

# HIPAA SECURITY POLICIES

APRIL 4, 2004

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>		
Policy and Procedure		
Policy Number	Revision Number	Effective Date: 4/4/04
<b>Access Control</b>		
<p><b>Background:</b>     <b>164.312(a)(1)</b> The Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to take reasonable steps to prevent access of unauthorized workforce members, vendors, and contractors to Richmond Behavioral Health Authority’s information systems and to the testing and revision of software. This also means restricting access to Protected Health Information for only those entities that have access privileges.</p> <p>Access controls have to do with restricting access to resources (e.g., paper, disks, workstations) and allowing only privileged entities (e.g., persons and applications) to access Protected Health Information.</p>		
<p><b>Policy:</b>        It is the policy of the Richmond Behavioral Health Authority that the Privacy and Security Officers are responsible for establishing the policy and procedures for assigning access privileges to entities that need access to Protected Health Information.</p>		
<p><b>Procedures:</b></p> <ul style="list-style-type: none"> <li>○ <b>Unique User Identification:</b> <ol style="list-style-type: none"> <li>1. The Security Officer and MIS Department will be responsible for providing a unique name and/or number for identification to each new staff upon hire</li> <li>2. The MIS Department is to keep a log of Unique User Identification assignments to ensure that reuse of user ID’s is prohibited</li> </ol> </li> <li>○ <b>Emergency Access Procedure:</b> <ol style="list-style-type: none"> <li>1. The Security Officer and MIS Department will maintain a log of individuals who have authorized access to the site during emergency mode operations</li> </ol> </li> <li>○ <b>Automatic Log-Off</b> <ol style="list-style-type: none"> <li>1. The workstations will automatically lock-up after a predetermined time of inactivity and only pre-approved screen savers will be used on equipment</li> </ol> </li> </ul>		

RICHMOND BEHAVIORAL HEALTH AUTHORITY		
Protocol and Procedure		
Policy Number	Revision Number	Effective Date: 4/4/04
<b>Audit Trail</b>		
<p><b>Background:</b> The proposed HIPAA Security rule defines audit controls as “mechanisms employed to record and examine system activity” and the consensus seems to be that Audit Trail is “the result of monitoring each operation on information.” Generally, Audit Trail identifies <b>who</b> (login ID) did <b>what</b> (read-only, modify, delete, add, etc) to <b>specific data</b> (identify member and data about that member that was acted upon), and <b>when</b> (date/time stamp). Under the HIPAA Privacy Rule it is necessary to also know “<b>Why</b>” the data was accessed, so audit logs will need to go beyond the simple capture of login name, date/timestamp, and action taken associated with the data that was accessed.</p> <p>One of the purposes of the audit trail is to actively monitor access to Protected Health Information. Another is to be in a position to assess the damage should someone break-in or accidentally access Protected Health Information.</p>		
<p><b>Objective(s):</b> Establish Policy and Procedures for Audit Trail associated with applications and networks at Richmond Behavioral Health Authority (RBHA).</p>		
<p><b>Policy:</b> The RBHA MIS Department will provide an audit trail for applications and networks. The format of the logs is given in the description of the two logs -- login/logoff log and data access log.</p> <p>It is the responsibility of the Security Officer to analyze the logs to determine unauthorized access.</p> <p>All logs will be password protected.</p> <p>All logs will be retained for 6 years.</p>		

**Procedure:**

Inventory records, media records and configuration logs are affected by the acquisition of hardware and software. They all must be modified accordingly. Particular attention must be given to hardware devices and corresponding software that enable the transmission or transfer of Protected Health Information:

- Storage devices including but not limited to tape drives, CD-R/W, fixed disk drives and floppy disk drives
  - Remote access devices
  - Transmitting devices
- Unsecured telephones, PDAs and the like
  - Laptops

Attention must be also given to applications that transmit Protected Health Information.

*[Probably the best way to ready a workstation is to: (1) first create a standard hard disk image for a particular class of workstation, (2) duplicate it on the new workstation and (3) configure it for a particular person.]* When the items are installed or uninstalled, the configuration log will be initiated or modified accordingly. Refer to the policy and procedure for Security Configuration Management.

**Only acquisitions of hardware and software that that are designed to keep Protected Health Information safe are to be ordered and installed. This is a judgment call; but, factors to consider include the benefits that the item enables, the vulnerabilities that it enables, and the risk of Protected Health Information being disclosed.**

## **Login/Logoffs Log**

The elements of the log are as follows:

Identification of the person making the access

- Surname
- Middle initial
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

Organization making the entry

Role of the person making the access

Name of application and version number that is used to access data (application could be on a mainframe, server or workstation)

Date and time stamp of login

Date and time stamp of logoff

Note: This log is at the application level. In some instances, it is prudent to record which network the user used to enter the network, where the data resides, and the authentication server that was used to authenticate the user.

## Data Access Log

The elements of the log are as follows:

Identification of the person making the access

- Surname
- Middle initial
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

Organization making the entry

Name of application and version number that is used to access the data (application could be on a mainframe, server or workstation)

Date and time stamp of Access

Operation being performed (read-only, add, modify, delete)

Purpose of operation (many times this can be inferred from the operation or transaction)

Name of the individual (subject) whose record is being accessed

Data actually accessed (in practice this is likely to be less than the ideal)

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

### **(Chief) Security Officer**

**Background:** The Security Officer's main focus is to protect information from unauthorized access, unauthorized modification, and still have the information available to those that need it.

**Objective(s):** Establish accountability for security in Richmond Behavioral Health Authority (RBHA).

**Policy:** The Security Officer will be accountable for: (1) developing and implementing security policies and procedures for RBHA and (2) training for all members of the workforce that come in contact with Protected Health information. The training program will be developed in conjunction with the Privacy Official who provides for privacy training.

The Security Officer will be responsible for conducting continuous risk assessment and analysis. As significant threats are discovered, management support for additional initiatives and countermeasures will need to be sought and implemented.

The Security Officer will be responsible for the security infrastructure of the organization. This will be done in conjunction with the Manager of Information Systems.

The Security Officer will be responsible for preparing annually a Security Certification Report (refer to the policy for Certification).

The Security Officer along with the Privacy Officer are responsible for mitigating the affects of all disclosures that are not HIPAA compliant or contrary to the RBHA's own security goals.

The Security Officer will be responsible for assuring supervision of maintenance personnel by an authorized, knowledgeable person and having formal procedures and instructions for the oversight of computer and network maintenance personnel when the personnel are near health information pertaining to an individual.

## ***RICHMOND BEHAVIORAL HEALTH AUTHORITY***

### Protocol and Procedure

Policy Number

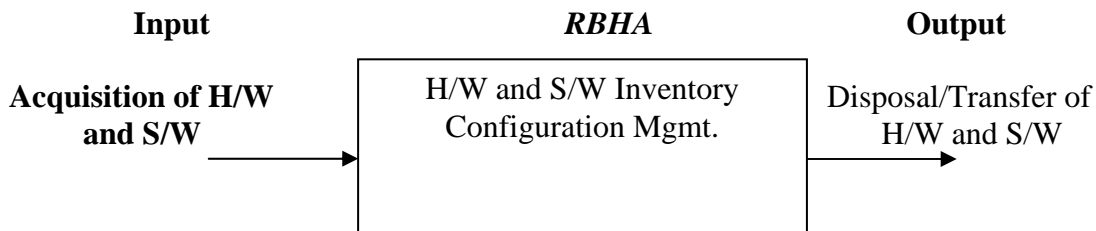
Revision Number

Effective Date: 4/4/04

## **Device and Media Controls *164.310 (d)(1)***

**Acquisition Of Hardware and Software:** One of the prime security vulnerabilities is unauthorized hardware and software on computers within Richmond Behavioral Health Authority (RBHA). It is important for to only allow acquisition of hardware and software that is authorized to be acquired and installed. The primary reason for this is to minimize the risk of having unauthorized Protected Health Information from being electronically transmitted or physically taken from RBHA.

The diagram below identifies some mechanisms (policies) for controlling hardware and software. It provides context for the Acquisition of Hardware and Software policy.



**Policy:** It is the policy of *RBHA* to ensure that all procedures governing the receipt and removal of hardware and electronic media that contain PHI into and out of *RBHA*, and the movement of these items within the facility will be adhered to by all workforce members. Additionally, all members of the workforce will follow policies on disposing, removing, acquiring and installing hardware and software with the purpose of preventing unauthorized Protected Health Information from being electronically transmitted or physically taken from *RBHA*.

**Procedure:** All orders of computer hardware and software will be approved by the *MIS Department* even if the price of the item is zero or another organization is willing to pay *RBHA* to install the item.

All computer hardware and software will be installed by the *MIS Department*. No installation is to be performed by members of the workforce that are unauthorized by the *MIS Department*.

Devices and software that have the potential to transmit or transfer Protected Health Information should be minimized and only authorized for certain computers.

Inventory records, media records and configuration logs are affected by the acquisition of hardware and software. They all must be modified accordingly.

Particular attention must be given to hardware devices and corresponding software that enable the transmission or transfer of Protected Health Information:

- Storage devices including but not limited to tape drives, CD-R/W, fixed disk drives and floppy disk drives
- Remote access devices
- Transmitting devices
- Unsecured telephones, PDAs and the like
- Laptops

Attention must be also given to applications that transmit Protected Health Information.

*[Probably the best way to ready a workstation is to: (1) first create a standard hard disk image for a particular class of workstation, (2) duplicate it on the new workstation and (3) configure it for a particular person.].* When the items are installed or uninstalled, the configuration log will be initiated or modified accordingly. *Refer to the policy and procedure for Security Configuration Management.*

Only acquisitions of hardware and software that that are designed to keep Protected Health Information safe are to be ordered and installed. This is a judgment call; but, factors to consider include the benefits that the item enables, the vulnerabilities that it enables, and the risk of Protected Health Information being disclosed.

**Audit Trail:** The HIPAA Security rule defines audit controls as “mechanisms employed to record and examine system activity” and the consensus seems to be that Audit Trail is “the result of monitoring each operation on information.” Generally, Audit Trail identifies **who** (login ID) did **what** (read-only, modify, delete, add, etc) to **specific data** (identify member and data about that member that was acted upon), and **when** (date/time stamp). Under the HIPAA Privacy Rule it is necessary to also know “**Why**” the data was accessed, so audit logs will need to go beyond the simple capture of login name, date/timestamp, and action taken associated with the data that was accessed.

One of the purposes of the audit trail is to actively monitor access to Protected Health Information. Another is to be in a position to assess the damage should someone break-in or accidentally access Protected Health Information.

Establish Policy and Procedures for Audit Trail associated with applications and networks at RBHA.

The *RBHA MIS Department* will provide an audit trail for applications and networks. The

format of the logs is given in the description of the two logs -- login/logoff log and data access log.

It is the responsibility of the Security Officer to analyze the logs to determine unauthorized access.

All logs will be password protected.

All logs will be retained for 6 years.

### **Login/Logoffs Log**

The elements of the log are as follows:

Identification of the person making the access

- Surname
- Middle initial
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

Organization making the entry

Role of the person making the access

Name of application and version number that is used to access data (application could be on a mainframe, server or workstation)

Date and time stamp of login

Date and time stamp of logoff

Note: This log is at the application level. In some instances, it is prudent to record which network the user used to enter the network, where the data resides, and the authentication server that was used to authenticate the user.

## **Data Access Log**

The elements of the log are as follows:

Identification of the person making the access

- Surname
- Middle initial
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

Organization making the entry

Name of application and version number that is used to access the data (application could be on a mainframe, server or workstation)

Date and time stamp of Access

Operation being performed (read-only, add, modify, delete)

Purpose of operation (many times this can be inferred from the operation or transaction)

Name of the individual (subject) whose record is being accessed

Data actually accessed (in practice this is likely to be less than the ideal))

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

## Facility Access Controls

**Background:** *164.310(a)(1)* The Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to implement necessary policies, procedures, and safeguards to limit physical access to information systems. An important part of the overall security program is physical security. When routine, non-routine or contingent events occur, physical security must be maintained.

**Policy:** It is the policy of *Richmond Behavioral Health Authority* that the Security Officer is responsible for establishing the policy and procedures for physical access. An ID or security token will be issued to every member of the workforce. Keys will also be issued to selected members. Keys for access to the computer room or closet are to be highly restricted to MIS Department staff. Keys to the records area are also highly restricted to Medical Records' staff. When readable tokens are used, the Security Officer will maintain token readers at the MIS Computer/Server Room. The MIS Department will maintain a current list of physical access privileges for each person.

*Physical Security* -- The Security Officer will be responsible for coordinating with the HR Department as it relates to providing keys, tokens and ID cards and assigning physical access privilege. Physical access privileges assigned to the workforce (usually employees and contractors) are used in conjunction with keys, tokens and ID cards. [If ID cards are used, there may be corresponding badge readers.]

### Access Privilege Log

#### Identification

- Surname
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

Organization making the entry

Role (or other category)

Date role assigned

Date role revoked

Privileges  
Date privileges assigned  
Date privileges revoked

Exception privileges  
Date exception privileges assigned  
Date exception privileges revoked

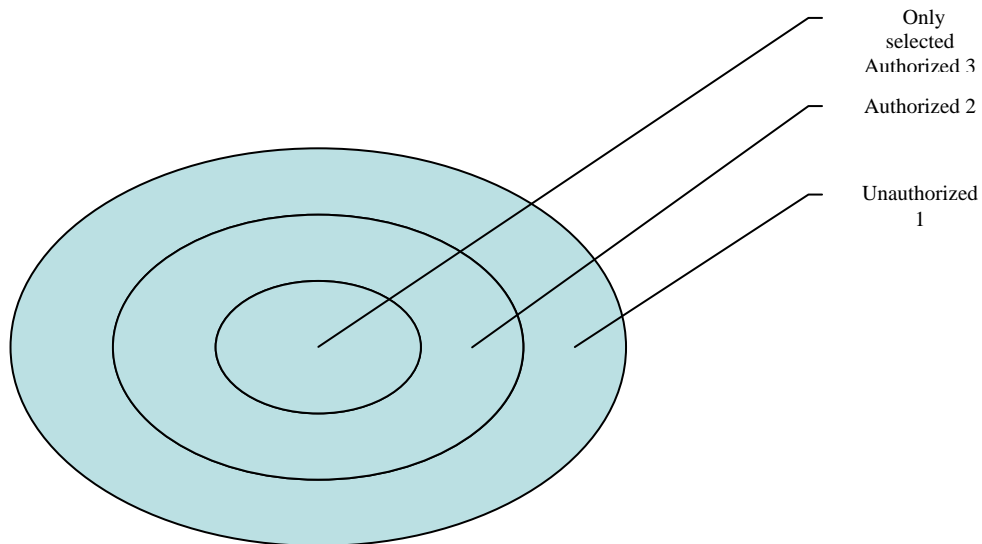
Date last audited

### **Contingency Operations**

Physical security will entail the following:

- Establish a security perimeter around the facility to keep unauthorized people out
- Knowing who crossed the perimeter, in the event of an emergency
- Make it everyone's task to ask anyone that is not a consumer or a member of the workforce if he is authorized to be inside the perimeter

#### RINGS OF SECURITY PERIMETER



During normal work hours anyone can enter ring 1. Only authorized people may enter ring 2. Few people are permitted in areas that are designated as ring 3 areas which are used for Emergency Physical Access only.

The following table indicates who should be authorized in each ring.

Ring/Areas	Those Authorized
Ring 1- Lobby, public bathrooms	Anyone during business hours
Ring 2- Hallways, group rooms, medical section, and service delivery areas	Only authorized consumers and members of the workforce
Ring 3- Computer Room/Medical Records/Human Resources	Selected members of workforce, Security Officer, IS and Medical Records staff

A contingency plan is developed to provide the best possible recovery capability in the event that recovery and security measures were not effective and some loss of capability or data has occurred. One of the values of a contingency plan is that planning has taken place before the contingency event; therefore, valuable recovery time is not lost in planning *"after the fact"*.

The emphasis is on system and data recovery/contingency planning, not business recovery.

The Information Systems Department is responsible for maintaining the disaster recovery and contingency plan (*Policy #* ) for system and data recovery. The plan identifies the roles and associated responsibilities should a contingency event occur.

This plan is integrated in the overall business recovery and contingency plan.

This procedure is for short time outages only. Long term outages are covered by the disaster recovery and contingency plan.

If the information system is down for any reason, it is important that operations continue. This can most easily be done by relying on manual operating contingency procedures.

- Once a system is down for a specified period as determined by the Security Officer or Manager of Information Systems in conjunction with the Executive Director, a code blue alert for a particular system will be declared. While the data from the system will temporarily be unavailable, information that normally is entered in the system will be accumulated manually using the input forms.

Upon recovery of the system, the information system service will be restored, accumulated forms will be entered into the system and the code alert cancelled.

## **Facility Security Plan**

The facility security plan focuses on accessibility and integrity of data through such mechanisms as firewalls, access controls, and encrypting data when the information is transmitted or stored. Policies and procedures are established to ensure the prevention; detection, containment, and correction of security breaches involving risk analysis and risk management.

The Security Officer will ensure:

- Locked access to sensitive areas such as Computer Room/Systems Room
- Maintain In/Out log of selected authorized staff who has physical access to sensitive areas

## **Access Control and Validation Procedures**

- All consumers and visitors (including vendors) will sign in upon entry and will be escorted at all times (facilitated by lobby receptionist and security guards)
- All staff will wear identification badges and visitors will wear visitors badges when in facility (visitors will turn in passes upon signing out of building)

## **Maintenance Records**

- The MIS Department will maintain an up-to-date configuration log for every computer system
- The Security Officer will maintain a log of events regarding repairs and modifications to all physical components of the facility including hardware, locks, doors, and walls.

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

## Information Access Management

**Background:** *164.308(a)(4)* Information Access Management has to do with creation, administration, and oversight of policies to ensure that personnel are granted levels of access to electronic protected health information based on their responsibilities.

**POLICY:** It is the policy of Richmond Behavioral Health Authority (RBHA) to adhere to standards set by HIPAA and that only authorized personnel will be granted access electronic protected health information (PHI) by:

- Establishing an access privilege log
- Maintaining a record to track modifications to access rights and privileges

### **Isolating Health Care Clearinghouse Function**

- Implementing procedures to isolate Health Care Clearinghouse functions to ensure that only authorized personnel have access to electronic PHI

### **Access Authorization**

In order to appropriately comply with the Security Standards and effectively maintain healthcare operations, access will be determined by a role-based and context-based assessment:

- Access to a consumer's PHI will be available to the direct service provider, his/her immediate supervisor, and other providers on the same service unit/team
- Emergency Services/Crisis Intervention staff will have access to all consumers' PHI
- Direct service providers, Managers/Supervisors, Executive Director, Healthcare operations staff will have access to all consumers' PHI
- Medical Records staff will have access to consumers' PHI
- Reimbursement staff will have access to all consumers' PHI
- IT staff will have access to all consumers' PHI
- Data Entry staff will have access to all consumers' PHI, as needed, to complete

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

data entry

- Facility Coordinator and Facility Maintenance staff will not have access to any consumer PHI

### **Procedures to Ensure Appropriate Access and Access Authorization**

- Upon hire, each staff member will be identified by the “class” in which their job functions fall
- *Human Resource staff or Supervisors* will ensure that new hires complete the appropriate *Access Request form* in order to establish the appropriate level of access, and request a unique user identification number; Supervisors must sign this form to verify accuracy
- IT staff will ensure that staff are trained during their orientation, to include information on the degree of access permissible by their job functions, security policies and procedures, and setting of passwords
- Removable media (i.e. diskettes, CD’s, zip disks, etc.) that contain PHI will be secured at all times to prevent unauthorized access
  - If any removable media is lost or misplaced, an agency *Incident Form* must be completed by the staff member and processed as per the *Risk Management Policy*
- *All PHI is to be kept in the agency’s client data system. In instances when PHI must be kept temporarily on individual hard drives, access must be limited by protecting the file. .*
- As per *RBHA* IT policy, staff should log-off when leaving a workstation to prevent unauthorized access
- *Client Data System/ PC’s* will have automatic lockout when the workstation has been unattended for \_\_\_\_ time, to ensure security of PHI and to prevent unauthorized access
- IT staff will periodically audit usage, to the degree possible, to identify any unauthorized access by staff
- IT staff will review, audit and modify access levels on a periodic basis
- Supervisors and IT staff will ensure that access to electronic PHI is terminated at an employee’s termination from employment, and re-assessed for access limitations in the event of transfer from one job class (i.e. category) to another
  - *Supervisors* will ensure that all access devices are returned by the employee at the time of termination or transfer (if appropriate), and document this on the appropriate form
  - *Supervisors or Human Resources staff* will ensure that IT staff are informed of all staff terminations
  - In the event of an adverse staff termination, IT staff will be notified prior to informing the staff member, to ensure that information and

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

- systems are protected from potential retaliation
- IT staff will remove the staff member's name from internal e-mail systems and system access lists, and disable access to the network

*Physical Security* -- The Human Resources Department will be responsible for providing keys and ID cards and assigning physical access privileges. Physical access privileges assigned to the workforce (usually employees and contractors) are used in conjunction with keys and ID cards. [If ID cards are used, there may be corresponding badge readers.] Physical access privileges are used to restrict entry into buildings and certain areas or rooms. Refer to the Policy for Physical Access Control. The Department is to keep a log of privilege assignments (refer to the Sample Access Privilege Log).

### **Access Establishment and Modification**

Access controls have to do with restricting access to resources (e.g., paper, disks, workstations) and allowing only privileged entities (e.g., persons and applications) to access Protected Health Information. Individuals may, for example, have privileges based on the role of the individual, the time of day, the location, transaction type, department, or assigned by name. Examples of roles include a billing clerk or counselor working in Detox. The principal objective of access controls is to restrict access to only authorized entities.

Establishing access controls policy is the process for assigning privileges to people and other entities. It does not cover authentication of access control privileges via passwords or any other technical security services or mechanisms. Refer to the policies for Password Usage and Technical Security Services.

Establishing access controls is not to be confused with verifying identities. Refer to the policy and procedure for Verifying Identities.

*Information System Access Security* -- The Security Officer and Information Systems Department will be responsible for assigning Protected Health Information access privileges to authorized entities. The Department is to keep a log of privilege assignments (refer to the Sample Access Privilege Log).

A member of the workforce is not authorized to access another member of the workforce's client record or Designated Record Set unless it is for the purpose of treatment, payment or operations that is associated with the workforce member. The logs referred to above must be kept for six years. Refer to the Document Retention Policy.

The access control restrictions placed on the external users are the same or similar as the

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

access control restrictions that are placed on internal users.

Relative to information system access, all authorized users will need to sign on to the network before signing on to specific applications or desktops.

Emergency access relating to treatment, payment, or health care operations must be provided. The Information System Department will provide the procedures for emergency access.

The Privacy and Security Officers will establish a written privileges matrix that relates roles or other categories to physical and information access privileges. An entity or person may have more than one role. The matrix will be used by the Human Resources and Information Systems Departments to assign privileges. The Privacy Officer must approve all exceptions to the privileges matrix in writing.

The Privacy and Security Officers will audit entities or persons with access to Protected Health Information once a year using, for example, sampling techniques or actual access logs for specific systems. The results of the audit are to be documented.

## Access Privilege Log

### Identification

- Surname
- Given name(s)
- Universal ID (if available)
- Social security number
- Local ID1
- Local ID2

### Organization making the entry

#### Role (or other category)

Date role assigned

Date role revoked

#### Privileges

Date privileges assigned

Date privileges revoked

#### Exception privileges

Date exception privileges assigned

Date exception privileges revoked

Date last audited

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>		
Protocol and Procedure		
Policy Number	Revision Number	Effective Date: 4/4/04
<b>Security Management Process- Review, Response, Reporting</b>		

**POLICY STATEMENT:**

It is the policy of Richmond Behavioral Health Authority to manage the security of all electronic protected health information (ePHI). Information system security exists to guard ePHI from improper alteration or destruction. Further, a regular review of information activity is conducted to detect information system security violations, followed by a defined response and reporting procedure to contain and correct violations when suspected or confirmed violations are noted or reported.

**HIPAA SECURITY REGULATIONS ADDRESSED IN THIS POLICY:**

164.308(a)(1)(i) – Implement policies and procedures to prevent, detect, contain and correct security violations.

164.308(a)(1)(ii)(D) – Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

164.308(a)(5)(ii)(C) – Implement procedures for monitoring log-in attempts and reporting discrepancies.

164.308(a)(6)(i) – Implement policies and procedures to address security incidents.

164.308(a)(6)(ii) – Identify and respond to suspected or know security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

164.312(c)(1) – Implement policies and procedures to protect ePHI from improper alteration or destruction.

164.312.(c)(2) - Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

## PROCEDURE(S):

### I. PREPARATION POCESSES

- A. Security plans are developed for each system, platform, and protocol.
- B. The information system's audit trail tracking function is capable of reporting:
  - 1. all access codes logged into the system by date and time, and the location of information provided or removed;
  - 2. any unauthorized access attempts that are made;
  - 3. in such a way as to be downloaded to electronic tapes and stores off-site every month.
- C. Any changes or modifications made to the information system involving hardware, software, system configuration, system proceedings, the network is recorded for potential review in an investigation concerning a security incident.
- D. Integrity controls are implemented in the information system to minimize the risk that data can be improperly altered or destroyed.
- E. Acceptable levels of risk are defined, and minimum review frequency standards are determined for random reviews.
- F. *The Management Team*, and any designees, has a general idea of security issues and the security plans developed.
- G. Agency employees are trained on the security measures regarding ePHI upon initial orientation to the agency as a new employee and reviewed annually.
- H. An employee's access to view or update or input ePHI is determined by the position held [role based] within the agency.
- I. Employees allowed to update or input information into the Information System are thoroughly trained and their work is monitored to ensure compliance.
- J. The Security Management Process is evaluated and reviewed annually by the Security Officer.

- K. Documented changes to the Security Management Process will be communicated to all employees.

## II. REVIEW AND DETECTION PROCESS

- A. Random reviews of information system usage will include unannounced site surveys, verification of data entry accuracy, exception reporting, log-in attempts, and information system activity report. Timing of random reviews is determined by minimum frequency standards for each type of review and strategic events such as upgrades or system changes. Areas of review may include:
  - 1. Activity in the system when agency or IT department is not open;
  - 2. Activity in the system that is outside the assigned security level of the user;
  - 3. Unusual drops or spikes in disk space utilized by users;
  - 4. Log-in attempts and discrepancies;
  - 5. Users who do not log off at the end of their shift;
  - 6. Users that have sign-ons logged for days they are not working;
  - 7. Unusual activity in security management areas or high level table maintenance or system profile access;
  - 8. Users with no activity within a specified time period; remove accesses as appropriate based on inactive accounts.
- B. Specific review efforts shall be logged including date of review, type of review, staff member performing review, a brief listing of any violations noted against accepted levels of risk, and action taken. Any discrepancies or violations, suspected or confirmed, are reported immediately to the Security Officer and *Director of Corporate Compliance*. The Security Officer reviews the log at least monthly. The log is copied and forwarded to the *Director of Corporate Compliance* at least monthly.
- C. Agency employees have the obligation to report any discrepancies or violations, suspected or confirmed, immediately to the Security Officer and *Director of Corporate Compliance*.

## III. RESPONSE PROCESSES

### A. CONTAINMENT PROCESS

- 1. The Security Officer has the right to terminate any information system user's access at any time. Notification of immediate access termination due to suspected or confirmed information security violation will be communicated to the employee's immediate supervisor, the supervisor's Director,

Director of Administration, and *Director of Corporate Compliance*.

2. The Security Officer had the right to limit or terminate employees' access to the information systems in order to conduct an assessment of damage due to an information security violation.
3. A review of the information system's security processes is overseen by the Security Officer, or his designee, to determine the security breach and its impact on the systems and information maintained on the system. The Security Incident Response Team will include the Security Officer, or his designee, the *Director of Corporate Compliance*, and other employees as appointed by them.
4. A summary of assessment findings is documented and used in the Correction Process defined following.

#### B. CORRECTION PROCESS

1. The summary of assessment findings is used by the access user's supervisor, HR Administrator, and Director of Administration to determine corrective action as outlined in the *Agency Code of Conduct and Performance Expectations' Corrective Actions* policy. As applicable, law enforcement will be contacted.
2. The Security Incident Response Team will make recommendations to the *Management Team* concerning action necessary to mitigate, to the extent practical, any harmful effects of the security incident. As appropriate, the *Management Team* will report to or involve the Board.
3. The summary of assessment findings is used to update equipment, information procedures or policies in such a way as to prevent future security violations of this nature.

#### IV. DOCUMENTATION

- A. A manual will be maintained by the Security Officer which will document the following:
  1. Incident triggering investigation of suspected or known security violation;
  2. Actions taken and by whom to contain security breach;
  3. Actions taken and by whom to correct security breach;

4. Actions taken and by whom to mitigate harmful effects of the security breach.

B. The documentation in the manual will be kept at least 6 years.

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

## Workforce Security

**Background:** *164.308(a)(3)* The Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to take reasonable steps to ensure workforce security that includes appropriate authorization and/or supervision of staff accessing electronic PHI, workforce clearance procedures, and termination procedures. This also means restricting access to Protected Health Information for only those entities that have access privileges.

### Authorization and/or Supervision

The Security Officer will be responsible for the security infrastructure, training and oversight of computer and network maintenance personnel and will be accountable for:

- Developing and implementing security policies and procedures for Richmond Behavioral Health Authority
- Training all members of the workforce on access methods to electronic systems and information
- Identifying the persons or classes of persons in the workforce who need access to PHI
- Identifying the category(ies) of PHI to which access is needed
- Implementing procedures:
  1. review appropriate use of access by staff ID to ensure that access to electronic PHI is limited to the persons or class of persons needing access to achieve the purpose of their job,
  2. for review and approval of requests for access and ensuring supervisory sign-off on security add/change/delete requests, and auditing outstanding access devices (e.g. keys, swipe cards, etc.) and are returned at the time of a staff termination
  3. monitor all access to high profile or VIP consumer records
  4. ensure required screen saver/terminal locking is executed

### Workforce Clearance Procedure

An important part of the overall workforce clearance procedure is to ensure that individuals have the appropriate level of access and to prevent other workforce members who should not have access from gaining access. As the IS develops the capability of electronically restricting access, implementation of access controls will be handled through the MIS department.

# RICHMOND BEHAVIORAL HEALTH AUTHORITY

## Protocol and Procedure

Policy Number

Revision Number

Effective Date: 4/4/04

### **Procedures:**

- Upon hire, each staff member will be identified, cleared and recorded by the “class” in which their job functions fall before granting access to electronic protected health information
- The appropriate access level will be set according to the Information Access Management Policy.

### **Termination Procedures**

- Supervisors, Security Officer and IT staff will ensure that access to electronic PHI is terminated at an employee’s termination from employment, and re-assessed for access limitations in the event of transfer from one job class (i.e. category) to another
- Supervisors will ensure that all access devices are returned by the employee at the time of termination or transfer (if appropriate), and document this on the appropriate form
- Supervisors or the Security Officer will ensure that IT staff are informed of all staff terminations
- In the event of an adverse staff termination, IT staff will be notified prior to informing the staff member, to ensure that information and systems are protected from potential retaliation
- The Security Officer will ensure that the staff member’s name from internal e-mail systems, system access lists, and disable access to the network



**PROTOCOL/PROCEDURES:**

Consumer and/or employee PHI information will be regarded as confidential, and may not be used or disclosed except to authorized users for approved purposes. Access to PHI is only permitted for direct consumer care, approved administrative and/or supervisory functions, or with approval of the Privacy Officer, Security Officer, Director of Quality and Standards, Executive Director, or Human Resources Director.

**Permitted Use and Disclosures:**

The RBHA is permitted to use or disclose PHI in the following instances:

- To the individual who is the subject of the PHI
- In compliance with consent to carry out treatment, payment or health care operations;
- Without consent, if consent is not required and has not been sought;
- Pursuant to an Agreement.

<b>RICHMONT BEHAVIORAL HEALTH AUTHORITY</b>
Protocol and Procedure

**HIPAA SANCTIONS: Privacy and Security Violations**

**Required Disclosures:**

The RBHA is required to disclose PHI in the following instances:

- To an individual, when requested under and as required by SS164.524 (Access of individuals to PHI) or SS164.528 (Accounting of disclosure of PHI) of the HIPAA Regulations;
- To specific private entities that provide services under contractual agreements (health benefits, life insurance, Workers Compensation, etc.) in order to provide such services;
- When required by the Privacy Officer, Security Officer, Executive Director, Director of Quality and Standards, or Human Resources Director to investigate or determine compliance with HIPAA requirements.

**Minimum Necessary:**

When using or disclosing PHI, or when requesting PHI from another covered entity, the RBHA will make reasonable efforts to limit PHI to minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Minimum Necessary Provision applies to all other situations except it **does not apply to treatment or the following:**

- disclosures to or requests by a *health care provider for treatment;*

- uses or disclosures made to the *individual*;
- uses and disclosures made pursuant to an *authorization from the individual*;
- disclosures made to the *Secretary of U.S. Department of Health and Human Services*;
- uses or disclosures that are *required by law*; and
- uses or disclosures that is required for *compliance* with HIPAA.

**Sanction Exemptions:**

Sanctions will not apply to disclosures by employees who are *whistleblowers* or *crime victims*. The RBHA is not considered to have violated PHI disclosure requirements if the disclosure is by an employee or business associate as follows:

Disclosure by Whistleblowers:

- The employee is acting in good faith on the belief that the RBHA has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or,

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>
Protocol and Procedure
<b>HIPAA SANCTIONS: Privacy and Security Violations</b>

- That the care, services and conditions provided by the RBHA potentially endangers one (or more) RBHA consumer, employee or a member of the general public; or,
- The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered entity; or,
- The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the RBHA; or
- The disclosure is made to an attorney retained by or on behalf of the employee or business associate for the purpose of determining legal options regarding disclosure conduct.

Disclosure by Crime Victims:

A covered entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is a victim of a criminal act discloses PHI to a law enforcement official about the suspected perpetrator of the criminal act, and the disclosed PHI is limited to identification and location purposes.

**Mitigation:**

Mitigating circumstances include conditions that would support reducing the sanction in the interest of fairness and objectivity. The RBHA will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of PHI in violation of HIPAA regulations.

**Retaliation:**

The RBHA will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

- Exercises his rights or participates in the RBHA complaint process; or,
- Files a complaint with the Secretary of Health and Human Services; or,
- Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing; or,

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>
Protocol and Procedure

**HIPAA SANCTIONS: Privacy and Security Violations**

- Opposes any act or practice unlawful under HIPAA, providing that the individual acted in good faith, believing that the practice was unlawful, the manner of opposition is reasonable, and does not involve disclosure of PHI in violation of HIPAA regulations.

**PROCEDURES:**

consumer information in a public area; an employee leaves a copy of consumer medical information in a public area; an employee leaves a computer unattended in an accessible area with consumer information unsecured.

**Group II: Unauthorized use and/or misuse of PHI or records:**

This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with RBHA policies and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee looks up birth dates, address of friends or relatives; an employee accesses and reviews the record of a consumer out of curiosity or concern; an employee reviews a public personality’s record.

**Group III: Willful and/or intentional disclosure of PHI or records:**

This level of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent. Examples include, but are not limited to: an employee reviews a consumer record to use information in a personal relationship; an employee compiles a mailing list for personal use or to be sold.

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>
Protocol and Procedure

**HIPAA SANCTIONS: Privacy and Security Violations****Documentation:****Initial Reporting:**

Employees who observe or are aware of a breach must immediately report it to his/her Supervisor. The Supervisor will report the breach to the Privacy Officer and Security Officer, who will notify the Director of Quality and Standards, Executive Director and Human Resources Director.

Failure to report a breach of which one has knowledge will result in appropriate disciplinary action. Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

**Clear-cut Level I Breaches:**

For a breach involving any staff that is clearly a Level I breach, the Privacy Officer and Security Officer in conjunction with employee Supervisor, Director of Quality and Standards, Executive Director and Human Resources Director, will develop and implement an appropriate Plan of Correction, and in a timely manner.

**Breaches Other Than Clear-cut Level I Breaches:**

For all levels other than a clear-cut Level I breach, the Privacy Officer and Security Officer will establish an Investigation Team that will include senior Management and Human Resources representation, and/or legal counsel participation or consultation as instructed by the Executive Director.

The Investigation Team will conduct an appropriate investigation, commensurate with the level of breach and specific facts. This may include, but is not limited to, interviewing the employee accused of the breach, interviewing other employees or consumers, and reviewing documentation.

Upon conclusion of the investigation, the Investigation Team will prepare a written report including all findings and conclusions regarding the alleged breach, and forward it to the Privacy Officer and Security Officer. The Executive Director will make final determination of the appropriate disciplinary action, based on the report of the Investigation Team.

<b>RICHMOND BEHAVIORAL HEALTH AUTHORITY</b>
Protocol and Procedure
<b>HIPAA SANCTIONS</b>

**Reporting and Filing Requirements:**

For all levels of breach, after final resolution the initial report and all supporting documentation will be filed in a confidential file with the Privacy Officer and Security Officer. A copy of the report and supporting documentation will also be placed in the Personnel File of the employee.

RBHA will not participate in nor tolerate any form of retaliation against anyone filing a complaint against the agency. The central point of contact to report violations of this policy provides direct access to the Privacy Officer and Security Officer through the Division of Quality and Standards.

**DEFINITIONS:**

*“Confidentiality”* ---Entrusted communication of information that is considered private and implies an ethical or legal principle.

*“Confidentiality of Alcohol and Drug Abuse Patient Records”* ---The Confidentiality of Alcohol and Drug Abuse Patient Records rule (also known as 42 CFR, Chapter I, Part 2 or 42 CFR 2) establishes additional privacy provisions for records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with any drug or alcohol abuse program.

*“Good-Faith Reporting”* --- Reporting information known or believed to be true without fabrication or falsification.

*“Health Insurance Portability and Accountability Act of 1996”* ---A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives The United States Department of Health and Human Services (HHS) the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.

*“Investigation”* ---A detailed inquiry or systematic examination of the operations or a provider or its services regarding a violation of regulations or law. An investigation may be undertaken as a result of a complaint, an incident report, or other information that comes to the attention of the Privacy Officer and/or Security Officer.

*“Privacy Officer”* ---An individual identified by a covered entity to oversee the development, implementation, review, and revision of privacy policies and procedures and to ensure that the agency is compliant with all state and federal laws and regulations pertaining to privacy and confidentiality.

*“Security Officer”* ---An individual identified by a covered entity to oversee the development, implementation, review and revision of security policies and procedures to ensure that the agency is compliant with all state and federal laws and regulations pertaining to HIPAA Security Regulations.

*“Physical Security”* ---Pertains to the control of facilities and related offices and equipment.

# **RICHMOND BEHAVIORAL HEALTH AUTHORITY**

## **PROTOCOL AND PROCEDURES**

### **COMPLAINT REPORTING AND CENTRAL POINT OF CONTACT**

#### **PROCEDURE (S):**

1. Reporting of Privacy Violations
  - a. RBHA provides a central point of contact for all families and individuals served, agency employees, and/or those who serve as legally authorized representatives to report actual or perceived breaches of confidentiality:

Richmond Behavioral Health Authority  
Division of Quality and Standards  
Attention: Privacy Officer and Security Officer  
107 South Fifth Street  
Richmond, Virginia 23219  
Phone: 804-819-4000
  - b. Reports should be made promptly and in good-faith.
  - c. Reports can be made anonymously and/or confidentially. Individuals making complaints will be requested to submit their complaint in writing to the Privacy Officer and Security Officer.
  - d. If the individual requires assistance in documenting their complaint, the Privacy Officer and Security Officer or designee will provide the assistance.
  - e. Upon receiving a complaint, the Privacy Officer and Security Officer will proceed as directed in the policy and procedure titled *Privacy Investigation*.
  - f. An individual may report or make a complaint to the agency's Privacy Officer, Security Officer, Director of Quality and Standards, Executive Director, or Consumer Affairs staff if they believe a complaint resulted in retaliatory action by the agency.
  - g. If the individual requires assistance in making their complaint in written form, the Privacy Officer and Security Officer or designee will provide the necessary assistance.
2. Response of the Privacy Officer and Security Officer:
  - a. Upon receiving a complaint, the Privacy Officer and Security Officer will:

- (1) Document the receipt of the complaint
  - (2) Document the date, time, and name of the person making the Complaint and identifying them as consumer, authorized representative, or employee.
  - (3) Perform or coordinate the investigation of the complaint
  - (4) Determine the need to notify the Human Resources Manager
  - (5) Document and coordinate the investigation and the resolution of the complaint
  - (6) Communicate the outcome of the complaint to the appropriate individuals including, at a minimum, the Executive Director and Director of Quality and Standards
  - (7) If individuals are not satisfied with the results of the investigation, they have the right to proceed with external reporting to the Local Human Rights Advocate or the federal Department of Health and Human Services.
- b. Upon completion of the investigation the Privacy Officer and Security Officer will provide a written report to the Executive Director and Director of Quality and Standards.
- c. The Privacy Officer and Security Officer will provide yearly reports, which include; the number of complaints received, category of complaint, location cited in the complaint, and additional documentation from the investigations and resolutions of complaints.

## **Use of RBHA Resources**

**Computer, Internet, and E-mail Use:** The entire computer system, including e-mail, is the property of the RBHA. As such, all messages, documents or information contained within the system or sent via e-mail are also the property of the Authority. Consequently, all available computer functions should be used primarily for Authority business.

Because the content of e-mail messages can be intercepted and made public in a number of ways, it is important that you do not transmit confidential information or information that could be embarrassing to you or to the RBHA in e-mail transmissions. The Authority absolutely prohibits the use of e-mail to send any information, statements or opinions that are libelous, slanderous, defamatory, discriminatory, offensive, pornographic, inflammatory, threatening, or harassing.

Excessive personal use of the Authority's e-mail system will be considered inappropriate and may subject the employee to disciplinary action. Use of the Authority's e-mail system for limited personal use is permitted.

The RBHA also currently provides access to on-line information services, including Internet access, through a number of computer terminals. The following guidelines define acceptable use of the Internet and all other external information resources:

- Accessing of sexually explicit material or obscene information contained within any public or private electronic forum is strictly prohibited unless directly related to bona fide RBHA matters.
- The downloading of information or software files is prohibited unless directly related to RBHA business. All imported electronic material is subject to applicable copyright laws.

While recognizing reasonable privacy concerns, the Authority must maintain sufficient access to documents and e-mail messages to protect its interests and the interests of the RBHA's consumers. Accordingly, the RBHA retains the right to monitor any employee's computer, including e-mail and on-line site access, at anytime.

**Playing computer games on RBHA equipment at any time is prohibited, whether on or off duty.**

**The use of any RBHA equipment or resources for the benefit of other business or social entities is strictly prohibited.**

**Because a violation of this policy may cause liability to the RBHA, uniform compliance is expected. Failure to adhere to this policy may result in discipline, up to and including termination of employment.**

# HIPAA PRIVACY POLICIES

APRIL 4, 2003