

---

---

**Texas Association of Counties**

---

**HIPAA SECURITY POLICY**

**April 19, 2005**

---

---

Approved: \_\_\_\_\_  
Sam D. Seale, TAC Executive Director

April 20, 2005

**TABLE OF CONTENTS**

- PART 1. Introduction..... 5
  - 1.1 Purpose..... 5
  - 1.2 Scope..... 5
- PART 2. General Policies..... 5
  - 2.1 Acceptable Use Policy..... 5
    - a. Unacceptable Uses..... 5
    - b. Department Use Policies..... 6
  - 2.2 Ownership of Data and Systems..... 6
    - a. Data and Systems Owned by TAC..... 6
    - b. No Expectation of Privacy..... 7
  - 2.3 Compliance and Sanctions for Violations..... 7
  - 2.4 User Responsibilities..... 7
  - 2.5 Incident Reporting and Response..... 8
    - a. Types of Security Incidents..... 8
    - b. Severity Levels..... 8
    - c. Security Incident Reporting and Response..... 9
    - d. Reporting and Incident..... 9
    - e. Security Incident Investigation..... 9
  - 2.6 Relationship to Other TAC Policies..... 9
    - a. Personnel Policy..... 9
    - b. Department Policies..... 10
    - c. Physical Security Policy..... 10
  - 2.7 Policy Review and Revision..... 10
- PART 3. Information Security..... 10
  - 3.1 Security Organization and Responsibilities..... 10
    - a. The Chief Information Officer (CIO)..... 10
    - b. The Information Resources Department Security Officer (“ISO”)..... 10
    - c. The HIPAA Security Officer (HSO)..... 11
    - d. The Director, Program Administration:..... 11
    - e. The Manager, Health and Employee Benefits Department:..... 11
    - f. EBP Employees:..... 11
    - g. The HIPAA Security Committee..... 12
  - 3.2 Administrative and Management Controls..... 12
    - a. Risk Assessment and Management..... 12
      - 1. Risk Analysis..... 12
      - 2. Risk Management..... 12
    - b. Asset Classification and Control..... 12
      - 1. Inventory of Assets..... 12
        - a) Hardware..... 12
        - b) Applications and Software..... 12
        - c) Data..... 13
      - 2. Classification of Information..... 13
      - 3. Information Labeling and Handling..... 13
      - 4. Information Access Management..... 13
    - c. Personnel Security..... 13

1.	Including Security in Job Responsibilities.....	13
2.	Personnel Screening and Policy.....	13
3.	Confidentiality Agreements.....	13
d.	Access Control.....	13
1.	Authorization and Clearance Procedures.....	14
2.	System Access Procedures.....	14
3.	Third Parties.....	14
4.	Business Associates.....	14
5.	Access Authorization Review.....	15
6.	Termination Procedures.....	15
e.	Password/Passphrase Policy.....	15
1.	Password/Passphrase Required.....	15
2.	Password Selection Standards.....	16
3.	Password Change Policy.....	16
4.	Third Parties.....	16
f.	Security Education and Training.....	16
1.	Initial Information Security Training.....	16
2.	Training Administration and Procedures.....	17
3.3	Physical and Environmental Protection.....	17
a.	Facility Security Plan.....	18
1.	Securing Offices, Rooms and Facilities.....	18
2.	Changes to Physical Security.....	18
b.	Equipment Security.....	18
1.	Equipment Use.....	18
2.	Workstation Security.....	18
3.	Teleworking.....	19
c.	Physical Accountability.....	19
1.	Workstation and Server Controls.....	19
2.	Device and Media Controls.....	19
a)	Mobile Computing Devices.....	19
b)	Media.....	19
1)	Disposal.....	19
2)	Media Re-Use.....	20
3)	Encryption and Decryption Required.....	20
d.	Removal of Property.....	20
3.4	Technical Controls.....	20
a.	Network Controls.....	20
b.	Access Control.....	21
c.	Auditing and Monitoring.....	21
1.	Audit Controls.....	21
2.	Information System Activity Review.....	21
3.	The following assets, as a minimum, shall be monitored:.....	21
d.	Data Integrity.....	22
e.	Transmission Security.....	22
1.	Encryption and Decryption.....	22
2.	Insecure Networks.....	22

3.	Approved Methods for Transmitting EPHI .....	22
4.	Approved EPHI Ciphers .....	22
f.	Prevention and Detection of Malicious Software .....	22
g.	Systems Development and Maintenance. ....	23
PART 4.	Compliance with Legal Requirements.....	23
PART 5.	Disaster Recovery and Business Continuity .....	23
a.	Applications and Data Criticality Analysis.....	24
b.	Contingency Plans. ....	24
1.	Data Backup Plan.....	24
2.	Disaster Recovery Plan.....	24
3.	Emergency Mode Operation Plan.....	24
c.	Testing and Revision Procedures.....	24
PART 6.	Appendix.....	<b>Error! Bookmark not defined.</b>

---

## **PART 1. Introduction.**

---

### **1.1 Purpose.**

This Policy provides direction and establishes the information technology-related security requirements for the Texas Association of Counties Health and Employee Benefits Pool (“HEBP”) and those Texas Association of Counties’ operations on behalf of HEBP that use Electronic Protected Health Information (“EPHI”), as required by 45 Code of Federal Regulations, §§ 164.302 – 164.318 (“HIPAA Security Rule”).

### **1.2 Scope.**

This policy applies to all TAC employees, as well as contractors, business associates, consultants, temporaries, and others who perform services on behalf of HEBP and use, manage, or come in contact with EPHI as a part of such service.

---

## **PART 2. General Policies.**

---

### **2.1 Acceptable Use Policy.**

TAC information resources (including but not limited to, the TAC network, Internet, workstations, devices, e-mail, applications, and data) may only be used for appropriate business purposes. Occasional, incidental personal use is permissible so long as:

- It does not consume more than a trivial amount of resources;
- It does not interfere with staff productivity;
- It does not preempt any business activity;
- It is not a use that has been identified below as an unacceptable use.

#### **a. Unacceptable Uses.**

Inappropriate use exposes TAC systems to risks including virus attacks, compromise of network systems and services, and legal liability. The following activities are prohibited:

- Harassment. In particular, using a TAC computing asset to actively engage in procuring or transmitting material that is in violation of TAC’s sexual harassment and hostile workplace policies;
- Destruction of or damage to equipment, software, or data belonging to TAC or others;
- Effecting security breaches or disruptions of network communication;
  - “Disruption” includes, but is not limited to:
    - network sniffing;
    - pinged floods;
    - packet spoofing;
    - denial of service;
    - forged routing information for malicious purposes;
  - “Security breaches” include, but are not limited to:
    - accessing data of which the employee is not an intended recipient;
    - logging into a server or account that the employee is not expressly authorized to access;
- Unauthorized copying, downloading, or using copyrighted materials;
- Engaging in any activity that might be harmful to systems or to any information/data stored thereon, such as:
  - Creating or propagating viruses, trojans, e-mail bombs, etc.;
  - Disrupting services or damaging files; or
  - Making unauthorized or non-approved changes.
- Under no circumstances is an employee of TAC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TAC-owned resources.

**b. Department Use Policies.**

Nothing contained herein prohibits individual departments from imposing stricter use policies.

**2.2 Ownership of Data and Systems.**

**a. Data and Systems Owned by TAC**

All applications, data, and other system resources are owned or operated by the Texas Association of Counties. No employee has any legal or equitable interest in any such system, application, or data. Any data, system, or application created, stored, or maintained on the TAC system is and remains the property of TAC. Any application, process, program, design, data or other information resource asset created by an employee using TAC resources is the property of TAC and all employees hereby grant, transfer, and assign any and all intellectual property rights to TAC. The use of privately-owned equipment or data is strictly prohibited without prior written approval of the HIPAA and Information Resources Department (“IRD”) Security Officers.

## **b. No Expectation of Privacy**

Although the Acceptable Use Policy authorizes limited personal use of TAC information technology resources, users shall have no expectation of privacy with regard to that use or with regard to any personal information or data stored thereon. In addition, neither TAC nor any TAC-related entity, including HEBP, shall be liable for loss or damage to any personally owned or created data or equipment contained on or connected to the TAC system.

For security and network maintenance purposes, authorized individuals within TAC may monitor equipment, systems and network traffic at any time. TAC reserves the right to audit networks and systems to ensure compliance with this policy.

## **2.3 Compliance and Sanctions for Violations.**

All workforce members are required to comply with these policies. Violation of the provisions of this policy could result in disciplinary action, up to and including termination and possible criminal prosecution. Non-workforce members with access to TAC systems shall be subject to sanctions according to their written contract and/or state or federal civil and criminal sanctions. TAC reserves the right to revoke a user's privileges at any time and users may be denied access (with or without notice) for violations of this policy.

## **2.4 User Responsibilities.**

- Access only the accounts, files, and data that are publicly available, or to which you have been given authorized access.
- Use business-related information for tasks related to job responsibilities and not for personal purposes.
- All workstations and laptops shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, by logging off, or by locking the screen when the host will be unattended.
- Specific information about information system vulnerabilities must not be distributed to persons without prior approval of the HIPAA and IRD Security Officers.
- Employees have a duty to report all information security violations or suspected information security violations and/or problems to the IRD staff on a timely basis so that prompt remedial action may be taken.
- Users may not download unauthorized software, including applications, screensavers, toolbars, etc., without permission from the Chief Information Officer ("CIO").
- Passwords must not be written down and left in a place where unauthorized persons might discover them.

- Users must not store fixed passwords in dial-up communications programs, Internet browsers, or related data communications software unless authorized by the IRD.

## **2.5 Incident Reporting and Response.**

A security incident is a computer or network-based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources. A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

### **a. Types of Security Incidents.**

Security incidents include, but are not limited to:

- Security Policy violations;
- Software Malfunctions;
- Worms, Trojans, and Viruses;
- Intrusion attempts;
- Physical security breaches or attempts;
- Compromised passwords; and
- Compromised data.

### **b. Severity Levels**

Incidents occurring within the TAC systems are given different levels of severity depending on the extent of the incident.

- Low – Only a small number of systems are affected with a virus that has been known and that the current anti-virus protection is handling. A small number of machines are being scanned from an outside source, but no attack or penetration has taken place.
- Medium – A significant number of systems are being scanned or penetration or denial of service attacks attempted with no effect on operations; there are many occurrences of a known virus, but they are being handled by anti-virus software. There are a few isolated instances of a new computer virus not being handled by anti-virus software. Suspected access of sensitive data has occurred or is likely to occur.
- High – Penetration has occurred or denials of service attacks have been detected with significant impact on operations. Known unauthorized access to sensitive data has occurred or is likely to occur.

**c. Security Incident Reporting and Response.**

All security incidents shall be immediately reported to IRD staff who will take appropriate remedial action. This action may include temporary denial of service to or from hosts, subnets, or domains, internal or external. Reports of security incidents shall be made in writing on a form provided by the IRD Security Officer. This required written report may be prepared post-incident if the nature of the incident required immediate remedial action.

**d. Reporting an Incident**

TAC will maintain a phone number where incidents can be reported along with an e-mail address that employees can use to submit questions. TAC will maintain a website that will inform users of potential security concerns. The website will also contain a list of IRD contacts for users to contact if they have specific questions or concerns.

**e. Security Incident Investigation.**

The IRD Security Officer and the HIPAA Security Officer will investigate all security incidents, assess the damage and give a written report of their findings to the CIO. Depending on the nature and severity of the incident, the CIO may forward a copy of the report to the Director of Program Administration, TAC Legal, the Manager of the Employee Benefits Department and/or the TAC Executive Director. For medium and high severity incidents, the report should contain the basic facts surrounding the incident, the cause of the incident, the remedial action taken, the damage (or possible damage), and recommendations as to actions to be taken to prevent future occurrences. The record of the investigation shall be maintained for a period of six years from the date of the final report. All reports of security incidents are confidential to the extent allowed by law and may only be disclosed on the authority of the CIO, with the advice and consent of TAC Legal.

If the investigation indicates that there was a possibility of compromise of EPHI, the HIPAA Security Officer will prepare a separate incident report which focuses on the potential compromise of the EPHI and forward that report to the Director of Program Administration, the Manager of the Employee Benefits Department and to TAC Legal. That report shall be maintained by the HIPAA Security Officer for a period of six years from the date of the report. All reports of security incidents involving the possible compromise of EPHI are confidential to the extent allowed by law and may only be disclosed on the authority of the Director of Program Administration, with the advice and consent of TAC Legal.

**2.6 Relationship to Other TAC Policies.**

**a. Personnel Policy**

The TAC Personnel Policy governs all general personnel matters.

## **b. Department Policies**

In matters relating to information security, this policy governs. Department policies, however, may be more restrictive provided that they do not have the effect of diminishing the effectiveness of this policy – as determined by the CIO.

## **c. Physical Security Policy**

This policy only applies to those areas where information technology resources and EPHI are physically located and, as to the physical security in those locations, this policy will govern over the TAC Physical Security Policy. The CIO and the HIPAA Security Officer will work with the TAC physical security team to ensure that there is a seamless integration between these policies and the TAC Physical Security Policy and that all parties are clearly aware of the physical security requirements of each.

## **2.7 Policy Review and Revision.**

The CIO and the HIPAA Security Officer shall review this policy at least once every year to determine its effectiveness and to make any necessary adjustments due to changes in technology, the legal environment, or to the current threat environment. The CIO and/or the HIPAA Security Officer may make more frequent reviews or changes to this policy in response to any internal or external environmental change that presents a significant risk to the information or information infrastructure of the organization. Any such changes must be approved by the TAC Executive Director before they become effective. Any such changes must also be submitted to the TAC Board and the HEBP Board for ratification.

---

# **PART 3. Information Security.**

---

## **3.1 Security Organization and Responsibilities.**

### **a. The Chief Information Officer (“CIO”)**

The Chief Information Officer, assisted by the IRD Security Officer (“ISO”), has overall authority and responsibility for Information Technology security, systems, equipment, and applications.

### **b. The Information Resources Department Security Officer (“ISO”)**

The IRD Security Officer reports to the CIO and is the primary security contact, coordinator, and incident responder in matters relating to Information Technology security. The ISO, working in partnership with the HIPAA Privacy Officer (HPO)

and the HIPAA Security Officer (HSO), as a team, executes this Policy. Delegation of duties in response to remediation will be coordinated by the ISO and accountability for corrective actions will be enforced directly by the CIO, in coordination with the Executive Director and the department managers.

**c. The HIPAA Security Officer (HSO)**

The HIPAA Security Officer is appointed by the TAC Executive Director and has operational responsibility for the enforcement and management of this policy as set forth herein. The HSO's duties include, but are not limited to:

- Ensuring that appropriate security measures and standards are implemented and enforced with regard to EPHI. The security measures implemented should be based on the criticality, sensitivity, and public or private nature of the data, and may include methodologies, change management, and operational recovery plans;
- Review rights of authorized users of EPHI on a regular basis;
- Review access and system logs for systems that contain EPHI;
- Work with the ISO and the CIO on all security matters;
- Investigate and report on security problems and issues and refer such matters to the appropriate officials;
- Develop conditions of use or authorized use procedures for EPHI; and.
- Provide training to regularly remind workers about their obligations with respect to information and EPHI security.

**d. The Director, Program Administration**

The Director of Program Administration has operational authority relating to the collection, access, dissemination, and security of EPHI.

**e. The Manager, Health and Employee Benefits Department**

The Manager of the Employee Benefits Department is the custodian of all electronic information created, collected, and maintained by or on behalf of HEBP. The Manager has the authority and responsibility for operational decision-making in all matters relating to EPHI collection, access, dissemination, and security in keeping with the Director of Program Administration's policies and instructions relating to access control, data sensitivity, and data criticality.

**f. EBP Employees**

All EBP employees have the responsibility for information security on a day-to-day basis. They are required to read, understand, and follow these policies. They further have the duty and responsibility to report any and all security incidents in the manner set forth in this Policy.

**g. The HIPAA Security Committee**

The HIPAA Security Committee develops and maintains the HIPAA Security Policy. The HIPAA Security Committee consists of the following individuals:

1. The Chief Information Officer;
2. The IRD Security Officer;
3. The HIPAA Security Officer;
4. Legal Department Representative(s); and
5. The Director of Program Administration, or a designee.

**3.2 Administrative and Management Controls**

**a. Risk Assessment and Management**

1. Risk Analysis

Periodic risk assessments will be performed at appropriate intervals to ensure that security controls are adequate to address the current threat level.

The initial risk assessment was completed in September, 2004.

2. Risk Management

The CIO, working with the HIPAA Security Officer and TAC Legal, will implement security measures and safeguards for each EPHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The diverse nature of the operations within TAC and HEBP necessitates a high level of autonomy in planning, designing and implementing HIPAA security measures and safeguards. Subject to Section 2.7 above (“Policy Revision”), security policy and controls shall be updated as appropriate within a reasonable time after a security issue has been identified, after a periodic risk assessment, and after a Policy review.

**b. Asset Classification and Control**

1. Inventory of Assets

a) Hardware

All equipment and devices that use, process, or store EPHI shall be inventoried, labeled, and accounted for by the HIPAA Security Officer.

b) Applications and Software

All applications and software that use, process, or store EPHI shall be documented, inventoried, and accounted for by the HIPAA Security Officer. Such accounting shall include version numbers, patch/upgrade history, license agreements, and other similar information.

c) Data

All data elements and their metadata that are contained on an application or system that uses, processes, or stores EPHI shall be catalogued and stored in a data dictionary maintained by the HIPAA Security Officer.

2. Classification of Information

All data and other EPHI shall be reviewed to determine the level of sensitivity and criticality and shall be classified according to its risk of loss, compromise, or damage.

3. Information Labeling and Handling

Classified data shall be properly labeled and controls implemented to protect the data against unauthorized access. The date of declassification or destruction shall be included as part of the classification information.

4. Information Access Management

Information access shall be managed by the EBP Manager with the assistance of the HIPAA Security Officer and the HIPAA Privacy Officer. Access to EPHI shall be authorized as provided for below.

**c. Personnel Security**

1. Including Security in Job Responsibilities

All job descriptions for positions which handle EPHI or other TAC classified information must include security and proper handling of classified information in the description of the job responsibilities of the position.

2. Personnel Screening and Policy

All employees with access to EPHI shall be appropriately screened prior to granting them access to EPHI.

3. Confidentiality Agreements

Certain employees may be required to sign confidentiality agreements depending on their level of access to EPHI.

**d. Access Control**

All access to EPHI granted to workforce members will be authorized, controlled, and supervised. Access to sensitive or classified information resources is based upon a “need to know” or a “need to use.” Any employee that will have access to EPHI or to systems that contain EPHI shall only be granted the level of access required to perform the functions of the position.

1. Authorization and Clearance Procedures  
The HSO controls access to EPHI and may condition such access on the satisfactory results of a background check, and after HIPAA training and initial computer security training.
2. System Access Procedures  
The HSO shall authorize access to EPHI for the workforce member on a form provided by the IRD. The IRD shall periodically provide to the HSO a list of workforce members with access to EPHI.
3. Third Parties  
Access by third parties other than business associates to TAC systems and/or to EPHI shall be strictly limited and controlled. The granting of access shall be on a case-by-case basis with the concurrence of the CIO, TAC Legal, and the HSO.
4. Business Associates  
The HSO may authorize a business associate to have access to EPHI if the business associate executes a Business Associate Agreement that complies with HIPAA requirements.

All Business Associate Agreements must contain the following provisions:

- a) The business associate will implement appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that the business associate creates, receives, maintains, or transmits on behalf of HEBP, including EPHI that is exchanged or transmitted between the business associate and HEBP.
  - b) The business associate will report to HEBP as soon as possible any unauthorized use or disclosure of EPHI, including any security incident not provided for by its contract, of which it becomes aware.
  - c) The business associate will require any agent or a subcontractor, to whom the business associate provides EPHI, to agree in writing to the same restrictions and conditions that apply to the business associate with respect to such EPHI.
  - d) The business associate shall certify in the original contract that they are in compliance with the minimum HIPAA security standards and must, each year of the contract term, certify, in writing that they continue to be in compliance.
  - e) Any other provision required by TAC or HEBP's Privacy or Security Policies.
- If a business associate materially violates the Business Associate Agreement or the HIPAA rules, TAC will notify the Business

Associate, and address the violation in accordance with the HIPAA rules.

- A Business Associate Agreement is not required when HEBP discloses EPHI to a provider of health care services, for purposes of providing medical treatment to the individual to whom the EPHI pertains.

5. Access Authorization Review

Access rights to EPHI systems shall be reviewed by the HSO and the IRD both annually and every time a workforce member's employment status changes (both internal and external) to determine whether access rights to EPHI need to be granted, modified, or revoked.

6. Termination Procedures

A supervisor of a workforce member whose access to EPHI is no longer appropriate shall immediately notify the HIPAA Security Officer, who shall initiate the termination sequence. Revocation of access to EPHI shall be initiated by the HSO when access is no longer appropriate. The IRD shall terminate access on the date designated by the HSO. If the revocation is due to the termination of employment, the IRD shall terminate network access immediately.

When access is revoked due to termination of employment, the employee's supervisor shall also notify the IRD which shall, unless otherwise requested, immediately terminate TAC network access also.

When any workforce member's employment is terminated, the supervisor must notify the IRD immediately.

Access to systems may be denied by IRD (with or without notice) for violations of this policy or possible security threats to the system. If IRD revokes a user's access, it will immediately notify the HIPAA Security Officer.

**e. Password/Passphrase Policy.**

1. Password/Passphrase Required.

Computer and communication system access control must be achieved through passwords or passphrases that are unique to each individual user. All vendor-supplied default passwords must be changed before any computer or communications system is used. Users will be given an initial password and must change that password on first login.

- Do not share the password assigned to you.
- Select an obscure password and change it frequently.
- Understand that you are responsible for all activities on your username/account ID.
- Ensure that others cannot learn your password.

- If you have reason to believe that your username/account ID or password has been compromised, contact IRD immediately.
  - Users must employ different passwords on each of the systems to which they have been granted access.
2. Password Selection Standards.  
Users are required to select their own passwords in accordance with these password selection standards. All passwords/passphrases shall be "strong" and shall meet the following requirements:
- contain at least 8 characters; and
  - contain at least one letter in uppercase, one letter in lowercase, and one symbol.
3. Password Change Policy.
- All users will be automatically required to change their passwords at least once every six months.
  - Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.
4. Third Parties.  
Every user ID established for a non-employee must have a specified expiration date.

#### **f. Security Education and Training**

Individual workforce members are a critical factor in protecting and securing EPHI, confidential data, and systems. All members of the workforce shall receive position-appropriate training in both the TAC Security Policies and the HIPAA Security Policy and procedures which are designed to ensure the confidentiality, integrity and availability of electronic protected health information (EPHI) (“the HIPAA Security Policies”). Training may be given through e-mailed security updates, internet-based materials or any other appropriate means. Training shall be documented.

1. Initial Information Security Training  
All members of the workforce with access to EPHI shall receive training on the HIPAA Security Policy. New members of the workforce with access to EPHI will receive training prior to being granted access to EPHI.

All workforce members will be trained specifically on maintaining the security of EPHI. Workforce members who have access to EPHI in the course of performing their jobs will receive broader and more detailed training appropriate to their position.

### Periodic Security Refresher Training

All employees shall receive appropriate supplemental security training. Employees will also receive periodic security reminders and updates.

### 2. Training Administration and Procedures

- The Security Committee will determine what level of training is appropriate for each job position, considering whether and to what extent the position has access to EPHI and other factors relevant to TAC security.
- The HIPAA Security Committee will prepare position-appropriate training for all workforce members and coordinate with the Human Resources Department to schedule the training.
- The training program will include procedures to document the training given each workforce member in that member's personnel record and in the records of the HIPAA Security Committee. The Committee's training records will be kept for at least 6 years.
- The Security Official will notify the Director of Human Resources whenever a material change in policies and procedures occurs, and additional training will be developed and scheduled.
- All policies and procedures will be made available for members of the workforce to review or reference when needed.
- The Security Official will retain all training materials for six years after the date they are superseded by revised materials.

## **3.3 Physical and Environmental Protection**

TAC protects all facilities, workstations, and rooms where EPHI is being conducted from unauthorized access or usage through a variety of methods, including: lockable doors accessible only to appropriate key holders; monitored access entry points to rooms where EPHI is being conducted; ID and hard password authorization for network logins; and password protected screen savers for unattended workstations.

The operations of HEBP are conducted in the TAC Building. Access to the TAC Building, including its garage, will be controlled to prevent inappropriate access.

## **a. Facility Security Plan**

Unauthorized access to TAC facility is safeguarded and controlled through number pad locks, badge swipe locking mechanisms, locks requiring keys, and security awareness through employee training.

### **1. Securing Offices, Rooms and Facilities**

- Workstations and work areas that are used to access protected health information are located in controlled areas that have physical protections including locks, key cards, or similar devices.
- All physical files pertaining to HEBP operations will be stored in a locked room. Only designated staff will access to this room.
- Fax machines and printers dedicated for use by EBP employees will be located in a secured room accessible only by designated personnel. Printed materials or faxes containing PHI must be physically secured at all times. If copying is required, materials containing PHI must not be left unattended on the copier.
- Security codes, locks and/or key cards will be changed or re-programmed as necessary when an employee terminates.
- The HIPAA Room, Scanner Room, and File Room will each be secured with a code lock and an automatic door-closer. These doors may not be propped open. Codes will be changed periodically and may not be given out to any one, including unauthorized TAC employees. Codes will be changed whenever an EBP employee terminates employment in the department.
- EBP members may leave their office doors open when they are occupying their offices. However their offices must be locked at all times when they are not occupied.

### **2. Changes to Physical Security.**

All repairs/modifications performed on the physical components of TAC's security must be submitted to the CIO and the HIPAA Security Officer for review and concurrence. All repairs and maintenance performed within secure areas or which affect or implicate physical security of the TAC building must be documented and maintained.

## **b. Equipment Security**

### **1. Equipment Use.**

In addition to the TAC Acceptable Use Policy (Section 2.1), EPHI shall not be accessed from unauthorized workstations.

### **2. Workstation Security.**

- The workstations of every individual with access to PHI, including EPHI, will be organized and kept in a manner that prevents inappropriate access to PHI.
- When working on a file that contains PHI, the designated personnel will keep those files secured at all times. If these

personnel must leave their office, either at the end of the day or otherwise, the file must be locked in the desk, the office door locked, or the file returned to the secure file room. No files, papers, disks, CD or any other materials containing EPHI will be left unsecured at any time.

- Computers will not display EPHI in a manner or at a time when it would allow for the inadvertent disclosure of EPHI, and an employee's computer will never display EPHI when the employee is not at the computer.
- Computer monitors must either be placed so that they cannot be seen from the doorway, or a protective device must be installed, to prevent unauthorized viewing of EPHI.

3. Teleworking

1. Accessing EPHI on the network from remote computers is not allowed unless authorized by the HSO.

**c. Physical Accountability.**

1. Workstation and Server Controls

TAC IRD authorizes and is responsible for the purchase, assignment, and removal of all devices (new or currently in use) that have or will have EPHI installed. Reassignment and removal of these devices will be documented. Before movement of equipment that is also a sole source of EPHI, TAC IRD is responsible for creating and testing for recoverability a backup copy of all EPHI on the equipment to be moved prior to its relocation. The backup media/hardware containing the EPHI must be kept at a location separate from the origin and destination of the equipment from which it was sourced.

2. Device and Media Controls.

The HIPAA Security Officer authorizes and is responsible for the proper management of media or hardware containing EPHI.

a) Mobile Computing Devices

Only authorized computing devices may be connected to any application or supporting system that contains EPHI. No EPHI may be stored unencrypted on the hard drive of a mobile computing device.

b) Media

1) Disposal.

When the useful life of equipment and/or media has been reached, the media is to be rendered unreadable by forensic wiping, physical destruction, or degaussing the media. All

storage media that contains or has contained EPHI shall be disposed of as follows:

- Hard drives – remove, degauss, and smash or melt;
- Floppy disks – degauss, shred and burn;
- CD/DVD disks – smash and melt; and
- Flash memory devices – degauss, smash and melt.

The HIPAA Security Officer shall keep a destruction log containing the description of the media, the date of destruction, the method of destruction and the name of the person performing the destruction.

2) Media Re-Use

The HIPAA Security Officer authorizes and is responsible for approving media for reuse in an EPHI and non EPHI environment and for the removal of EPHI from media that will be reused in a non EPHI environment. Storage media that contain or have contained EPHI shall be clearly labeled and may not be reused for purposes other than for using, storing, or processing EPHI. Unless said media is saved for purposes of archiving or records retention, it shall be promptly destroyed and its destruction logged.

3) Encryption and Decryption Required

EPHI that is moved or transmitted from the system must be encrypted. This requirement does not apply to EPHI that is transferred electronically over a secure network.

**d. Removal of Property**

No information technology equipment or EPHI may be removed from their location without specific authorization from the HIPAA Security Officer. Any such removal and its return shall be logged by the HIPAA Security Officer. The HIPAA Security Officer shall report any equipment and or EPHI that is not returned or its destruction authenticated and logged. The report shall be maintained for a period of at least six years from the date of the report.

**3.4 Technical Controls**

**a. Network Controls**

No unauthorized wireless devices, including but not limited to devices using the Bluetooth, 802.11x, etc. standards, may be attached to the TAC networks.

## **b. Access Control**

1. Unique User Identification - Each person with access to any TAC system shall have a unique user ID.
2. Automatic Session Logoff - Where possible, application sessions will timeout after a period of inactivity of 10 minutes. In the case that an application does not support session timeouts, workstation inactivity timeouts will be relied upon.

## **c. Auditing and Monitoring**

1. Audit Controls  
TAC IRD and the HIPAA Security Officer shall implement controls for auditing TAC information systems, policies, and procedures.
2. Information System Activity Review  
The network policy for TAC is to ensure the confidentiality, availability and integrity of EPHI. This goal will be achieved by ensuring that only authenticated users are able to access the network. The authentication systems will detect and respond to attempts by attackers that are attempting to circumvent authentication.

All sensitive and critical information processing systems shall be audited on a periodic basis. Auditing priorities shall be scheduled on the basis of incident history, application criticality and the sensitivity of the information. A minimum baseline of log and audit records that monitor specific system events shall be generated and periodically reviewed for all systems containing EPHI.

3. The following assets, as a minimum, shall be monitored:
  - Workstation, server, and network events and processes;
  - User access to workstations, servers, and network;
  - Interfaces to external systems with which TAC exchanges EPHI; and
  - Audit logs produced by system and network management and monitoring devices and tools
  - Relevant portions or summaries of system activity logs shall be treated as HIPAA-related documentation and follow HIPAA Security document retention rules.

The HIPAA Security Officer, working, with the IRD, will regularly review records of information system activity, including audit logs, access reports, and security incident reports. The IRD will notify the HIPAA Security Officer of any security incidents that might adversely impact EPHI system or data security.

#### **d. Data Integrity**

TAC shall maintain appropriate mechanisms to protect EPHI from improper alteration or destruction and shall maintain electronic mechanisms to corroborate that EPHI has not been improperly altered or destroyed. Such mechanisms shall, at a minimum, consist of access controls and password protection.

#### **e. Transmission Security.**

The purpose of this policy is to protect the confidentiality and integrity of EPHI that is transmitted via communications networks.

##### 1. Encryption and Decryption

EPHI transmitted via an insecure network such as the Internet must be transmitted via an approved method, and encrypted via an approved cipher.

##### 2. Insecure Networks

An insecure network is a network that lacks proper security controls. Insecure networks may expose unencrypted EPHI. Examples of insecure networks include, but are not limited to, the Internet, unencrypted wireless networks, and poorly-secured private networks.

##### 3. Approved Methods for Transmitting EPHI

The following methods for transmitting EPHI are approved:

- Connection-base: Point-to-Point VPN;
- Remote Internet access: VPN client connection;
- Web-based: Secure Socket Layer (SSL);
- File-based: Secure Copy (SCP);

All other forms of EPHI transmission are forbidden.

##### 4. Approved EPHI Ciphers

Approved encryption ciphers (algorithms) and minimum bit lengths, in order of preference are:

- AES: 192 bits
- Triple DES (3DES): 168 bits
- RC4: 128 bits

Use the strongest available cipher. Longer bit lengths may be used; shorter lengths are forbidden. Any cipher not explicitly allowed is denied.

#### **f. Prevention and Detection of Malicious Software**

TAC has an enterprise-level virus-scanning application. All desktops shall have anti-AdWare and SpyWare applications installed.

Recommended processes to prevent virus problems:

- Always run the Corporate standard. Supported anti-virus software is available from the corporate download site. Download and run the current version. Download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check this Recommended Processes list for updates.

**g. Systems Development and Maintenance.**

All systems development and maintenance activities shall take into consideration HIPAA and industry standard security practices and ensure that said systems and/or maintenance activities result in compliance with those requirements and standards.

---

## **PART 4. Compliance with Legal Requirements**

---

TAC information security policies were drafted to meet or exceed the protections found in existing laws and regulations, and any TAC information security policy believed to be in conflict with existing laws or regulations must be promptly reported to the TAC Legal Department and to the CIO.

---

## **PART 5. Disaster Recovery and Business Continuity**

---

TAC will maintain a set of contingency plans that includes a data backup plan, disaster recovery plan, and emergency mode operation plan. These plans will include testing and

revision procedures. A risk analysis shall be performed periodically to ensure that these plans remain relevant.

**a. Applications and Data Criticality Analysis**

The Plan, and revisions/updates to the Plan shall take into consideration the relative criticality of specific applications and data in support of other contingency plan components.

**b. Contingency Plans.**

Contingency plans shall be written and maintained to ensure the availability of business critical IT operations in the event of loss of service. Contingency plans include:

1. Data Backup Plan

The purpose of the data backup plan is to establish and implement policies and procedures to recover data in the event of loss. It will be the policy of TAC that exact retrievable copies of all EPHI as defined by the HIPAA Security Rule will be created on backup tapes. These tapes will be taken off-site to a vault by a 3<sup>rd</sup> party vendor.

2. Disaster Recovery Plan

The purpose of the disaster recovery plan is to establish and implement policies and procedures to reestablish business operations in the event of a catastrophic event. The disaster recovery plan shall include provisions for facility access controls and emergency access procedures.

3. Emergency Mode Operation Plan

The purpose of the emergency mode operation plan is to establish and implement policies and procedures to maintain critical business operations during an emergency. The emergency mode operation plan shall include provisions for facility access controls and emergency access procedures.

**c. Testing and Revision Procedures**

The Disaster Recovery Plan, the Emergency Mode Operation Plan, and the Backup Recovery Plan shall be tested at least once every twelve months – in whole or in part – and shall be appropriately revised as a result of any “lessons learned” or changed circumstances or conditions. The testing procedures shall include both technical and non-technical evaluations.