HIPAA PRIVACY POLICY (Approved 7/30/2013)

To maintain appropriate administrative, technical, and physical safeguards to protect Private Health Information (PHI) in the Health Insurance Portability & Accountability Act (HIPAA)

PURPOSE - The purpose of this resolution is to comply with HIPPA standards that protect individuals' medical records and other personal health information.

A. ADMINISTRATION

1. The Executive Director and Senior Staff are responsible for the development and implementation of the policies and procedures for SCHRA and shall administer this Privacy Policy.

2. The Human Resources Manager shall serve as the Agency Privacy Officer and shall be responsible for receiving complaints and will answer requests for more information about the policy.

B. **TRAINING**

1. All employees shall receive training on the policies and procedures with respect to protected health information (PHI) as necessary and appropriate for the employees to perform their jobs.

2. Training shall be provided to each current employee and thereafter to new members of the workforce within a reasonable time after the person joins the staff and to each member of the workforce whose functions are affected by a change in the policies or procedures.

3. All training shall be documented by the Human Resources office.

C. MINIMUM NECESSARY USES AND DISCLOSURE OF PHI

It is the policy of the Agency to make a reasonable effort to use or disclose, or to request from another health care provider, the minimum amount of PHI required to achieve the particular use or disclosure unless an exception applies.

The Agency will identify people or classes of people in its work force who need access to PHI to carry out their duties, the category or categories of PHI to which access is needed, and any conditions appropriate to such access.

For any non-routine request for disclosure of PHI that does not meet an exception, the Agency will review the request for disclosure on an individual basis.

Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.

Procedure

1. The Agency will identify role based access to PHI per job description, including:

   a. People or classes of people in its workforce who need access to PHI to carry out their duties, and

   b. The category or categories of PHI to which access is needed, including any conditions that may be relevant to such access.

2. The Agency, for any type of disclosure or request for disclosure that is made on a routine and recurring basis, will limit the disclosed PHI, or the request for disclosure, to that which is reasonably necessary to achieve the purpose of the disclosure or request.

3. The Agency, for disclosures or requests for that are ***not*** made on a routine and recurring basis (non-routine disclosures), will review the request to verify that PHI disclosed or requested is the minimum necessary. All requests for non-routine disclosures or requests that do not meet an exception will be reviewed using standard criteria.

4. Exceptions to minimum necessary requirements: The Agency will release information without concern for the minimum necessary standard as follows:

   a. Disclosures to or requests by a health care provider for treatment.

   b. Uses or disclosures made to the individual who is the subject of the PHI.

   c. Uses or disclosures made pursuant to an authorization signed by the individual.

   d. Disclosures made to the Secretary of the U.S. Department of Health and Human Services (federal government).

   e. Disclosures that are required by law (such as for Department of Health state surveys, federal surveys, public health reportable events, FDA as related to product quality, safety, effectiveness or recalls etc.).

   f. Uses and disclosures that are required for compliance with the HIPAA Privacy Rule.

5. The Agency may use or disclose an individual's entire Medical Record only when such use or disclosure is specifically justified as the amount that is reasonably necessary to accomplish the intended purpose or one of the exceptions noted above applies.

6. Requests for entire Medical Records that are not covered by an exception will be reviewed using standard criteria.

7. Reasonable Reliance: The Agency may rely on a requested disclosure as minimum necessary for the stated purpose(s) when:

   a. Making disclosures to public officials, if the official represents that the information is the minimum necessary for the stated purpose(s).

   b. The information is requested by another covered entity (health care provider, clearinghouse or health plan).

c. The information is requested by a professional who is a member of the Agency's workforce or is a Business Associate of the Agency for the purpose of providing professional services to the Agency, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).

d. The information is requested for research purposes and the person requesting the information has provided documentation or representations to the Agency that meet the HIPAA Privacy Rule. Contact the Privacy Officer to assist in the determination of whether such requirements have been met.

8. The Agency, upon determination that the use, disclosure or request for PHI is the minimum necessary or one of the above exceptions apply (see Items 4 and 6), will release the PHI to the requestor.

9. Agency Requests for PHI from Another Covered Entity: When requesting PHI from another Covered Entity, the Agency must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are made on a routine and recurring basis, the Agency shall take reasonable steps to insure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

For requests that are not on a routine or recurring basis, the Agency shall evaluate the request according to the following criteria:

a. Is the purpose for the request stated with specificity?

b. Is the amount of PHI to be disclosed limited to the intended purpose?

c. Have the requirements for supporting documentation, statements, or representations been satisfied?

d. Have all applicable requirements of the HIPAA Privacy Rule been satisfied with respect to the request?

D. USES AND DISCLOSURES OF PHI

Disclosure of PHI will only be allowed with a properly completed and signed authorization except:

- When required or allowed by law.
- As defined in the *Notice of Privacy Practices*:
    - For continuing care (treatment)
    - To obtain payment for services (payment)
    - For the day-to-day operations of the facility and the care given to the consumers (health care operations)

Disclosure of PHI will be centralized through the Agency Privacy Officer. In some instances, the Agency Privacy Officer will need to track information that is disclosed. All disclosures designated as trackable must be approved by the Privacy Officer to enable the Agency to provide an accounting of disclosures when requested.

Disclosure of PHI will be carried out in accordance with all applicable legal requirements and in accordance with Agency policy. Each Agency will be responsible for researching and abiding by applicable state laws and regulations.

Original Medical Records will not be removed from the premises, except when ordered by subpoena or by other court order.

Procedure

Responding to Specific Types of Disclosures:

1. Media: No PHI shall be released to the news media or commercial organizations without the authorization of the consumer or his personal representative.

2. Telephone Requests: Staff members receiving requests for PHI via the telephone will make reasonable efforts to identify and verify that the requesting party is entitled to receive such information.

Disclosures to Persons Involved with a Consumer's Care:

1. The Agency may disclose to a family member, other relative, close friend, or any other person identified by the consumer, PHI:

    a. That is directly relevant to that person's involvement with the consumer's care or payment for care; or

    b. To notify such person of the consumer's location, general condition, or death.

2. Conditions if the Consumer is Present**.** If the consumer is present for, or otherwise available, prior to a permitted disclosure, then the Agency may use or disclose the PHI only if the Agency:

    a. Obtains the consumer's agreement;

    b. Provides the consumer with an opportunity to object to the disclosure, and the consumer does not express an objection (this opportunity to object and the consumer's response may be done orally); or

    c. May reasonably infer from the circumstances, based on the exercise of professional judgment, that the consumer does not object to the disclosure.

3. Conditions if the Consumer is Not Present or is Incapacitated**.** The Agency may, in the exercise of professional judgment, determine whether the disclosure is in the best interest

of the consumer, and, if so, disclose only that PHI which is directly relevant to the person's involvement with the consumer's care if:

a. The consumer is not present,

b. The opportunity to agree/object to the use or disclosure cannot practicably be provided because of the consumer's incapacity, or

c. In an emergency.

4. Confirming Identity**.** The Agency shall take reasonable steps to confirm the identity of a consumer's family member or friend. The Agency is permitted to rely on the circumstances as confirmation of involvement in care. For example, the fact that a person admits a consumer to the Agency and visits weekly is sufficient confirmation of involvement in the consumer's care.

E. AUTHORIZATION FOR RELEASE OF PHI

In accordance with the HIPAA Privacy Rule, when PHI is to be used or disclosed for purposes other than treatment, payment, or health care operations, the Agency will use and disclose it only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization.

Procedure

Exceptions to Authorization Requirements

PHI may be disclosed without an authorization if the disclosure is:

1. Requested by the consumer or his personal representative (authorization is never required);
2. For the purpose of treatment;
3. For the purpose of the Agency's payment activities, or the payment activities of the entity receiving the PHI;
4. For the purpose of the Agency's health care operations;
5. In limited circumstances, for the health care operations of another Covered Entity, if the other Covered Entity has or had a relationship with the consumer;
6. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the HIPAA Privacy Rule; or
7. Required by other state or federal law.

Use or Disclosure Pursuant to an Authorization

1. When the Agency receives a request for disclosure of PHI, the Agency Privacy Officer shall determine whether an authorization is required prior to disclosing the PHI.

2. PHI may never be used or disclosed in the absence of a valid written authorization if the use or disclosure is:

    a. Of psychotherapy notes as defined by the HIPAA Privacy Rule;

    b. For the purpose of marketing; or

    c. For the purpose of fundraising.

3. If the use or disclosure requires a written authorization, the Agency shall not use or disclose the PHI unless the request for disclosure is accompanied by a valid authorization.

4. If the request for disclosure is not accompanied by a written authorization, the Agency Privacy Officer shall notify the requestor that it is unable to provide the PHI requested. The Privacy Officer will supply the requestor with an *Authorization to Use or Disclose PHI* ("*Authorization*") form.

(See sample *Authorization* form following this Policy.)

5. If the request for disclosure is accompanied by a written authorization, the Privacy Officer will review the authorization to assure that it is valid (see the "Checklist for Valid Authorization" following this Policy).

6. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Privacy Officer will notify the requestor, in writing, of the deficiencies in the authorization. No PHI will be disclosed unless and until a valid authorization is received.

7. If the authorization is valid, the Privacy Officer will disclose the requested PHI to the requester. Only the PHI specified in the authorization will be disclosed.

8. Each authorization shall be filed in the consumer's Medical Record.

Preparing an Authorization for Use or Disclosure

1. When the Agency is using or disclosing PHI and an authorization is required for the use or disclosure, the Agency will not use or disclose the PHI without a valid written authorization from the consumer or the consumer's personal representative.

2. The *Authorization* form must be fully completed, signed and dated by the consumer or the consumer's personal representative before the PHI is used or disclosed.

3. The Agency may not condition the provision of treatment on the receipt of an authorization except in the following limited circumstances:

    a. The provision of research-related treatment; or

b. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).

4. An authorization may not be combined with any other document unless one of the following exceptions applies:

a. Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;

b. Authorizations to use or disclose psychotherapy notes may only be combined with another authorization related to psychotherapy notes; or

c. Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if the Agency has not conditioned the provision of treatment or payment upon obtaining the authorization.

Revocation of Authorization

1. The consumer may revoke his authorization at any time.

2. The authorization may ONLY be revoked in writing. If the consumer or the consumer's personal representative informs the Agency that he/she wants to revoke the authorization, the Agency will assist him/her to revoke in writing.

3. Upon receipt of a written revocation, the Privacy Officer will write the effective date of the revocation on the *Authorization* form.

4. Upon receipt of a written revocation, the Agency may no longer use or disclose a consumer's PHI pursuant to the authorization.

5. Each revocation will be filed in the consumer's Medical Record

CHECKLIST FOR VALID AUTHORIZATION

When you receive a request for release of Medical Records containing PHI from any entity other than the consumer or the consumer's personal representative, and the disclosure is not for purposes of treatment, payment or health care operations or another disclosure required or permitted by the HIPAA Privacy Rule, you may not release those records unless the requestor has provided a valid authorization. Use this checklist to assure that the authorization is valid. **If any one element is missing, the Privacy Rule prohibits you from disclosing the information.** You should contact the requestor and explain why you cannot disclose the information.

_____The authorization must be written in plain language.

All of the following elements must be included in the authorization:

_____A specific and meaningful description of the information to be disclosed.

_____The name or other specific identification of the person (or organization or class of persons) authorized to make the requested disclosure.

_____The name or other specific identification of the person (or organization or class of persons) to whom the information will be disclosed.

_____The purpose of the requested disclosure. (If the consumer initiates the authorization, the statement "at the request of the consumer" is a sufficient description of the purpose).

_____An expiration date or an expiration event that relates to the consumer or the purpose of the disclosure.

_____Signature of the consumer or personal representative and date.

_____If signed by personal representative, a description of the representative's authority to act for the consumer.

Required Statements:

_____A statement that information disclosed pursuant to the authorization may be subject to redisclosure and may no longer be protected by the Privacy Rule.

_____A statement of the consumer's right to revoke the authorization in writing and either,

_____A reference to the revocation right and procedures described in the Notice of Privacy Practices;

OR

_____A statement about the exceptions to the right to revoke and a description of how the consumer may revoke.

_____One of the following statements, or a substantially similar statement:

- If the Covered Entity is not permitted to condition treatment or payment on the provision of an authorization: I understand that the Agency will not condition the provision of treatment or payment on the provision of this authorization.

  OR

- If the Covered Entity is permitted to condition the provision of research-related treatment on the provision of an authorization: I understand that the Agency will not provide research-related treatment to me unless I provide this authorization.

  OR

- If the Covered Entity is permitted to condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization: I understand that the Agency will not provide health care that is solely for the purpose of creating PHI for disclosure to *a third party* to me unless I provide this authorization.

Defective Authorizations

If an authorization has any one of the following defects, it is invalid and any use or disclosure made pursuant to the authorization will be in violation of the Privacy Rule:

_____The authorization has expired.

_____One of the required elements or statements is missing.

_____The Agency has knowledge that the authorization has been revoked.

_____The authorization violates the regulations governing conditioning treatment or payment upon signing the authorization, or combining authorizations.

_____The Agency has knowledge that information in the authorization is false.

F. SAFEGUARDING AND STORING PHI

The policy of this Agency is to ensure, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal or state regulation governing confidentiality and privacy of health information. The following procedure is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is, or will be, contained in a consumer's Medical Record. At the same time, the Agency recognizes that easy access to all or part of a consumer's Medical Record by health care practitioners involved in a consumer's care (nurses, physical therapists, and others) is essential to ensure the efficient quality delivery of health care.

The Privacy Officer is responsible for the security of all Medical Records. All staff members are responsible for the security of the active Medical Records at the nursing stations.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by the Agency, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:

1. Specific types of meetings where PHI may be discussed include, but are not limited to:
    a. Daily Standup or Department Head meetings
    b. Interdisciplinary Plan of Care meeting
    c. Medicare meeting
    d. Bill review meetings
    e. Family Care Conference
2. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
3. Meetings will be conducted in a room with a door that closes, if possible.
4. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.
5. Only staff members who have a "need to know" the information will be present at the meeting.
6. The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

Telephone conversations:

1. Telephones used for discussing PHI are located in as private an area as possible.
2. Staff members will take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
    a. Lowering the voice
    b. Requesting that unauthorized persons step away from the telephone area
    c. Moving to a telephone in a more private area before continuing the conversation
3. PHI shared over the phone will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

In-Person conversations:

- In consumer rooms

- With consumer/family in public areas
- With authorized staff in public areas

Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:

1. Lowering the voice
2. Moving to a private area within the Agency
3. If in consumer room, pulling the privacy curtain

Safeguards for Written PHI

All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.

Active Records:

1. Active Medical Records shall be stored in an area that allows staff providing care to consumers to access the records quickly and easily as needed.
2. Authorized staff shall review the Medical Record at its storage location, unless it is signed out in accordance with Agency procedure.
3. Active Medical Records shall not be left unattended on the desks or other areas where consumers, visitors and unauthorized individuals could easily view the records.
4. Medication Administration Records, Treatment Administration Records, report sheets and other documents containing PHI shall not be left open and/or unattended.
5. Only authorized staff shall review the Medical Records. All authorized staff reviewing Medical Records shall do so in accordance with the minimum necessary standards.
6. Medical Records shall be protected from loss, damage and destruction.

Active Files:

Active Files shall be stored in a secure area that allows authorized staff access as needed.

Thinned Records, Inactive Medical Records:

1. Thinned and inactive Medical Records will be filed in a systematic manner in a location that ensures the privacy and security of the information. The Privacy Officer or a designee shall monitor storage and security of such Medical Records. When records are left unattended, records will be in a locked room, file cabinet or drawer.
2. The Privacy Officer will identify and document those staff members with keys to stored Medical Records. The minimum number of staff necessary to assure that records are secure yet accessible

shall have keys allowing access to stored Medical Records. Staff members with keys shall assure that the keys are not accessible to unauthorized individuals.

3. Inactive Medical Records must be signed out if removed from their designated storage area. Only authorized persons shall be allowed to sign out such records.
4. Records must be returned to storage promptly.
5. In the event that the confidentiality or security of PHI stored in an active or inactive Medical Record has been breached, the Agency Privacy Officer and Executive Director shall be notified immediately.
6. Agency procedure will be followed if Medical Records are missing.

Inactive Files:

Inactive Business Office Files shall be stored in a systematic manner in a location that ensures privacy and security of the information.

PHI Not a Part of an Official Record:

1. Use of "shadow" charts or files is discouraged.
2. Any documentation of PHI shall be stored in a location that ensures, to the extent possible, that such PHI is accessible only to authorized individuals.

Office Equipment Safeguards

Computer access:

1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
2. All users of computer equipment must have unique login and passwords.
3. Passwords shall be changed periodically.
4. Posting, sharing and any other disclosure of passwords and/or access codes is **strictly prohibited.**
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.
6. Agency staff members shall log off their workstation when leaving the work area.
7. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.
8. Employee access privileges will be removed promptly following their departure from employment.
9. Employees will immediately report any violations of this Policy to their supervisor, Executive Director or Agency Privacy Officer.

Printers, copiers and fax machines:

1. Printers will be located in areas not easily accessible to unauthorized persons.
2. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. Sample language: "Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc). Access to such documents by unauthorized persons is prohibited by federal law."
3. Documents containing PHI will be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.
4. Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

G. EMAILING PHI

1. E-mail users will be set up with a unique identity complete with unique password and file access controls.
2. E-mail users may not intercept, disclose or assist in intercepting and disclosing e-mail communications.
3. Resident specific information regarding highly sensitive health information must not be sent via e-mail, even within the internal email system (i.e. information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
4. Users will restrict their use of email for communicating normal business information such as information about general care and treatment of consumers, operational and administrative matters, such as billing.
5. Users should verify the accuracy of the email address before sending any PHI and, if possible, use email addresses loaded in the system address book.
6. PHI may be sent unprotected via e-mail within a properly secured, internal network of the organization. When sending PHI outside of this network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information. Sample security measures include password protecting the document(s) being sent or encrypting the message.
7. All e-mail containing PHI will contain a confidentiality statement (see sample below).
8. Users should exercise extreme caution when forwarding messages. Sensitive information, including consumer information, must not be forwarded to any party outside the organization without using the same security safeguards as specified above.
9. Users should periodically purge e-mail messages that are no longer needed for business purposes, per the organization's records retention policy.
10. Employee e-mail access privileges will be removed promptly following their departure from the organization.

11. Email messages, regardless of content, should not be considered secure and private. The amount of information in any email will be limited to the minimum necessary to meet the needs of the recipient.

12. Employees should immediately report any violations of this guideline to their supervisor, Executive Director or Agency Privacy Officer.

Sample Confidentiality Statement

The information contained in this e-mail is legally privileged and confidential information intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any viewing, dissemination, distribution, or copy of this e-mail message is strictly prohibited. If you have received and/or are viewing this e-mail in error, please immediately notify the sender by reply e-mail, and delete this e-mail from your system. Thank you.

H. FAXING PHI

1. The fax machine should be located in an area that is not easily accessible to unauthorized persons. Examples include the business office or medical record office. If possible, the fax machine should not be located in a public area where confidentiality of PHI might be compromised. If this is not possible, a sign should be posted regarding access to the documents.

2. Received documents will be removed promptly from the fax machine. To promote secure delivery, instructions on the cover page will be followed.

3. Steps should be taken to ensure that the fax transmission is sent to the appropriate destination. These include:

    a. Pre-programming and testing destination numbers whenever possible to eliminate errors in transmission due to misdialing.

    b. Asking frequent recipients to notify the Agency of a fax number change.

    c. Confirming the accuracy of the recipient's fax number before pressing the send/start key.

    d. If possible, printing a confirmation of each fax transmission.

4. A cover page should be attached to any facsimile document that includes PHI. (See a sample cover page following this Policy.) The cover page should include:

    a. Destination of the fax, including name, fax number and phone number;

    b. Name, fax number and phone number of the sender;

    c. Date;

    d. Number of pages transmitted; and

    e. Confidentiality Statement (See sample below).

5. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system should be checked to obtain incorrect recipient's fax number. Fax a letter to the receiver and ask that the material be returned or destroyed.

6. A written *Authorization* for any use or disclosure of PHI will be obtained when the use or disclosure is not for treatment, payment or healthcare operations or required by federal or state law or regulation.
7. The PHI disclosed will be the minimum necessary to meet the requestor's needs.
8. Highly sensitive health information should not be sent by fax in certain states (e.g., information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).

Sample Confidentiality Statement:

The documents accompanying this transmission contain confidential protected health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

SAMPLE
FAX COVER PAGE

Agency Name
Agency Address
Phone Number
Fax Number

Confidential and Protected Communication

FAX COVER SHEET

DATE & TIME _____NUMBER OF PAGES_____

TO: _____
NAME

_____ _____
FAX NUMBER PHONE NUMBER

FROM: _____

COMMENTS:

VERIFICATION OF RECEIPT OF FAX:

This communication may contain confidential Protected Health Information. This information is intended only for the use of the individual or entity to which it is addressed. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is STRICTLY PROHIBITED by Federal law. ***If you have received this information in error, please notify the sender immediately*** *and arrange for the return or destruction of these documents*

I. COMPLAINTS

Any concerned individual has the right to file a formal complaint concerning privacy issues without fear of reprisal. Such issues could include, but are not limited to, allegations that:

- PHI that was used/disclosed improperly;
- Access or amendment rights were wrongfully denied; or
- The Agency's *Notice of Privacy Practices* does not reflect current practices accurately.

Procedure

1. All consumers or their personal representatives will be notified of their right to complain to the Agency or the Department of Health and Human Services in the Agency's *Notice of Privacy Practices.*
2. All concerns may be registered by telephone, mail, or in person.
3. Upon receipt of a complaint about a Agency's privacy policies or its compliance with those policies or the law, the complaint will be recorded on a *"Complaint"* form.
4. The Agency Privacy Officer will review the *Complaint* form to ensure that the information is complete, and take the necessary steps to get complete information:
    a. Document the date, time, and name of the person making the complaint.
    b. Investigate the complaint.

c. Document the resolution of the complaint.

5. Once the *Complaint* form is completed correctly, the Agency Privacy Officer will review and investigate the complaint to determine if a violation of the law or Agency policies has occurred.

6. Following this review, the Agency Privacy Officer shall submit his or her findings to the Privacy Officer for final review.

7. The Privacy Officer shall determine the substance of the findings and will:

    a. Document the resolution of the complaint.

    b. Communicate the outcome of the complaint with the individual filing the complaint within 30 days from receipt of complaint.

8. The Privacy Officer shall maintain documentation of all complaints received and their disposition for a period of at least six years (from the date of creation) in accordance with federal regulations.

9. SCHRA shall refrain from intimidating, threatening, coercing, discriminating or retaliatory acts against employees who exercise their rights under the Act including:

    a. filing a complaint

    b. testifying

    c. assisting or participating in an investigation, compliance review, proceedings or hearing

    d. opposing any act or practice made unlawful by this resolution, provided the employee has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI.

J. DISCIPLINE

It is the policy of this Agency to discipline employees who fail to comply with the Agency's policies and procedures regarding HIPAA.

Procedure

1. When a concern arises regarding a possible violation of HIPAA or the Agency's policies or procedures related to HIPAA, the Agency Privacy Officer shall begin an investigation promptly. (See the Policy "Complaints" regarding conducting an investigation.)

2. If, at the conclusion of the investigation, it is found that a violation of the Agency's policy or procedure has occurred, the employee involved shall be disciplined in accordance with the severity of the violation and the Agency's disciplinary policy. Violations can be classified according to intent such as:

    a. Level I Violations are those made accidentally or due to a lack of education.

b. Level II Violations are serious violations that are found to show purposeful disregard of Agency policy.

3. The Agency Privacy Officer shall review the circumstances surrounding any substantiated violation and take appropriate action to mitigate, to the extent possible, any harmful effects of the violation.

4. Documentation from the investigation shall be maintained as a part of the Agency's HIPAA documentation and retained for six years.

5. The disciplinary action report documenting the employee's violation shall be placed in the employee's personnel file.

K. RETENTION OF PHI RECORDS

PHI will be retained according to state and federal regulations whichever requires retention for the longer period of time.

PHI, including medical and financial records will be retained for a minimum of six years as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

In absence of state law specifying a greater retention period, Medical Records must be retained for at least six years after the date it was last in effect.

For minor consumers (persons who have not reached full legal age), the Medical Record must be retained for three years after the minor reaches legal age under state law or six years from the date of discharge, whichever is longer.

Medical records on which there may be pending litigation may be exempt from scheduled destruction at the discretion of the Agency.

If state laws and regulations require a greater retention time period, the greater will be followed.

Procedure

1. The Agency will review state laws and regulations to determine Medical Record retention period and "legal age" (generally 18 in Tennessee, although there are exceptions)

2. If state laws or regulations require a different retention period, the greater retention period will be followed.

3. The Agency will store the records until the retention period has expired. Records must be stored in a secure manner. The records must be protected from unauthorized access and accidental/wrong destruction.

4. At the expiration of the retention period, the Medical Records will be destroyed. Records should be destroyed annually in accordance with the retention time frames.

PHI stored in paper, electronic or other format will be destroyed utilizing an acceptable method of destruction after the appropriate retention period has been met.

Access to PHI stored on computer equipment and media will be limited by taking the appropriate measures to destroy electronically stored PHI.

L. DESTRUCTION OF PHI RECORDS

Paper Documents:

1. PHI maintained in paper format will be destroyed at the end of the retention period.
2. All paper documents that contain PHI will be destroyed using an acceptable method of destruction.
3. Acceptable methods of destruction include shredding, incineration, pulverization and use of a bonded recycling company.
4. An *Inactive Medical Record Filing/Destruction Log ("Destruction Log")* must be maintained to identify the destroyed records. At a minimum, the *Destruction Log* must capture the information listed below.
    a. Date of destruction (date/s records are destroyed),
    b. Destroyed by (name/s of the individuals responsible for destroying the records),
    c. Witness (name/s of the person witnessing the destruction),
    d. Method of destruction (method used to destroy records), and
    e. Resident information (full name, Medical Record number, date of admission, date of discharge).
5. Prior to destruction of boxed items, the Agency will verify the retention period has expired.
6. If the records are destroyed off-site through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.
7. The Agency will maintain destruction documents permanently.

Computer Data Storage Media

1. Personal Computers: Workstations, laptops and servers use hard drives to store a wide variety of information. Residents' health information may be stored in a number of areas on a computer hard drive. For example, health information may be stored in "Folders" specifically designated for storage of this type of information, in temporary storage areas and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data.

    a. To ensure that any consumers' health information has been removed, a utility that overwrites the entire disk drive with "1"s and "0"s must be used.

    b. If the computer is being re-deployed internally or disposed of due to obsolescence, the aforementioned utility must be run against the computer's hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.

    c. If the computer is being disposed of due to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser. This applies to PC workstations, laptops and servers.

2. Backup or Data Tapes:

    a. Tapes are typically re-used many times but generally only by the data processing groups within the Agency, which routinely must handle consumer health information. However, there may be situations where tapes are sent to external recipients for specific processing. Tapes used for this purpose should be segregated from the general pool used for backups. These tapes should be degaussed prior to use in creating the files being sent to ensure that no prior consumer health information remains on that portion of the tape beyond the end of the current file.

    b. Tapes or diskettes that are being decommissioned must be degaussed before disposal. This can be accomplished using a bulk tape eraser. Alternatively, the media may be pulverized or shredded.

3. Compact Disks (CDs) and Diskettes: CDs containing consumer health information must be cut into pieces or pulverized before disposal.

4. If a service is used for disposal, the vendor should provide a certificate indicating the following:

    a. Computers and media that were decommissioned have been disposed of in accordance with environmental regulations as computers and media may contain hazardous materials.

    b. Data stored on the decommissioned computer and/or media was erased or destroyed per the previously stated method(s) prior to disposal.