HIPAA POLICY

PROTECTED HEALTH INFORMATION USES AND DISCLOSURES

POLICY: A Covered Entity (the Agency) or Business Associate may not use or disclose Protected Health Information (PHI) except as permitted or required under HIPAA regulation.

PURPOSE: To protect the privacy of an individual

PERSONNEL: All personnel

PROCEDURE:

A. A Covered Entity is permitted to use or disclose PHI:
   1. To the individual
   2. For treatment, payment or health care operations
   3. Incident to a use or disclosure otherwise permitted or required when the Covered Entity has complied with the applicable requirements with respect to use or disclosure
   4. Except prohibited uses or disclosures
   5. Pursuant to an agreement or as otherwise permitted
   6. As permitted by HIPAA regulations

B. Covered Entities are required to disclose PHI:
   1. To an individual when requested
   2. When required by the Secretary to investigate or determine the Covered Entity's compliance.

C. Business Associates may use/disclose PHI only as permitted or required by the business associate contract or arrangement. The Business Associate may not use or disclose PHI in any manner that would violate HIPAA regulations.

D. The Business Associate is required to disclose PHI:
   1. When required by the Secretary to investigate or determine the Business Associate's compliance
   2. To the Covered Entity, individual or individuals designee to satisfy the Covered Entity's obligations with respect to an individual's request for electronic copy of PHI.

E. A Covered Entity or Business Associate may not sell PHI (for direct or indirect remuneration from or on behalf of the recipient of the PHI) without authorization which states that remuneration will result. "Sale" excludes disclosure for public health purposes, research purposes, treatment or payment, sale, transfer, merger of the Covered Entity or for activities by the Business Associate on behalf of the Covered Entity, when requested by an individual or as required by law.

F. When using/disclosing PHI or requesting PHI from another Covered Entity/Business Associate, reasonable efforts to limit the PHI to the minimum necessary must be made. Minimum necessary does not include disclosures for treatment, disclosures made to the individual or under specific authorization or disclosure to the Secretary or made by law or those made in compliance with HIPAA regulation.

G. PHI that the Covered Entity has agreed to restrict may not be used/disclosed.

H. PHI may be used to create de-identified information only to a Business Associate for a specific purpose.

I. A Covered Entity may disclose PHI to a Business Associate and may allow the Business Associate to create, receive, maintain or transmit PHI on its behalf if the Business Associate assures it will be safeguarded. A Business Associate may disclose PHI to a business associate subcontractor upon obtaining the same assurances.

J. A personal representative of an individual must be treated as the individual:
    1. If under authority of law is acting on behalf of an adult or emancipated minor.
    2. If acting as parent, guardian or acting *in loco parentis* on behalf of an unemancipated minor unless the minor has authority to act as an individual.

K. A Covered Entity must treat an executor, administrator or other person acting under applicable law as the deceased individual or estate with respect to PHI relevant to the representation.

L. A Covered Entity may elect not to treat a person as the personal representative if there is reasonable belief that the individual has been or may be subjected to domestic violence, abuse or neglect by such person or could endanger the individual.

M. Disclosure by whistleblowers is not considered a violation if believed in good faith that the conduct is unlawful or violates professional or clinical standards, or that care endangers someone and the disclosure is made to a health oversight agency or public health authority authorized to investigate or made to an attorney retained by the whistleblower's behalf.

N. Disclosures by workforce members who are victims of a crime does not violate HIPAA requirements if disclosure is made to a law enforcement official and is limited in and is about the suspected perpetrator of the criminal act.

O. Uses and Disclosures for which an authorization or opportunity to agree or object is required.

P. A Covered Entity must obtain authorization for any use/disclosure of psychotherapy notes, except to carry out treatment, payment or operations, use by the originator, use in the Covered Entity's training programs, or to defend itself in legal action brought by the individual.

Q. A Covered Entity must obtain authorization for any use or disclosure of PHI for marketing except when in the form of face-to-face communication to the individual or promotional gift of nominal value.

R. Authorizations for release must be complete, current and accurate. Authorizations may not be combined except in limited circumstances and may not be conditioned on any provision to an individual of treatment, payment, enrollment or eligibility for benefits.

S. Any individual may revoke an authorization at any time and the revocation must be in writing.

T. A Covered Entity must document and retain any signed authorization and provide a copy to the individual. Authorization must be written in plain language and contain at least these core elements:
    1. Description of the information to be used/disclosed
    2. Name of person(s) authorized to make the use/disclosure
    3. Name of person(s) authorized to whom the use/disclosure may be made
    4. Description of the purpose for use/disclosure. (This may be "at the request of the individual" if the individual does not elect a statement of purpose.)
    5. An expiration date or expiration event
    6. Signature of the individual and date. If signed by a representative, then a description of the authority to act as the representative
    7. Statements including the following:
        a. Individuals right to revoke authorization
        b. Exceptions to the right to revoke
        c. Ability or inability to condition treatment, payment, enrollment or eligibility on the authorization
        d. The potential for information to be disclosed

Uses and Disclosures requiring an opportunity for the individual to agree or to object.

A. A Covered Entity may use/disclose PHI under the following if the individual has been informed in advance of the use/disclosure and given the opportunity to agree or prohibit or restrict the use/disclosure such as:
    1. Being listed in a facility directory using specific, generic information
    2. Disclosing information directly relevant to the care or payment of care to a family member, other relative or close personal friend, or any other person identified by the individual
    3. Based on the exercise of professional judgment that the individual does not object
    4. When the individual is not present, based on circumstances, incapacity and professional judgment
    5. To assist in disaster relief efforts

B. A Covered Entity may disclose to a family member or other persons identified who were involved in the individual's care or payment, if the individual is deceased, consistent with prior expressed preferences.

C. Uses and Disclosures for which authorization or opportunity to agree or object is not required.

D. When the Covered Entity is required to inform the individual of, or when the individual may agree to, a use/disclosure permitted by this section, the Covered Entity's information and the individual's agreement may be given orally.

E. A Covered Entity may use/disclose PHI upon meeting the requirements of the statute to the extent that such use/disclosure is:
    1. Required by law and the use/disclosure complies with and is limited to the relevant requirements of such law,
    2. For public health activities
    3. When the Covered Entity reasonably believes the individual to be a victim of abuse, neglect or domestic violence and releases to a government authority authorized by law to

receive such reports,
4. For health oversight activities,
5. In the course of any judicial or administrative proceeding,
6. For law enforcement purposes,
7. Use/disclosure about decedents to coroners, medical examiners, funeral homes,
8. Organ, eye or tissue donation,
9. Research purposes,
10. To avert serious threat to health or safety,
11. Specialized government functions, or
12. Workers' compensation

F. Other Requirements Related to Use/Disclosure of PHI

G. Health information that does not identify an individual and to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. De-identified information does not contain:
   1. Names
   2. Geographic subdivisions smaller than state (can contain the initial 3 digits of the zip code in some circumstances)
   3. All elements of dates except year directly related to an individual (SOC, discharge, death, age, etc.)
   4. Phone and fax numbers
   5. Email addresses
   6. Social security numbers
   7. Medical record numbers
   8. Health plan numbers
   9. Account numbers
   10. Certificates or license numbers
   11. Vehicle identifiers
   12. Device identifiers
   13. URLs, IP addresses
   14. Biometric identifiers
   15. Photographic images
   16. Any other unique identifier

H. A Covered Entity must limit any request for PHI to the minimum necessary for the purpose and must implement policies that limit those requests.

I. The Covered Entity may use/disclose without authorization any minimum necessary uses of PHI which identify the persons/classes of persons who need access to PHI to carry out their duties and the category(ies) of PHI to which access is needed and any conditions appropriate to such access. A Covered Entity must make reasonable efforts to limit the access to those identified.

J. Minimum necessary disclosures of PHI, made on a routine or recurring basis, must limit the PHI disclosed to the amount reasonably necessary to achieve the purpose. A Covered Entity must develop criteria designed to limit PHI disclosure and review all requests using this criteria. Reasonable may be determined when:
    1. A public official represents that the information requested is minimum necessary,
    2. Another covered entity makes the request,
    3. Information is requested by a professional member of the workforce or is a Business Associate providing professional services to the Covered Entity, or
    4. Documentation complies with the regulations for a person requesting the information for research purposes.

K. A Covered Entity may not use, disclose or request an entire medical record, except when this is justified to meet the minimum necessary purpose.

L. A Limited Data Set (LDS), which excludes the following direct identifiers, may be used/disclosed under a data use agreement with the limited data set recipient for purposes of research, public health or health care operations:
    1. Names
    2. Postal address other than town/city, state and zip
    3. Telephone & fax numbers
    4. Email addresses
    5. Social security, medical record, health plan beneficiary, account, certificate/license numbers
    6. Vehicle or device identifiers
    7. URLs or IP addresses
    8. Biometric identifiers
    9. Full face photographic images

M. Data Use Agreements require that the LDS will only be used for limited purposes and:
    1. Must establish permitted uses/disclosures by the recipient
    2. May not authorize further uses/disclosures in a manner that would violate the regulations
    3. Establish who is permitted to use, receive LDS
    4. Provides that recipient will:
        a. Not use/disclosure further other than permitted by agreement or law
        b. Use appropriate safeguards to prevent uses/disclosures other than provided by the agreement
        c. Report to the Covered Entity any uses/disclosures of which it becomes aware
        d. Ensure that agents provided the LDS agree to same restrictions and conditions
        e. Not identify the information or contact the individuals

N. Covered Entity is not in compliance with the LDS if:
    1. They knew of material breach or violation of Data Use Agreement unless the Covered Entity had taken steps to cure breach or end violation and
    2. If steps were unsuccessful, the Covered Entity discontinues the disclosure to recipient and reports the problem to the Secretary.

O. The Covered Entity may use/disclose the following to the Business Associate or institutionally related foundation for the purpose of raising funds without authorizations:
    1. Demographic information (name, address, contact information, age, gender, date of birth),
    2. Dates health care was provided,
    3. Department of service information,
    4. Treating physician,
    5. Outcome information, or
    6. Health insurance status

P. The Covered Entity may not use/disclose PHI for fundraising for other purposes unless a statement is included in the Notice of Privacy Practice. The Covered Entity, with every fundraising communication, must provide the opportunity for the individual to elect not to receive further fundraising communications and may not condition treatment or payment on the individual's choice. The Covered Entity may not make fundraising communications if the individual has elected out but may provide an opt back in method.

Q. Prior to disclosure, a Covered Entity must:
    1. Verify identity of the person requesting PHI and the authority of the person to have access.
    2. Obtain documentation, statements or representations, oral or written, when required.

        a. An individual has the right to adequate notices (the Notice of Privacy Practices) of uses/disclosures of PHI that may be made by the Covered Entity and the Covered Entity's legal duties to protect that PHI. The notice must be made available upon request and no later than the date of the first service delivery for treatment, payment or, in an emergency, as soon as practicable after. The Covered Entity must maintain written acknowledgment of the receipt or its documented efforts.

R. If the Covered Entity maintains a website of services or benefits, the notice must be posted on the website and available electronically through the website. It can be provided via email if the individual agrees.

S. The Covered Entity must document compliance with the notice requirements, retain a copy of what was issued and, if applicable, any written acknowledgment of receipt.

T. The individual may request restricted use/disclosure of PHI, but the Covered Entity is not required to agree to any restriction. However, if the Covered Entity does agree to a restriction, the information may not be used/disclosed.

U. If the individual requests restriction of PHI to a health care plan pertaining solely to an item or service for which the individual paid the Covered Entity in full, the Covered Entity must agree.

V. A Covered Entity may terminate a restriction if:
    1. The individual agrees in writing or orally if documented.
    2. The restriction is not related to a required use/disclosure restriction.
    3. The termination is effective for PHI created or received after the notice of termination.

W. A Covered Entity must permit and accommodate reasonable requests from an individual to receive PHI information by alternative means or at alternative locations.

X. A request for confidential information (PHI) must be made in writing and may be conditioned upon receipt of payment, if applicable. The individual does not have to explain the basis of the request.

Y. An individual may not have access to nor obtain psychotherapy notes, information compiled for civil, criminal or administrative action or proceeding or information prohibited by law.

Z. The Covered Entity may, dependent upon the content and intent of the PHI, deny or temporarily restrict the individual's access. All requests will be reviewed by the Administrative Director for applicability. (See HIPAA §164.524) If a review of a denial to provide PHI is requested, the Privacy Officer will make a final determination.

AA. The Covered Entity will maintain documentation of designated record sets subject to access and the titles of the person(s) responsible for receiving and processing requests for access.

BB. An individual has the right to request an amendment to PHI or record within a designated record set unless the information was not created by the Covered Entity or is not part of the designated record set or it is determined that the information is accurate and complete. A request must be in writing and provide a reason to support the amendment. The Covered Entity must act within 60 days of the request and must make the approved amendment and identify records in the designated record set that are affected. If the amendment is denied, the Covered Entity must

provide a written denial including the basis for the denial and explain the individual's right regarding disagreement. The request for amendment and the written denial and/or dispute may be included with future use/disclosure if requested. Any disputed PHI must be identified and linked to the applicable documentation.

CC. The Covered Entity must make reasonable efforts to identify and notify those who would need the amended record. The Covered Entity must amend PHI when notified of by another Covered Entity of an amendment.

DD. An individual has the right to a written accounting of use/disclosure by the Covered Entity no more than six years prior to a request for accounting. The Covered Entity must act on the request no later than 60 days after the receipt of the request. The accounting is without charge initially for a 12-month period. Multiple requests within the same 12-month period may incur a cost-based fee if the individual is notified in advance of the charge. The Covered Entity must document the accounting in writing and meet the documentation requirements of the regulations.

EE. The Covered Entity must designate a privacy official responsible for implementing policies and a contact person/office responsible for receiving complaints and providing information.

FF. The Covered Entity must train all members of its workforce to the policies and procedures with respect to PHI as necessary and appropriate and must document the training.

GG. The Covered Entity must have appropriate safeguards in place to protect PHI.

HH. The Covered Entity must provide a process for complaints to be made regarding the policies and procedures related to PHI use/disclosure. Any complaint must be documented along with any disposition.

II. The Covered Entity is required to have in place, and to implement appropriate sanctions/disciplinary action against members of its workforce who fail to comply with the privacy policies and procedures of the Agency. The Covered Entity will document any sanctions applied. A Covered Entity must mitigate, to the extent practicable, any harmful effect known of a violation of the use/disclosure of PHI.

JJ. The Covered Entity may not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for filing a complaint or exercising any right related to the use/disclosure of PHI.

INTERNET AND ELECTRONIC MAIL USAGE

POLICY: The Agency will provide internet access and electronic mail (email) as a business tool to facilitate communications and the exchange of information to perform job functions. Users have an obligation to use the internet and email appropriately, effectively and efficiently.

PURPOSE: To define appropriate standards for secure, effective use of the company internet and email system.

PERSONNEL: All users of company email including employees, contractors, students and volunteers

PROCEDURE:

1. Employees may use the internet and email provided by the Agency for:
    a. Work-related purposes
    b. Sending and receiving email messages

2. Electronic accounts and passwords will not be shared or revealed to anyone else besides other authorized user(s).

3. Email/Internet Usage is to be in compliance with all applicable state and federal laws and regulations. Prohibited use of company internet/email includes but is not limited to:
    a. Copying/transmitting any document, software or other information protected by copyright and/or patent law, without proper authorization of owner;
    b. Downloading software or media files not completed by or authorized in writing by the Administrator or designee;
    c. Personal commercial use or mass distribution of non-agency information;
    d. Using the agency distribution lists for non-agency purposes;
    e. Transmission of highly confidential or sensitive information, e.g., discussion of HIV status, mental illness, chemical dependency, workers compensation claims or unsecured/unauthorized individual personal information and/or Protected Health Information (PHI) over any public or unsecured network;
    f. Any communication that is threatening, defamatory, obscene, offensive or harassing containing:
        1. Derogatory racial, national origin, or religious comments
        2. Sexual content
        3. Offensive language
        4. Content prohibited by local law or regulations
        5. Defamation or derogatory/abusive attacks on any individual groups or organizations
        6. Any material which would negatively reflect on this Agency.
    g. Knowingly causing interference with or disruption to any network, service or equipment or any user thereof;
    h. Attachments of confidential database files;
    i. Marketing purposes without explicit permission from the target recipient;
    j. Transmission of information to individuals without a legitimate business need for the information.

k. Contents of legal counsel without express authorization of counsel;
l. Misrepresenting, obscuring, suppressing or replacing a user's identity;
m. Attempting unauthorized access to data or attempting to breach any security measure on the system(s) or attempting to intercept transmissions without proper authorization.

4. The employee indemnifies the Agency for any direct loss or consequential loss suffered by the employee's breach of this policy. Users of the internet/email system who are found to be in violation of any part of this policy are subject to disciplinary action up to and including termination.

5. Users of the electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore, users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents. Internet/email communication systems are not secure; mail sent via the Internet or other external systems can be intercepted and read by individuals other than the intended recipient.

6. Intranet usage is intended to offer a more secure transmission. Information which is prohibited with internet transmissions may be more secure sent via intranet; however, certain precautions and requirements (HIPAA) must be met prior to individual personal information and/or Protected Health Information being transmitted:
   a. The transmission must be indicated as "Private" to demonstrate due diligence in protecting the patient's privacy;
   b. Personally confirm the email address of the recipient;
   c. Receipt must not be accessible to those not authorized to view PHI;
   d. Transmit only requested/authorized information.

7. The Agency recognizes that users may have reasonable expectations of privacy regarding electronic messages received and/or stored on the Agency's information system; however, use of internet/email is a business process. All messages originated or transported within or received into the company's system is considered the property of the company. The Agency reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property.

Generally, email messages constitute temporary communications, non-vital and discarded routinely; however, dependent upon the content of the message, it could be considered a more formal record and should be retained. Information stored electronically is subject to the legal discovery process and can be subpoenaed.

RELEASE OF CLINICAL RECORDS INFORMATION

POLICY: The Agency may not use or disclose protected health information under Federal law without appropriate authorization(s). Information disclosed may contain information that is protected by federal and state law.

PURPOSE: To protect the patient's right to confidentiality.

PERSONNEL: Specifically designated personnel are primarily responsible for responding to requests for written information from medical records. The final decision for releasing information in questionable cases is made by the Administrative Director, Clinical Manager/Agency Director (Supervising Nurse), legal counsel for the Agency, and/or designated personnel.

DEFINITIONS:

Court Order: Order issued directly by the court for release of information.

Docket Number: Court registration number appearing on subpoena duces tecum must be present before subpoena is considered valid. If no number is on the subpoena, a number can be obtained by calling the court clerk.

Emancipated Minor: A decree of emancipation is entered by the Juvenile court when a minor has reached 16 years of age or when married. Emancipated minors may sign for release of their clinical record.

Electronic Media: Electronic storage material on which data is or may be recorded electronically, transmission media used to exchange information already in electronic storage media (internet, dial-up, etc.)

Guardian:

A. ***Estate Guardianship:*** One appointed by the court to take care of the financial affairs only of an individual.

B. ***Full Guardianship:*** One appointed by the court to take care of all affairs of an individual.
   1. A full guardian appointed by the court has rights identical to the patient's rights in regard to release of information.
   2. If a legal guardian has been appointed by a court, a certified copy of the Guardianship Paper must be obtained and filed in the patient's clinical record.

C. ***Guardian Ad Litem:*** A court-appointed legal guardian, usually on a temporary basis, while a competency suit is in process.

Limited Data Set: Health information that excludes certain, listed direct identifiers such as names, postal address information, telephone/fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers and account numbers of the individual or of relatives, employers, or household members of the individual.

Minimum Necessary: Under HIPAA, the minimum necessary standard requires covered entities to make all "reasonable" efforts to limit the PHI to accomplish the purpose of the disclosure

Power of Attorney: Legal instrument authorizing one to act as the attorney or agent of the grantor.

A. A copy of this statement authorizing one to act as the agent of another must be obtained and filed in the patient's clinical record.
B. The person authorized to act as agent of the grantor shall not have the right to release confidential information from said grantor's clinical record unless the "Power Of Attorney Statement" specifies this privilege.
C. Durable Power of Attorney for patients who are legally competent must be considered valid.
D. Upon expiration of the patient, any Power of Attorney granted by the patient must be considered to be revoked.

Public Health Authority*:* An agency or authority of the US, state, a territory, a political subdivision of a state or territory, or Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including employees or agency of such public agency or its contractors or person or entities to whom it has granted authority, that is responsible for public health matters as part of its office mandate

Subpoena: An order issued by a court, administrative commission, court reporter, notary public or attorney which commands a witness to appear at a trial or other proceedings to give testimony and in certain circumstances, to provide documents.

A. ***Deposition Subpoena:*** Subpoena used to compel the attendance of a witness at a deposition, usually to be taken in an attorney's or court reporter's office. This subpoena is used for pretrial discovery.
B. ***Notary Subpoena:*** A subpoena notarized by a notary public as opposed to one issued by a court of law. The record is taken to the attorney's office or office of the court reporter instead of to a court.
C. ***Subpoena Duces Tecum:*** A subpoena which, in addition to requiring the attendance of a witness, requires him/her to bring to court the records described in the subpoena and allow review/reproduction of the records.

Third Party Payers: Insurance companies, federal, state and other governmental or private entities responsible for paying a patient's bill.

PROCEDURE:

A. The Agency must maintain a written or electronic record of the patient's clinical treatment (designated record set). Any authorized release of any clinical record must be directed to the Privacy Officer or Corporate Compliance Officer.

B. Non-Confidential Information - "Non-privileged" information can be released under certain circumstances without requiring the patient's written authorization. Certain identification data obtained on admission is considered "non-privileged," which means that this data may be given without violating the patient's right to privacy or the patient/physician privilege. However, even this information should be given out with caution. The "need to know" should always be considered.
    1. Name of patient

2. City of current residence
3. Dates of admission and discharge

C. Confidential information - All other information not listed above.

D. Students enrolled in an educational program may be authorized by the Administrative Director or Clinical Manager/Agency Director (Supervising Nurse) to have access to clinical records. Students will be supervised by an instructor in his/her program and will treat all information in clinical records as confidential.

E. The Agency is permitted to use/disclose information as follows:
   1. To the patient
   2. For treatment, payment or health care operations
   3. As required by law once the Agency has complied with applicable requirements, with a valid authorization.

F. Release of Clinical Records to the Individual - The Agency recognizes that a patient may request that a copy of the clinical record be released. The following are guidelines for such requests:
   1. A patient's clinical record (whether hard copy or electronic form) must be made available to a patient, free of charge, upon request at the next home visit, or within 4 business days (whichever comes first).
   2. The Agency employee/contractor who receives the request from the patient shall document which records are being requested. This information must be communicated to the Agency Director or designated personnel in a timely manner to comply with the release of clinical records regulation.
   3. The Agency shall document what records were released to the patient and date they were delivered. This documentation shall be maintained in the patient's clinical record.

G. Release of Clinical Records to Other Entities - The patient or legal guardian may consent to the release of the patient's clinical record to someone else. The Agency must release the patient's clinical record if the following is completed:
   1. The consent must be in writing.
   2. The written consent must be signed and dated by the patient or guardian.
   3. A patient's consent for the release of the clinical record to another person will specify the provider making the disclosure, the name of the patient, the extent of the information being disclosed and that the consent is subject to revocation at any time on or before the expiration date, and clearly identify the designated recipient and where to send the copy.

H. A copy of the patient's consent must be included in the patient's clinical record.

I. When a decision to release a record has been made, the patient's clinical record will be reviewed by the Administrative Director, Clinical Manager/Agency Director (Supervising Nurse), or designated personnel.

J. The Agency may deny, in part or in whole, access to information. If the Agency denies, the Agency must provide a timely, written denial to the individual in plain language which contains:
   1. The basis for the denial;
   2. A statement, if applicable, for the individual's right to review the record and how to exercise review rights;

3. A description of how a complaint may be submitted to the Agency or to the Secretary, including the name, title, phone number of the designated person.

K. If the Agency does not maintain the requested information, the Agency must inform the individual where to direct the request, if the Agency knows.

L. The individual may request a review of any denial to access.

M. The individual has the right to have the Agency amend PHI maintained in the designated record set. The Agency may deny an amendment request if:
   1. The information was not created by the Agency.
   2. The information is not part of the designated record set maintained by the Agency.
   3. The information would not be available for inspection by law.
   4. The information is accurate and complete.

N. The Agency requires a request for amendment to be in writing and a reason provided for the requested amendment. The Agency must stipulate this requirement in advance. The Agency has 60 days to act on the request. The Agency may take the following actions:
   1. Grant the amendment
   2. Deny the amendment, in whole or in part, and provides a written denial
   3. Take an extension of no more than 30 days if the Agency provides the individual with a written statement of the reasons for the delay and the date the action will be completed.

O. If the Agency grants the amendment, in whole or in part, the Agency must make the appropriate amendment, identify the records in the designated record set affected by the amendment and append or link to the amendment. The Agency must inform the individual in a timely manner that the amendment was accepted, and obtain from the individual identification and agreement of relevant persons with which the amendment needs to be shared. The Agency must make reasonable efforts to inform and provide the amendment to those identified or those having relied upon, the information that must be amended.

P. If the Agency denies the request for amendment, the Agency must provide a written denial in a timely manner, in plain language containing the basis of the denial, individual's right to submit a written statement of disagreement and information on how the individual may file such a statement.

Q. The individual may request for any denial that a copy of the statement of disagreement and the denial be provided with any future disclosures. The Agency must include material appended in future disclosures if a statement of disagreement has been appropriately filed or the individual requests such.

R. The Agency must amend PHI whenever another Covered Entity informs the Agency of amendments to a designated record set.

S. Court Orders/Subpoenas - The Agency may release information from the clinical record without prior authorization if the Administrative Director or the Clinical Manager/Agency Director (Supervising Nurse) is served with a valid subpoena. It shall be the policy of the Administrative Director, Clinical Manager/Agency Director (Supervising Nurse), or designated personnel to verify

the legality of the subpoena issued.

1. The following are requirements for a valid subpoena:
    a. The Subpoena technically must be served to the person to whom it is addressed in order to be valid. However, if the subpoena is issued in the name of a corporation, it is then sufficient to serve an agent of the corporation such as the record custodian.
    b. Subpoenas may be issued by a clerk of the court, an administrative office of a designated commission or by the attorney of record on an individual case. A subpoena from courts outside the State, under certain circumstances, is enforceable. The agency attorney may give guidance.
    c. The date, time and place of appearance must be stated on the subpoena.
    d. The docket number should be evident. If it is not, the court clerk can be called for the number.
    e. The subpoena must include the name of the case indicating plaintiff and defendant including on whose behalf the subpoena is issued.
    f. The items being subpoenaed must be named. This includes specification of the exact clinical record wanted according to admission or discharge date.
2. If any questions exist about the validity of the subpoena, the Administrative Director or the Clinical Manager/Agency Director (Supervising Nurse) should consult with the agency's legal counsel. In cases of litigation involving the Agency, the Administrative Director or the Clinical Manager/Agency Director (Supervising Nurse) should notify the person he/she reports to and the agency's legal counsel.
3. Courts and administrative agencies have authority to require the following of Agency personnel:
    a. Be present at trials, hearings and depositions.
    b. Give testimony concerning records.
    c. Bring the patient's clinical record and allow review/reproduction of the record.
4. When receiving subpoenas:
    a. Prior to releasing records, identify the type of subpoena to determine if additional legal processes are needed. Subpoena duces tecum is required for a person to both appear at the court and to bring the patient's clinical record.
    b. Check the subpoena for additional documents (i.e. court order).
    c. Consult with the agency's legal counsel, if needed.
    d. Document in patient's clinical medical record notification of the attending physician regarding the subpoena.
    e. Read through the clinical record verifying for completion including signature and title of discipline(s). Each page must include the patient's name.
    f. Submit copies unless otherwise requested. When originals are requested, ask if copies would suffice. Inform the person serving the subpoena that he/she will be expected to incur the cost of the copying.
    g. Contact the appropriate attorney requesting the clinical record and set up time with him/her just prior to the court appearance.
    h. Under no circumstances will a clinical record be left in the custody of an attorney or a court. A special court order is needed for this; courts rarely request this.
5. General guidelines regarding subpoenas:
    a. Subpoenas for producing documentary evidence should be signed by the clerk of the court and bear the official court seal.
    b. Subpoenas issued by an administrative agency of the State must be signed by the Agency in order to be valid. The agency personnel named should be personally

handed a copy of the subpoena and paid a fee for court attendance and mileage. Subpoena must be honored or penalties for contempt of court may result. The subpoena must specify which documents are needed by the court.

c. Time can be saved when receiving a subpoena if the Administrative Director or the Clinical Manager/Agency Director (Supervising Nurse):
    1. Contacts the attorney issuing the document and discusses its purpose.
    2. Makes arrangements with the attorney issuing the subpoena regarding the time to meet with the attorney just prior to the court appearance.
    3. Determines whether copies will be satisfactory.
    4. Determines how many copies may be required.

T. The first accounting in any 12-month period is without charge to the patient. A fee may be charged to a patient for his own healthcare information for subsequent requests within the 12-month period if notified in advance and if given an opportunity to withdraw or modify the request to avoid or reduce the fee. Cost- based fees include:
    1. Labor for copying
    2. Supplies for creating the copy
    3. Postage, if the copies are requested to be mailed
    4. Preparation, if agreed by the individual.

U. Photocopying Fees - As a rule third party insurance carriers are not charged a fee for photocopying of material from the clinical record; however, attorneys, courts and others requesting information may be charged a fee for photocopying. The fees for photocopying materials are as follows:

V. Basic retrieval fee for first 10 pages may not exceed $30.00 (thirty dollars).

W. Charge of $1.00 per page for the 11th through 60th page.

X. Fifty cents per page for the 61st through 400th page.

Y. Twenty-five cents for any remaining pages.

Z. Add actual cost of mailing or shipping.

AA. There will be a mileage fee to be paid per established agency
    a. mileage reimbursement for any records that are to be delivered in person.

BB. Record of Materials Released - The Agency will keep an account in the patient's clinical record and in an Agency Log of clinical records released for six years. If requested by the individual, the Agency must provide an accounting of disclosures of PHI. The accounting must include:
    1. Date of disclosure
    2. Name of entity or person who received the PHI, and if known, the address of the entity or person
    3. Brief description of the PHI disclosed
    4. Brief statement of purpose of the disclosure, or a copy of the written request
    5. If multiple disclosures were made for a single purpose, the frequency, periodicity or number of disclosures made and the date of the last disclosure
    6. If the disclosure was made for specific research purposes of 50 or more individuals, then the name of the protocol, purpose and criteria for selecting records, brief description of type of PHI disclosed, date or time
        a. period, name, address and phone of research sponsor and a statement concerning the possible disclosure. The Agency may assist in contacting the research entity if requested.

Medical Document Release During Emergency

A. During an emergency, the Agency shall comply to State and federal medical records regulations as well as HIPAA and agency policies and procedures. All records will be secure and readily available to support continuity of care during an emergency.

B. Release of PHI to a Public Health Authority: A covered entity may release protected health information to a public health authority (PHA) for the purpose of preventing or controlling disease, injury, or disability for purposes of emergency preparedness as stated in 45 CFR 164.512(b)(1)(i). The disclosure is subject to minimum necessary information.

C. Release of PHI to Other Recipients:
   1. Agencies who seek information for public health purposes: may disclose PHI for treatment and public health information if:
      a. The Agency and agency (source of the information) has a data use agreement with the recipient of the information as stated in 45 CFR 164.514(e), and
      b. The Agency and agency disclose only a limited data set.
   2. Health Care Provider that uses or discloses information for treatment purposes: The Agency and agency may disclose minimum necessary PHI for treatment purposes.
   3. Another person or agency that would use or disclose information for treatment or certain health care operations: The Agency and agency may disclose minimum necessary PHI.

CONFIDENTIALITY

POLICY: The Agency shall preserve the confidentiality of its data/information and the privacy/confidentiality of its patients, personnel and Business Associates.

PURPOSE: To maintain the confidentiality of patient information and to comply with state and federal Breach Notification laws and regulations

PERSONNEL:
I. All personnel and volunteers of the Agency
II. Business Associates

DEFINITIONS:
Specific to Breach
Breach - means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purposes of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at 45 CFR Section 164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate (as applicable) demonstrates that there is a low probability that the PHI has been compromised or an exception applies.

Business Associate (BA) - an entity (or a subcontractor entity) that creates, receives, maintains and/or transmits PHI on behalf of a Covered Entity and requires routine access to PHI as defined under HIPAA Privacy Rule, HITECH Act and Breach Notification Rule; directly liable for failure to comply.

Electronic Media – electronic storage material on which data is or may be recorded electronically, transmission media used to exchange information already in electronic storage media (internet, dial-up, etc.)

Unsecured PHI - PHI that is "not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.

Work force - refers to employees, volunteers, trainees and other persons whose conduct, in the performance of work for a CE, is under the direct control of such entity, whether or not they are paid by the CE.

PROCEDURE:

A. Observance of patient information confidentiality policies and procedures is a condition of employment and failure to comply will result in disciplinary action up to, and including, termination and civil or criminal legal action.

B. Written consent of the patient, patient representative, court appointed guardian or a court order shall be presented as authority for release of medical information.

C. All clinical and non-clinical notes, written and electronic, completed by field staff should be submitted on a daily basis. Confidential materials carried in vehicles for use by staff should be safeguarded. Removal of the confidential materials should be performed daily. In the case of vehicular failure or accident, the confidential materials should be removed and safeguarded if at all possible.

D. When possible, only the documents required for patient care of a particular patient should be carried into the patient's house. Documentation for other patients should be left in a folder, notebook, file box, or maintained in a password protected electronic form. These shall be kept in the employee's locked vehicle during patient visits or otherwise safeguarded.

E. Notes, written and electronic, from contractors or Caregivers should be secured by the Caregivers until submitted.

F. All paper patient medical records in the Agency should be secured in file cabinets or closed rolling bins after office hours. Electronic records will be password protected. The clinical record, its contents, and the information contained therein must be safeguarded against loss or unauthorized use.

G. Personnel providing direct patient care or functioning in a supervisory position may keep a current, pertinent copy of patient information for their use as long as all patient-specific documentation is safeguarded from breaches of confidentiality. All documents related to specific patients must be returned to the Agency when the employee no longer requires the use of them for patient care.

H. Conversation regarding patients outside the Agency shall be confined to those persons with a need to know and be conducted in a non-public place.

I. Patient information obtained by personnel during agency employment and used for the benefit of either the employee outside of employment or another health care entity is strictly forbidden and will be considered a breach of confidentiality. Employees or former employees violating this policy will be reported to the appropriate licensing body.

J. Access to patient information via computer will be password-protected and limited to those with a need to know. Employees, vendors and volunteers with access to PHI will comply with Agency policies on confidentiality.

K. Vendors will be required to sign a statement of confidentiality to protect confidential business, patient, and personnel information. Failure to do so may result in termination of the vendor.

L. Sensitive data regarding patients (i.e. psychiatric patients and patients who are HIV+) is kept separate from other charts to further limit access.

M. The exception to the confidentiality rule is the "Tarasoff Warning." The Tarasoff Warning requires the psychiatrically trained professional to warn third parties when it is known that the patient poses a danger of imminent physical harm to those third parties.

N. If the patient is a minor and not in state custody and the patient poses a danger of imminent physical harm to others/self, the parent(s) must be notified.

O. Field staff must complete their clinical notes on agency supplied forms or an agency provided point of care mobile computer, and additionally comply with the following requirements:
    1. Clinical note information will be entered and saved on Agency supplied, agency approved paper forms, or Agency supplied mobile computers. The use of any non-agency approved paper forms or non-agency technological devices is prohibited.
    2. Users will secure clinical documentation that contains confidential information in a secure area (desk, cabinet, room, etc.)
    3. All printed notes not submitted as part of the medical record will be destroyed.
    4. Upon termination, the employee will furnish all tangible, confidential information prepared based on the case notes and not retain any copies, extracts or other reproductions in whole or in part.
    5. Under no circumstance will the employee willingly allow the PHI to be viewed, on paper or electronically, by persons who are non-employees of the Agency.

P. During the initial assessment/admission, the agency must inform the patient/client about the agency's *Notice of Privacy Practice* and explain patient rights with respect to the Health Insurance Portability and Accountability Act (HIPAA). The notice is included in written patient education. These rights are the right to:
    1. Notice of privacy practices for protected health information.
    2. Request restriction of use and disclosure
    3. Receive confidential communications
    4. Access information
    5. Amend information
    6. Accounting disclosures

Q. The agency will limit access of PHI to the minimum information necessary for the recipient's legitimate need and/or purpose.

R. A privacy policy notice will be posted in a prominent location within each agency (reception area). The Agency will have copies available upon individual request.

S. The agency will retain copies of its notice for a period of at least six (6) years from the date of publication or its last effective date, whichever is later.

BREACH NOTIFICATION

POLICY: This Agency will provide breach notification when unauthorized access, acquisition, uses and/or disclosure of the organization's patient protected health information occurs.

PURPOSE: To provide guidance for breach notification when unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs.

To adhere to Federal and State laws and regulations governing breach notification of protected health information.

PERSONNEL:

I. All personnel and volunteers of the Agency

II. Business Associates

DEFINITIONS:

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

Breach – Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purposes of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at 45 CFR Section 164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate (as applicable) demonstrates that there is a low probability that the PHI has been compromised or an exception applies.

Breach excludes –

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate – an entity (or a subcontractor entity) that creates, receives, maintains and/or transmits PHI on behalf of a Covered Entity and requires routine access to PHI as defined under HIPAA Privacy Rule, HITECH Act and Breach Notification Rule; directly liable for failure to comply.

Covered Entity – means a health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

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

Electronic Media – electronic storage material on which data is or may be recorded electronically, transmission media used to exchange information already in electronic storage media (internet, dial-up, etc.)

Individually Identifiable Health Information – means:

A. That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse;
B. Relates to the past, present, or future physical or mental health or condition of an individual;
C. The provision of health care to an individual or the past, present, or future payment for the provision of health care to an individual; and
D. Identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official – Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of the law.

Organization – For the purposes of this policy, the term "organization" shall mean the Covered Entity to which the policy and breach notification apply.

Protected Health Information ("PHI") – Protected health information means individually identifiable health information that is:

A. Transmitted by electronic media,
B. Maintained in electronic media, or
C. Transmitted or maintained in any other form or medium.

Unsecured Protected Health Information – Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in guidance that is to be issued annually on the HHS website, as is required by section 13402(h)(2) of Pub. L. 111-5.

Workforce –employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity.

PROCEDURE:

A. Discovery of breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization's Business Associates). The organization shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (Business Associate) of the organization.

    1. Following the discovery of a potential breach, the organization shall begin an investigation, conduct risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been accessed, acquired, used, or disclosed as a result of the breach. The organization shall also begin the process of determining what external notifications are required or should be made.

    2. Breach Investigation: The Agency's privacy officer or other designated investigating representative will act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate. The investigator shall be the key facilitator for all breach notification processes to the appropriate entities. All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

B. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not quality as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach

notification requirements, the organization will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

C. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the Business Associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of the delay.

D. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time or period specified by the official, or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

E. Content of the Notice: The notice shall be written in plain language and must contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

F. Methods of Notification: The method of notification will depend on the individuals or entities to be notified. The following methods must be utilized accordingly:
    1. Notice to Individuals: Notice shall be provided promptly and in the following form:
        a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. Notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first- class mail to the next of kin or personal representative shall be carried out.
        b. Substitute Notice: In the case where there is insufficient or out of date contact information that prevents direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out of date contact information that prevents written notification to the next of kin or personal representative.
            1. In a case in which there is insufficient or out of date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
            2. In the case in which there is insufficient or out of date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
        c. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.
    2. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 individuals. The notice shall be provided in the form of a press release.
    3. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS internet website a list of identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 individuals is accessed, acquired, used, or disclosed.
        a. If a breach affects 500 or more individuals, a Covered Entity must provide the

Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by following the link https://www.hhs.gov/ocr/complaints/index.html and completing all information. If a covered entity that has submitted a breach notification form to the Secretary discovers additional information to report, the covered entity may submit an additional form, checking the appropriate box to signal that it is an updated submission. If, at the time of submission of the form, it is unclear how many individuals are affected by a breach, covered entity must provide an estimate of the number of individuals affected. As this information becomes available, an additional breach report may be submitted as an addendum to the initial report.

b. For breaches that affect fewer than 500 individuals, a Covered Entity must provide the Secretary with notice annually. All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by following the link https://www.hhs.gov/ocr/complaints/index.html and contain all required information.

G. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be logged for each breach:

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known;
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.);
3. A description of the action taken with regard to notification of individuals regarding the breach; and
4. Resolution steps taken to mitigate the breach and prevent future occurrences.

H. Business Associate Responsibilities: The business associate ("BA") of the organization that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses **unsecured** protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been accessed, acquired, or disclosed during such breach. The BA shall provide the organization with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals. Regardless,

it is still the burden of the organization to document this notification.

I. Workforce Training: The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

J. Complaints: The organization must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization's breach notification processes.

K. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

L. Retaliation/Wavier: The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility benefits.

M. Breach Notification Under Texas Law
    1. Definitions:
        a. Breach of System Security - means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.
        b. Disclose - to release, transfer, provide access to, or otherwise divulge information outside the entity holding the information.
    2. Duty to Notify: A person who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (D) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
    3. Residency Consideration: Notwithstanding Subsection (B), the requirements of Subsection (B) apply only if the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of

Texas or another state that does not require a person described in Subsection (B) to notify the individual of a breach of system security. If the individual is a resident of a state that requires a person described by Subsection (B) to provide notice of a breach of system security, the notice of the breach of system security provided under the state's law satisfies the requirements of Subsection (B).

4. Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
5. Delay in Notification: A person may delay providing notice as required by Subsection (B) or (D) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.
6. Method of Notice: A person may give notice as required by Subsection (B) or (D) by providing:
    a. Written notice;
    b. Electronic notice, if the notice is provided in accordance with 15
        1. U.S.C. Section 7001; or
    c. Notice as provided by Subsection (G).
7. If the person required to give notice demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:
    a. Electronic mail, if the person has electronic mail addresses for the affected persons;
    b. Conspicuous posting of the notice on the person's website; or
    c. Notice published in or broadcast on major statewide media.
8. Notwithstanding Subsection (E), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.
9. If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.

ACCOUNTING OF DISCLOSURES

POLICY: Patients have a right, and Agencies have an obligation pursuant to the Health Insurance Portability and Accountability Act, to receive a written accounting of disclosures of their protected health information (PHI) from the respective Agency, for PHI of up to six years prior to the date from which the accounting is requested (a patient may request an accounting for a period of time less than six years).

PURPOSE: To document a patient's right to request and receive a written accounting of disclosures of a patient's protected health information.

DEFINITIONS:

HIPAA – Health Insurance Portability and Accountability Act

Protected Health Information (PHI) – Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

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

Limited data set – Protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: names, postal address information, telephone or fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, and full face photographic images

PROCEDURE:

A. Disclosing PHI
   1. Patients have the right to receive an accounting of disclosures of PHI from Agencies during a time period specified up to six (6) years prior to the date of the request for an accounting by the patient.
   2. Not all disclosures require tracking or need to be accounted for upon request by the patient. Those disclosures excluded from accounting include:
      a. Information related to treatment, payment or health care operations;
      b. To the patient about his or her own information;
      c. To persons involved in the patient's care;
      d. For national security or intelligence purposes;
      e. To correctional institutions or law enforcement officials as permitted under the law;
      f. Disclosure made prior to the date of compliance with the privacy standard;
      g. Incidental disclosures;
      h. Disclosures that are part of a limited data set; and
      i. Disclosures for which the Agency has obtained a written authorization from the individual.

j. All disclosures of PHI, other than those documented above, must be tracked by the Agency either manually or electronically.
k. Disclosures include any information regardless of format including hard copy, verbal release and electronic medical records.

B. Request for Accounting of Disclosure. When a patient makes a request for an accounting of disclosures, the written accounting for each disclosure must include:
1. Date of disclosure;
2. Name and address, if known, of the entity or person who received a copy of the PHI;
3. Brief description of the PHI disclosed;
4. A brief statement of purpose that reasonably informs the individual/patient of the purpose of the disclosure or a copy of the written request for disclosure; and
5. If multiple disclosures are made to the same Agency or person for the same reason, it is not necessary to document for each disclosure. The Agency may document instead the first disclosure, the frequency or number of disclosures made during the accounting period, and the date of the last disclosure in the accounting period.

C. Requirements of Accounting. The patient's request for an accounting must be acted upon no later than sixty (60) days after receipt. Agencies are required to:
1. Provide the accounting as requested, or;
2. If the Agency is unable to process the request for an accounting within the timeframe specified above, then it may extend the time by no more than thirty (30) days, but only if:
a. The Agency provides the patient a written statement documenting the reason for the delay within the allowed time period and the date when the accounting will be provided and;
b. The Agency has taken no other extensions of time with regards to this particular request.
3. The Agency will provide the first accounting at no charge to the patient in any 12-month period. Patients requesting additional requests for disclosure within a 12-month period will be charged a reasonable fee, based on the Agency's cost of providing the accounting.
4. Before charging a fee to the patient, the Agency will inform the patient and allow them the opportunity to withdraw or modify their request to avoid or reduce the fee.

D. Documentation Requirements
1. The agencies will document and retain documentation, in written or electronic format, for a period of six years:
2. All information required to be included in an accounting of disclosures of PHI;
3. All written accountings provided to individuals and;
4. Titles of persons or offices responsible for receiving and processing requests for an accounting from individuals

E. Suspension of Accounting. There are limited exceptions when a health oversight agency or law enforcement officials may request that disclosures made to them not be provided to the patient on a temporary basis. If questions arise, please contact Agency Legal Department.

DATA AND INFORMATION

POLICY: To collect appropriate information and maintain confidentiality.

PURPOSE: To maintain health care records in accordance with legal, accrediting and regulatory agency requirements.

PERSONNEL: All personnel

PROCEDURE:

A. HIPAA regulations define health information as "any information, whether oral or recorded in any form or medium" that:
   1. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and
   2. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."

B. Protected health information (PHI) under HIPAA includes any *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual (that is *identified* information). It also includes health information with data items which reasonably could be expected to allow individual identification.

C. The information contained in the health record is kept at the location from which services are provided. The record belongs to the Agency and the patient is entitled to the protected right of information. All patient care information shall be regarded as confidential and available only to authorized users. A patient's clinical record (whether hard copy or electronic form) must be made available to a patient, free of charge, upon request at the next home visit, or within 4 business days (whichever comes first).

D. A copy of medical records may leave the Agency at the discretion of and with permission from the Administrator/Alternate Administrator/Agency Director. All copies of records must be returned and then shredded by appropriate personnel.

E. The types and amount of information gathered and recorded about a patient shall be limited to that information needed for patient care, outcomes data reporting and for claims processing.

F. All individuals engaged in the collection, handling or dissemination of patient health information shall be specifically informed of the responsibility to protect patient data and the penalty for violation of this trust. Violation of confidentiality of patient information shall be cause for immediate disciplinary action.

G. The collection of any data relative to a patient, whether by interview, observation or review of documents, shall be conducted in a setting which provides maximum privacy and protects the information from unauthorized individuals.

INFORMATION MANAGEMENT AND CYBERSECURITY

Purpose: All aspects of the agency's success and client's quality of care are based on information and the decisions that are based on the available information. Security of client information is the top priority agency. Additionally, the agency's business information is maintained confidentially within the organization.

Policy:
Information management drives agency decisions and quality of care. When processing information, the security of client information will remain the top priority.

Procedure:
1) The agency will process information in a timely and efficient manner to provide access to the most current data for decision making.

2) To ensure the continued availability of information the agency routinely performs data backups. Electronic backups are rotated off site, so that in the event of a disaster the agency will be able to maintain continuity of care and information base. The backup location should be secure. Refer to the Disaster Plan for restoring services and ePHI during service interruptions.

3) Client information will be limited to the person directly involved in the client's care.

- Examples of possible data inputs:
- Physician
- Referrals Sources
- Clients
- Caregivers/Client Family
- Community Resources
- Staff

11) Data flows within the organization with respect to privacy of client information. With respect to client confidentially information flow is open amongst staff and client.

12) Information leaves the agency to promote the welfare of clients and the viability of the agency with respect to maintaining client confidentiality.

13) All agency staff (employee and contractor) having access to Government databases including HHSC, TMHP, billing and data collection portals and similar information, such as is outlined in Texas HB 3834 of the 86th TX legislature will be required to complete A Texas DIR (Department of Information Resources) Cybersecurity Training meeting the state requirements annually. The administrator will attest to completion and affirm with each state services contract established or renewed.

14) Agency information management services team and the agency administrator will ensure a practice of password changes on company computer systems and electronic devices in accordance with security and privacy attestations for government contracting.

BUSINESS ASSOCIATE CONTRACT-HIPAA- PHI

Purpose: To ensure that business associates are in compliance with safeguarding protected health information.

Policy:
It is the policy of this agency to safeguard protected health information (PHI), therefore this agency requires the same of it business associates. Business associates are required to safeguard protected health information that they may come into contact with from this agency. Before this agency will collaborate with another business, a business associate contract must be in place.

Procedure:
1) The Administrator will require all business associates to sign a business associate contract prior to allowing access to any protected health information.

2) If the business associate refuses to the sign agreement, the Administrator should attempt to learn the reason for the refusal, but may not move forward with services until a signed business associate contract is in place.

3) Business associates must disclose all their business associates that will have access to agency protected health information as a result of the business collaboration.

4) If a business associate has a business associate that will have access to protected health information, it must also sign a Business Associate Contract prior to being allowed contact with PHI. Regardless of how many business associates or how deep the level of business associates extends; all business associates that will have access to this agency protected health information must sign a Business Associate Contract prior to being permitted access to PHI.

5) If business associate breaches unsecured PHI, they must perform a PHI Breach Risk Assessment to determine the level of risk and provide the risk assessment to **the Agency** within 5 business days of learning of the occurrence.