be accessed electronically via Citrix.
   b. Forward office phone to home phone or cell phone.

\textsuperscript{29} 45 CFR § 164.504(e)(2)(ii)(H).
Section II. Physical Safeguards

A. Facility Security, Access Control and Validation

Building

1. The building management grants after-hours access only to authorized personnel requested by each department. Access shall be by use of individually assigned ASU identification cards. The cards are scanned electronically at the building entrance by Isaac system locks that have been pre-programmed for authorized users.
   a. All CHiR permanent workforce members shall be granted after-hours access upon submission of the appropriate request form.

2. The property manager provides on-site security seven days per week and the university police patrol the campus facilities around the clock.

CHiR Office Suite

1. The CHiR suite of offices is located within a larger suite of offices at the Downtown Phoenix Campus, 502 E. Monroe St, Suite C320, Phoenix, AZ 85004, which are under the ASU College of Health Solutions. The main suite shall be accessible only to authorized users who swipe their ASU identification cards at the pre-programmed Integrated System for ASU Access Control (ISAAC) lock.
   a. Only CHiR workforce members shall have door access to the section of the suite allocated to CHiR.
   b. All access attempts are logged individually into each programmable door lock.
   c. The door to the CHiR suite of offices shall remain closed at all times. Workforce members are to ensure that the door closes securely behind them during each entrance and exit. Any malfunctions of the door are to be immediately reported to the CHiR administrator.

30 45 CFR § 164.310(a).
d. The CHiR suite of offices shall be removed from the building master keys; therefore, building personnel (maintenance, custodians, etc.) cannot access the suite, except during business hours and under surveillance by CHiR workforce members.

3. Individual data staff offices shall have the same localized programmable lock as the door to the CHiR suite of offices. Three levels of access to the data staff offices must be maintained.
   a. All Access – Authorized data management staff can access all data management offices. At least one CHiR workforce member can access these areas in the event that the authorized data management staff are unavailable or in emergency situations only.
   b. Restricted Access – Temporary data staff (i.e., students, guest researchers) and non-data staff assigned to a secure office can only access their assigned office.
   c. No Access – All remaining CHiR workforce members have no access to the data staff offices.

4. Data staff shall secure their offices when leaving the suite for any extended period of time.
   a. Unoccupied or vacant data staff offices shall remain locked when not in use.

**CHiR Office Suite Visitors**

1. All non-CHiR workforce members shall be designated as visitors.
   a. College of Health Solutions workforce members shall be treated as visitors when accessing the CHiR-only side of the office suite.

2. All visitors must sign the visitor log located at the door to the CHiR suite of offices.

3. All visitors, with the exception of some maintenance and facility personnel, must be escorted at all times when in the CHiR-only side of the office suite.
**CHiR Office Suite Special Access**

1. ASU Police and the property manager may access the suite in an emergency via the secure key control system (Knox Box) maintained on the campus facility.
2. ASU Tempe Lock Services may access the suite to perform lock updates and lock maintenance as requested and to download the access logs.

**CHiR Server**

1. All data files containing PHI must be stored on CHiR’s server which is maintained by UTO in their HIPAA-compliant environment. No such files are permitted to be stored on local workstations.
2. Physical access to the CHiR servers is restricted to authorized UTO staff and is secured behind access-controlled doors (logged) with on-site surveillance.

**Contingency Operations**

1. It shall be the responsibility of each workforce member to protect and maintain confidentiality of PHI and other confidential data in the event of a disaster or emergency.
   a. Workforce members shall secure their workstations and any other office or workspace assigned to them.
2. During a disaster or emergency, at least two designated CHiR workforce members shall be authorized to access all areas of the CHiR suite.
3. In the event of a loss of data on the server, the CHiR Security Officer shall access the most recent and complete online snapshot of the data to restore the lost data.
4. In the event of a pandemic, shutdown, or evacuation of campus facilities for more than 48 hours, the CHiR Security Officer or designee will monitor the situation and notify other workforce members as needed and when it is safe to return to the campus.

**Maintenance Records**

1. All repairs and modifications to the CHiR suite that are related to security (i.e., doors, locks and walls) shall be documented electronically in the appropriate file by the center administrator. Other maintenance may also documented in a similar manner.

---

31 45 CFR § 164.310(a)(2)(i).
B. Workstation Use & Security\textsuperscript{32}

\textbf{In-Office Workstations}

1. Individual computer workstations shall be password protected when not in use, and workforce members shall lock their workstations when leaving their office or workstation. All workstations shall utilize the automatic password lock provided by the operating system to lock workstations after 10-15 minutes of inactivity.

2. Network and server passwords of each workforce member shall be distinct and revised on a regular basis.

3. No files containing PHI shall be stored on local workstations or laptops, PDAs, flash drives or other portable devices or accessed on unapproved networks.

4. Server access windows shall be properly closed (logged off), workstations shut down, all confidential project paperwork or files secured and offices locked at the close of each workday.

5. At no time shall paper reports or printouts containing PHI or other confidential information be left unsecured, unattended, or allowed to leave the CHiR Office Suite. Any paper reports or printouts that are no longer needed must be shredded and securely disposed of as soon as possible.

6. Unauthorized software shall not be installed on any workstation in the CHiR office suite. All software requests must be approved by the CHiR Security Officer.

7. Any suspected or actual unauthorized use of your workstation should be promptly reported to the CHiR Security Officer.

8. Workforce members with Level 1 and Level 2 data access shall adhere to the following additional requirements:

   a. Workstations shall be positioned such that unauthorized individuals cannot view or access PHI on computer monitors of authorized personnel.

   b. PHI shall not be printed to any printer outside of the CHiR office suite. CHiR workforce members with access to PHI may print PHI to a networked printer within the CHiR only section of the office suite, but they must promptly retrieve such documents from the printer.

\textsuperscript{32} 45 CFR § 164.310(b); 45 CFR § 164.310(c).
External/Remote Workstations

1. Workforce members must have approval from his/her supervisor to work remotely from home or some other location.

2. Each workforce member must have a secure and appropriate environment to work remotely, including the following:
   a. Telephone or mobile phone for conference calls.
   b. Computer with a secure internet connection.
   c. Home networks must be within the same residence and have no file sharing capabilities enabled.

3. Workforce members with Level 1 and Level 2 data access must adhere to the above requirements for workstations accessing PHI and the following additional requirements:
   a. Use only the office laptop for remote work. A current Off-Campus Use of Equipment Authorization must be on file in the workforce member’s personnel file.
   b. An unsecured Wi-Fi connection is strictly prohibited.
   c. Remote work in a public place (i.e., airports, hotels, parks, library, café, etc.) is strictly prohibited.
   d. Workstation must be used in a location and positioned such that unauthorized individuals cannot view or access PHI during the remote session.

1. To prepare for remote work, workforce members must ensure the following:
   a. Take home only material relevant for work. No material containing PHI can be taken out of the office. PHI can only be accessed electronically via Citrix.
   b. Forward office phone to home phone or cell phone.
C. Device and media controls

Disposal
1. If any Business Associate Agreement or other agreement is terminated, CHiR will, within the designated time stipulated in the aforementioned agreement, return to Covered Entity, destroy, or render unusable all PHI that CHiR maintains in any form or format.
2. All disposals of hardware or electronic media, including those containing PHI or which have accessed PHI, are processed through the College IT Staff and ASU Property Control department with no exceptions.
   a. All hard drives shall be removed from all equipment and destroyed and/or rendered unusable using an ASU UTO approved method.
   b. All storage media (CDs, DVDs, disks, etc.) shall be destroyed using an ASU UTO approved method.
3. All PHI or other confidential information in paper form shall be shredded in a cross-cut shredder.

Media Re-use
1. All electronic media to be made available for reuse must first have the hard drives wiped and reformatted by College IT Staff if media will be reused within the department or the Property Control Department if media will be reused outside of the department.
   a. The CHiR administrator will submit a request for wiping/reformatting to the College IT Staff or Property Control.
   b. The electronic media are wiped using the DBAN 3 boot disk. The media will remain out of service until the wiping/reformatting is complete. Usable media will be reused or sold.

Accountability
1. All workstation and office equipment shall be inventoried at least annually by CHiR administration or upon reassignment or movement to alternate locations. Inventory results shall be maintained in a dated, electronic file on the CHiR administration drive.

---

33 45 CFR § 164.310(d)
2. Any lost or stolen devices or media should be promptly reported to the CHiR Security Officer.

Data backup and storage
1. In the event of physical relocation of the CHiR servers or movement of data from one server to another, the CHiR Security Officer will work with UTO to ensure that all data on the server is securely maintained or securely transferred.
Section III. Technical Safeguards

A. Access Control

Unique User Identification
1. One unique user identification (ASURITE ID) will identify each person accessing the university computing network and/or CHiR server.
2. Remote access to the server is restricted to a password authenticated Citrix web application.

Emergency Procedures
1. See Section I.G: Contingency Procedures.

Automatic Lockout or Logoff
2. All workstations shall utilize the automatic password lock provided by the operating system to lock workstations after 10-15 minutes of inactivity.
3. Sessions on the server shall continue until shut down by the user, but Citrix will log users out of its environment automatically after 10 minutes of inactivity.

Encryption and Decryption
1. See Section I.A – Data Management and Disclosure Accounting

B. Audit Controls

1. See Section I.H: Privacy and Security Management Process

C. Integrity

1. See Section I.A – Data Management and Disclosure Accounting
2. The internal Windows system data stamps are used to determine if modifications have occurred unknowingly to any files.

34 45 CFR § 164.312(a).
35 45 CFR § 164.312(b).
36 45 CFR § 164.312(c).
D. Person or Entity Authentication

1. If an individual or entity requests access to PHI or any confidential data held by CHiR as permitted by 45 CFR § 164.524, CHiR will, within the allotted time frame specified in the agreement with the Covered Entity, forward such request in writing to the Covered Entity.

   a. CHiR is not responsible for verifying the identity of the individual making the request. The Covered Entity will be responsible for making all determinations regarding the granting or denial of such request for access to PHI, and CHiR will not release any PHI held by ASU directly to an individual or entity.

E. Transmission Security

1. See Section I.A – Data Management and Disclosure Accounting

---

37 45 CFR § 164.312(d).
38 45 CFR § 164.312(e).