Katy Trail Community Health
Privacy Policies

Origination Approval: Linda Messenger **Date:** 5/08

Revisions Approved By Board of Directors: July 22, 2021

Board President

Chief Executive Officer:

Privacy Policies

Standards for Privacy of Individually Identifiable Health Information

Privacy Standards for the Protection of Protected Health Information

Katy Trail Community Health

Privacy/Medical Records Policy
Table of Contents

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Safeguards to Protect the Privacy of Protected Health Information
Policy Number: 7.01
BOD Approval: 10/2009
Effective Date: 5/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will establish appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI). Privacy Policies and Procedures will be reviewed every two years. Any documentation records required within these policies and procedures will be maintained for a minimum of six years (CFR 164.316).

II. GUIDELINES:

1. KTCH will maintain a unique electronic clinical record for every patient receiving ongoing care at any of its locations. Patients who were seen prior to April 1, 2009 will also have a unique paper clinical record.

2. KTCH will safeguard PHI from reasonably anticipated uses or disclosures which are in violation of KTCH Privacy Policies and Procedures, the Privacy Rule's standards, and other applicable privacy laws.

3. KTCH will use the following types of safeguards for protecting the privacy of protected health information (PHI):
    a. **Administrative Safeguards:** These include, but are not limited to:
        - Implement policies and procedures to prevent, detect, contain, and correct security violations.
    b. **Physical Safeguards:**
        - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
    c. **Technical Safeguards:**
        - Implement policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

III. REFERENCES

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. Parts 160 and 164

Policy Title: Safeguards to Protect the Privacy of Protected Health Information- Administrative Safeguards
Policy Number: 7.02
BOD Approval: 10/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will implement appropriate Administrative safeguards to protect protected health information.

II. GUIDELINES:

1. **Security Management:** KTCH will implement policies and procedures to prevent, detect, contain, and correct security violations through:

    a. **Risk Analysis** (method of determining what kinds of controls are needed to protect KTCH information systems and other assets).
        i. Corporate Compliance Officer and IT vendor to conduct assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information by evaluating:
        - **Assets** — The resources KTCH wants to protect, including computers, networks, applications, databases, hardware, software, facilities, and patient health information (PHI).
        - **Threats** — Events that could occur and cannot ever be eliminated, although you can reduce the likelihood of occurrence or mitigate their impact. Even stringent security cannot eliminate every threat, including events such as hurricanes, earthquakes, viruses, hackers, data destruction and modification, theft of PHI, fire, false alarms, bomb threats, sabotage, fraud, or embezzlement.
        - **Vulnerabilities** — Weaknesses or "windows of opportunity" that could allow a threat to materialize. For example, not having a current and up-to-date security plan could cause employees to allow unauthorized access to systems by leaving systems logged on when they are not in use. Another example would be employees who do not log off their computer at lunch or share their password with co-workers.

- **Losses** — Anything that can be taken away from the organization. This includes loss of PHI by modification or destruction, theft of equipment, delays, or denials of service, or even loss of life. For example, a local hospital had a list of Alzheimer's patients stolen that was used to present false invoices to the individuals, who then sued the hospital for releasing personal information.
- **Safeguards** — Administrative, physical, or technical controls designed to provide protection against threats and reduce identified vulnerabilities. Examples of safeguards could include terminals that log off automatically; user authentication devices, such as biometric mice; background checks on key personnel; and an emergency mode operation plan.

b. **Risk Management**
   i. Implement security measures to reduce risks and vulnerabilities of PHI against reasonably anticipated threats or hazards to the security of PHI.
   ii. All charts will be maintained in locked areas when not attended by appropriate staff.
   iii. Fax machines will be in safeguarded areas.
   iv. Computer systems will have appropriate security measures to protect and guard against malicious software.

c. **Sanction Policy**
   i. Appropriately discipline KTCH employees (per KTCH Personnel Policies) who fail to comply with the security policies regarding PHI.

d. **Information System Activity Review**
   i. Regularly review the electronic medical records (EMR) system activity, including but not limited to audit logs, access reports, and security incident tracking reports.

KTCH will assign security responsibility through:

a. **Assigned Security**
   i. The Privacy Officer, under the supervision of the Chief Operating Officer, is responsible for the development and implementation of the Privacy Policies and Procedures, in consultation with the IT Vendor and Corporate Compliance Officer.

ii. The IT Vendor under the supervision of the Corporate Compliance Officer is responsible for security of the software and hardware.

b. **Workforce Security**

i. All members of KTCH will have appropriate access to electronic protected health information. KTCH will prevent employees, including contract employees, from having unnecessary access using passwords, time outs on computers, and limited access to the practice management system and/or EMR system dependent on job duties. The Corporate Compliance Officer has full responsibility in limiting or granting computer access levels for the practice management system and/or EMR. The IT Vendor will assist in the implementation and process for security measures.

ii. Employees will be required to log off their computer system when leaving their work area to prevent unauthorized users from accessing electronic PHI. Employees will keep their computer screens faced in such a way that unauthorized staff, patients, or visitors are not able to view electronic protected health information.

iii. When employment of a KTCH employee ends, the IT Vendor will be notified by the department manager on the *Employee Action* form so that access to the EMR can be removed immediately.

c. **Security Awareness and Training**

i. KTCH employees will be trained annually on PHI. This training will include aspects of protecting and managing PHI, and:

i. Security Reminders
ii. Protection from malicious software (opening emails from unknown senders, etc.)
iii. Log-in Monitoring
    1. Monitoring log-in attempts and reporting discrepancies
iv. Password Management
    1. Creating, changing, and safeguarding passwords

d. **Security Incident Procedures**

i. KTCH employees will notify the Privacy Officer immediately if they suspect or know of a security breach within the electronic PHI system, including the Practice Management

system, Electronic Medical Record system, or fax transmittals. Any incident of this kind will be reported on an event report. The Privacy Officer or his/her designee will investigate and mitigate to the extent practical. Documentation will include the outcome of the event and be kept by the Privacy Officer.

e. **Contingency Plan**

ii. KTCH will have all electronic PHI data backed up daily. In case of fire, natural disaster, vandalism, system failure, or other damage to systems containing PHI. The IT Vendor will maintain a copy of all backed up data off-site.

f. **Evaluation**

iii. A review of the Privacy Policies and Procedures will occur by the Privacy Officer, Chief Operating Officer, and the Quality Committee of the Board every two years. Environmental and/or operational changes affecting the security of electronic PHI will be evaluated.

2. **Business Associate Contracts and Other Agreements.** A business associate may be permitted to create, receive, maintain, or transmit electronic PHI on KTCH's behalf when the business associate has administrative, technical, and security measures in place to protect PHI, and a business associate agreement has been signed by both parties.

This standard does not apply to other health care providers concerning treatment of an individual, transmission of electronic PHI by a group health plan or an HMO, or health insurance issuer on behalf of a group health plan to a plan sponsor, or government entities who are sponsoring a health plan (i.e. Medicare and Medicaid).

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.308

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Safeguards to Protect the Privacy of Protected Health Information- Physical Safeguards
Policy Number: 7.03
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will implement appropriate physical safeguards to protect protected health information (PHI).

II. GUIDELINES:

1. **Facility Access Controls**:
   a. KTCH will limit physical access to its electronic information systems and the areas where they are housed. IT, and administrative staff are the only staff who have access to the server room.
   b. Computers which can access PHI are accessible to staff only. Restricted access is achieved through individual staff log on and system security parameters.
   c. KTCH has a security system to prevent unauthorized physical access to the building, and limits afterhours access to specific staff which may include, but not limited to administrative staff, physicians, and providers.

2. **Workstation Use and Security:**

a. All staff will be trained on protection of PHI annually. The physical placement of staff computers will be in such a way to prevent visitors or unauthorized users from viewing electronic PHI. Employees will log off their computers when leaving their workstation.

3. Device and Media Controls:

   a. When receiving or removing electronic media and/or hardware containing electronic PHI, staff will protect this information in the same fashion as electronic PHI.
   b. All PHI in electronic form which is to be disposed of will be destroyed. Computer hard drives will be erased, electronic media (discs, tapes) will be erased or shredded. The electronic form of PHI will not be disposed of in regular trash without PHI being removed.
   PHI will be backed up and/or copied prior to movement of equipment if needed

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.310

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Safeguards to Protect the Privacy of Protected Health Information- Technical Safeguards
Policy Number: 7.04
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will implement appropriate Technical safeguards to protect protected health information (PHI).

II. GUIDELINES:

1. KTCH will implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights through:
    a. Using a unique name by each employee for identifying and tracking user identity.
    b. Electronic PHI will be backed up daily so that access can occur in an emergency.
    c. Automatic log off will occur on each electronic information system.
    d. Electronic PHI will be electronically protected by a firewall.

2. KTCH will implement hardware, software, and/or procedural mechanism that record and examine activity in the information systems that contain or use electronic PHI.

3. KTCH will protect electronic PHI from improper alteration or destruction by set security levels by job duties and will have the capability to verify that a person or entity seeking access to electronic PHI is the one claimed by firewall log-in. Technical security measures will guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, and that it is not improperly modified.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.312

Policy Title: Safeguards to Protect the Privacy of Protected Health Information- Organizational Requirements

Policy Number: 7.05

BOD Approval: 12/2009

Effective Date: 05/2008

Responsibility: All Staff

Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will implement appropriate organizational standards to protect protected health information (PHI).

II. GUIDELINES:

1. KTCH may enter into Business Associate Contracts or other agreements to create, receive, maintain, or transmit electronic PHI on its behalf. Examples of this exchange of information would be to claims processing or administration, data analysis, , utilization review, quality assurance, and billing. It is the responsibility of KTCH that their business associates will:
   a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity as required.
   b. Ensure the business associate and/or their partners will provide reasonable and appropriate safeguards to protect its electronic PHI.
   c. Report to KTCH any security incident of which it becomes aware.
   d. Authorize termination of the contract by KTCH if KTCH determines that the business associate has violated a material term of the contract.

2. **Identification of Business Associates:** KTCH will identify all its business associates. A business associate is a person or entity that provides certain functions, activities, or services for or to KTCH involving the use and/or disclosure of protected health information (PHI).

3. **Satisfactory Assurance/Documentation:** KTCH will obtain satisfactory assurance that the business associate will appropriately safeguard KTCH patients PHI. KTCH will document this agreement through a written contract with the business associate that meets the requirements of this procedure.

4. **Required Contract Elements:** Every written contract with a business associate will identify the uses and disclosures of a patient's PHI that are permitted or required by the business associate, except any uses or disclosures that would not be permitted by KTCH under the HIPAA standards. The contract will detail how the business associate will:

a. Not use or further disclose the information other than as permitted or required by the contract or as required by law.
b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.
c. Report to KTCH any use or disclosure of the information not provided for by its contract of which it becomes aware.
d. Ensure that any agents, including a subcontractor, to whom it provides the information, agrees to the same restrictions, and conditions that apply to the business associate with respect to the information.
e. Make the information available to KTCH when it receives a patient's request to access his or her protected health information for amendment, and for request for accounting of disclosures.
f. Make available its internal practices, books, and records relating to the use and disclosure of PHI to KTCH and the Secretary of the Department of Health and Human Services for purposes of determining the parties in compliance with the contract and with the standards, implementation specifications and other requirement of the Privacy Rule.
g. At the termination of the contract, return or destroy all PHI that the business associate still maintains in any form and retain no copies of the information. If return or destruction is not feasible, extend the protections of the contract to the information remaining and limit further uses and disclosures to the purpose that made the return or destruction infeasible.

5. **Optional Contract Elements:** KTCH may permit a business associate to use the PHI for the proper management and administration of the business associate or to carry out its legal responsibilities and may permit the business associate to disclose the information for these purposes if the disclosure is required by law, or:
   a. the business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will be held confidentially and used or further disclosed only as required by law or for the intended purpose.
   b. the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

6. **Contract Violations:** If KTCH knows of a pattern of activity or practice business associate that constitutes a material breach or violation of the business associate's obligations under the contract, KTCH will take reasonable steps to cure the breach or end the violation, as applicable. If these steps are unsuccessful, KTCH will terminate the contract, if feasible, or, after consultation with legal counsel, report the problem to appropriate federal authorities.

III. REFERENCES:

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.504

Policy Title: Use of Notice of Privacy Practices
BOD Approval: 9/2013
Responsibility: All Staff

Policy Number: 7.06
Effective Date: 7/2013
Distribution: All Departments

I. POLICY:

An individual has a right to request adequate notice of the uses and disclosures of PHI that may be made by Katy Trail Community Health (KTCH), of individual patient rights, and KTCH's responsibilities. KTCH is required to provide a written Notice of Privacy Practices to all patients, as well as other individuals who may request a copy.

II. GUIDELINES:

Requirements for Electronic Notice:
KTCH maintains a website that provides information about customer services and/or benefits. The Notice of Privacy Practices must be posted on the website and must be made available to users in electronic form.

Documentation of Notice:
KTCH must document compliance with the Notice of Privacy Practices requirements by retaining copies for six years. The Acknowledgement of Receipt (or, if not obtained, the documentation of good faith efforts and reasons for not obtaining it) must be placed in the patient's medical record.

Revisions to the Notice:
KTCH must promptly revise and distribute the Notice of Privacy Practices whenever there is a material change to the users or disclosures, the individual's rights, KTCH's legal duties, or other privacy practices stated in the notice.

Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which the material change is reflected. The effective date must be shown in the Notice of Privacy Practices.

The revised notice must be made available upon request and must be posted in a clear and prominent location where it is reasonable to except patients to be able to read it.

Enforcement:
All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

Emergency Exception:

In emergencies, KTCH is not required to provide the Notice of Privacy Practices at the time of first service delivery. In such circumstances, the Notice of Privacy Practices may be provided as soon as reasonably practical after the emergency situation

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.520

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: General Policy on Uses and Disclosures of PHI
Policy Number: 7.07
BOD Approval: 9/2013
Effective Date: 8/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) employees may use and disclose PHI for treatment, payment and/or healthcare operation purposes. Except in the limited situations where the "Minimum Necessity" standard does not apply, KTCH and its employees shall use and disclose only the "Minimum Necessary" amount of information required to accomplish the intended purpose of the use, disclosure or request

II. DEFINITIONS:

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity that maintains it (i.e., KTCH only).

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information (i.e. KTCH).

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Payment means:

- Activities relating to a patient that are undertaken by:
  - A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
  - A health care provider or health plan to obtain or provide reimbursement for the provision of health care.
- These activities include, but are not limited to:
  - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims.
  - Risk adjusting amounts due based on enrollee health status and demographics characteristics.
  - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance), and related health care data processing.

  - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.
  - Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
  - Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursements.
- Name and address.
- Date of birth.
- Social security number.
- Payment history.
- Account number; and
- Name and address of the health care provider and/or health plan.

Health Care Operations means any activities of KTCH to the extent the activities are related to providing and/or monitoring and improving health care, including the following activities:

- Conducting quality assessments and improvement activities, including outcome evaluations and development of clinical guidelines. Population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, reviewing the competence or qualifications of health care professionals, and evaluation their performance, as well as conducting training programs.
- Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care, providing that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable.
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
- Business planning and development, such as conducting cost management and planning related analyses related to managing and operating KTCH, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- Business management and general administrative activities of KTCH, including, but not limited to: management activities related to HIPAA compliance; customer services; resolution of internal grievances; sale, transfer, merger, or consolidation of covered entities; creating de-identified health information or a limited data set; and fundraising for the benefit of KTCH.

Minimum Necessary means the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request. Under this standard, when using or disclosing PHI or when requesting PHI from another covered entity, KTCH must take reasonable steps to limit PHI from another covered entity, KTCH must take reasonable steps to limited PHI to the minimum necessary amount of information. The Minimum Necessary standard does not apply to:

- Disclosures or requests by a health care provider for treatment (trainees may be included as health care providers for this purpose).
- Uses or disclosures made to the individual, as permitted or required under the HIPAA privacy rule and Missouri law.
- Uses or disclosures made pursuant to a valid authorization.
- Disclosures to the U.S. Department of Health and Human Services, as required by the HIPAA privacy rules.
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for compliance with applicable provisions of the HIPAA privacy rules.

For more information or explanation regarding the Minimum Necessary, please see the KTCH Minimum Necessary Use and Disclosure Privacy Policy.

Indirect Treatment Relationship means a relationship between an individual and a health care provider in which:

- The KTCH provider delivers health care to the individual based on the orders of another health care provider; and
- The KTCH provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services, products, or reports to the individual.

III. GUIDELINES:

Permitted Uses and Disclosures

KTCH may use and disclose PHI for:

- Its own treatment, payment, or healthcare operations.
- Treatment activities of a health care provider.
- The payment activities of another covered entity or healthcare provider.
- The healthcare operation activities of another covered entity or health care provider, if each entity has or had a relationship with the individual who is the subject of the PHI being requested, and the disclosure is:
  - For a purpose listed in the definition of health care operations; or,
  - For healthcare fraud and abuse detection or compliance.
- Another covered entity that participates in an organized healthcare arrangement with KTCH for any healthcare operation activities of the organized health care arrangements.

For KTCH to use and disclose PHI for purposes other than those listed above, see KTCH policies of *PHI Uses and Disclosures Based on Patient Authorizations* and *Notice of Privacy Practices.*

Personal Representatives, Minors, and Deceased Individuals

For information regarding proper uses and disclosures for Personal Representatives, Minors, and Deceased Individuals, see the KTCH policy *Personal Representatives, Minors, and Deceased Individuals.*

Enforcement:

All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

IV. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. §164.501, 164.502(b), 164.514(d)(1)

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Minimum Necessary Use and Disclosure
BOD Approval: 09/2013
Responsibility: All Departments

Policy Number: 7.08
Effective Date: 08/2013
Distribution: All Departments

I. POLICY:

When using or disclosing PHI, or when requesting PHI from another covered entity, KTCH shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. All persons who handle PHI in any manner are expected to know and comply with the provisions of this policy.

II. GUIDELINES:

Required Assessment of Routine and Non-Routine Disclosures and Augmentation of this Policy

KTCH is responsible for the following tasks:

- KTCH administration must:
  - Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.
  - Review requests for disclosure on an individual basis with such criteria.
  - Augment this policy with written provisions covering the criteria for non-routine disclosures and the process for reviewing them; and
  - Train affected members of KTCH workforce and implement the augmented policy provisions

Limitations on Use and Disclosure of PHI-

- **Access to PHI:** Access to PHI within KTCH shall be limited in accordance with KTCH's Information Technology Policies and Procedures. Access to PHI and any conditions on such access shall be granted based on the individual's or class of individuals' role as determined by the appropriate administrator. Access rights and controls shall be modified or altered promptly as needs and/or personnel change.

- **Requests for Uses or Disclosures of PHI:** Except in emergency situations, any request for PHI that is directed to the medical records custodian must include the requestor's name, unique identified (such as DOB), and the specific information requested.

- **Audits:** The Privacy Officer will be responsible for facilitating random checks to ensure the minimum necessary standard is being applied when using and disclosing PHI and HIM will forward the audit results to the KTCH privacy officer.

- **Requests for Use and Disclosure of an Entire Medical Record:** KTCH personnel may not use, disclose or request an entire medical record, except when the entire medical record is justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

- **Good Faith Reliance:** The medical records custodian may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum amount necessary to accomplish the purpose of the request when:

    - The information is requested by another covered entity.
    - The information is requested by a professional (such as an attorney or accountant) providing professional services either as an employee or as a business associate.
    - The disclosure is made to health care-related entities or agencies for purposes that do not require consent, authorization, or opportunity to agree or object, and the official has represented that the information is the minimum necessary or is required by law;
    - Adequate documentation or representations have been provided by a person requesting the information for research purposes; this includes requested where:
        - The relevant IRB or privacy board documentation represents that proposed research meets the minimum necessary standard.
        - The requestor asserts that the information is sought solely to review PHI as necessary to prepare a research protocol; or
        - The requestor asserts that the information is for research on decedents.

In summary, PHI may be used internally by KTCH personnel for treatment purposes. PHI may not be released outside of KTCH without appropriate authorization and documentation.

Disclosures for Payment-
Only the minimum necessary PHI shall be disclosed for payment functions, as provided through contractual agreements. Persons handling PHI in a payment context shall refrain from publicizing patient diagnosis information. This policy shall apply to checks collected, credit card paper receipts, and envelopes and invoices sent to consumers.

Disclosures Required by Law-
Disclosures Ordered by a Court or Administrative Tribunal:

The minimum necessary standard does not apply to disclosures ordered by an administrative tribunal or court. Only the information expressly authorized by the order is to be provided.

PHI About a Victim of a Crime or Abuse:

The minimum necessary standard shall apply to information released to law enforcement regarding victims of crime or abuse. However, if the law requires

information to be released, then disclosure must be made in compliance with and limited to the relevant requirements of such law.

Enforcement:

All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. §§ 164.501; 164.514(b), (d); 164.506; 164.512(b), (f)(3), (l)

Policy Title: Use and Disclosure of PHI for Judicial or Administrative Proceedings
Policy Number: 7.09
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

As a rule, KTCH personnel may not disseminate PHI without authorization except as permitted by HIPAA's Privacy Rules.

PHI may be used or disclosed during judicial or administrative proceedings to the extent permitted by the Privacy Rules and Missouri law.

Disclosures during judicial or administrative proceedings must be supposed by a legally valid order of a court or administrative tribunal, subpoena, or discovery request. Such documents will be transmitted to the Privacy Officer, promptly upon receipt. He/She then will consult with the CEO as to if there are any questions as to whether, when and/or how to respond to the request

II. GUIDELINES:

Permitted Disclosures-

Authorized Requests- An authorized, legal request for PHI may be authorized with verification of the patient signature. Only the specifically authorized requested PHI will be released. Any and all requests must specifically state what part of the chart is being requested aligning with the minimum necessity rule.
If the authorization does not have a valid signature, records will only be released with a court ordered subpoena.

Authorizations without the Patient's Signature- If the health center receives a legally valid order of a court or administrative tribunal, subpoena, or discovery request, the document will be immediately given to the Privacy Officer. The Privacy Officer can continue with the process if the following two bullets have been met:

- The document must be signed by a judge of the court. No other signatures will be valid.
- If the document is a subpoena, the subpoena must be from the state of Missouri. Any subpoenas issued by other state courts or administrative agencies are not valid in Missouri, and KTCH cannot comply.

Invalid Requests-

If either of these bullets applies, the Privacy Officer will immediately notify the requesting party of that KTCH cannot comply with the request and the specific reason why the request will not be fulfilled.

Valid Requests-

If neither of these bullets applies, the Privacy Officer will immediately present the document to KTCH's CEO for approval before processing.

When and if the request is processed, only the specifically authorized requested PHI will be released. All requests must specifically state what part of the chart is being requested aligning with the minimum necessity rule.

If the subpoena is a request for a provider testimony, it must be immediately routed to corporate council, as that is to determine (1) the scope of the testimony and (2) whether there is a possibility that the litigation might be connected to a malpractice lawsuit. KTCH will then decide about whether this request needs to be routed to HRSA or if we can allow our providers to testify.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.512(e)

Policy Title: Use and Disclosure of PHI by and for Personal Representatives, Minors, and Deceased Individuals
Policy Number: 7.10
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

The health center will treat a personal representative as the individual as outlined in the Privacy Rules, federal and state laws. KTCH will grant a personal representative access to the PHI only as applicable by law. There are circumstances where KTCH is not required to recognize a personal representative

II. GUIDELINES:

Definitions-
Personal Representative- A person who has legal authority to act on behalf of the individual in making decisions relating to health care. This may include parents, legal guardians or conservators, certain caregivers, or properly appointed agents, such as those identified in a valid power of attorney for health care, Natural Death Act Declaration, living will or advance health care directive.

Minor- An individual under the age of 18 who has not been legally emancipated by a court or is:

- Not married or divorced
- Not given birth or have a child
- Not on active duty with the U.S. Armed Forces
- Not at least 15 years of age or older **and** living away from home and managing his/her own financial affairs (regardless of source) **and** the parents or guardian are not liable for the medical care provided with the individual's consent.

For further definition of "*Minor"* refer to the clinical policies, *Consent for Treatment*.

Personal Representatives-
KTCH will treat a personal representative as the individual for the following purposes:

- Acknowledging receipt of the Notice of Privacy Practices
- Authorizing the use and disclosures of the individual PHI to third parties
- Authorizing the use and disclosures of the individual's PHI to the personal representative, but only to the extent permitted by other federal and state law.
- Exercising other individual rights granted by the Privacy Rule, to the extent consistent with other federal and state law.

The Privacy Rule does not change other federal and state laws that govern access to medical records. KTCH will grant a personal representative access to PHI only as authorized by applicable law.

Note: KTCH is not required to recognize a personal representative if it reasonably believes that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by the personal representative; or
- Recognizing the personal representative could endanger the individual; and
- KTCH, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Emancipated Minors and Adults-
If, under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions relating to health care, KTCH will treat that person as a personal representative for purposes of HIPAA compliance.

The Privacy Rule does not change other federal and state laws that govern access to medical records. KTCH will grant a personal representative access to the individual's medical records only as authorized by applicable law. Generally speaking, Missouri law grants all former and current adult patients or their guardians or conservators the right to inspect, request amendments, and make copies of the individual's medical records (except in the instance when KTCH does not recognize a personal representative due to reasonable belief, as listed above).

If a minor has been legally emancipated, his or her guardian or parent cannot be recognized as a personal representative. Refer to the clinical policy, *Consent for Treatment* for more information regarding legal or verbal emancipated minors.

Unemancipated Minors-
If, under applicable law, a parent, guardian, or other person has legal authority to act on behalf of an unemancipated minor in making health care decisions, KTCH must treat the person as a personal representative with respect to relevant PHI.

A minor may legally consent to a particular type of treatment without consent of a responsible adult. The minor will be treated as the individual for HIPAA compliance purposes. By way of example, minors may lawfully consent to the following types of treatment, among others:

- Pregnancy-related services
- Testing of venereal diseases (including sexually transmitted infections)
- Treatment for drug and/or alcohol use

A full listed can be found in the clinical policy, Consent for Treatment

Except as permitted by Missouri law or as authorized by a minor in writing, KTCH is prohibited from telling the minor's parent(s) or legal guardian about medical care the minor is legally able to authorize.

Deceased Individuals-
If, under applicable law, am executer, administrator, or other person has authority to act on behalf of a deceased individual or his/her estate, KTCH must treat that person as a personal representative with respect to PHI that is relevant to the representation. Under Missouri law, the personal representative (such as, executor or administrator) of the deceased individual's estates, are the only person(s) who may obtain PHI about the deceased individual or authorize its disclosure to others.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.502(g); 164.514(h)

Policy Title: Permitted Use and Disclosure of PHI to Family & Friends- Individual Care and Notification Purposes
Policy Number: 7.11
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

KTCH may use and disclose certain PHI (as described below) without the individual's written consent or authorization to release the information. In these cases, the individual must be informed in advance of the permitted use or disclosure and can agree, prohibit, or restrict the disclosure and have the opportunity to agree, prohibit, or restrict the disclosure. KTCH may orally inform the individual's agreement or objection to a use or disclosure permitted by this policy. KTCH staff must document the agreement, prohibition, or restriction in the medical record. In some circumstances, KTCH may use or disclose certain information without consent, authorization, or oral agreement as outlined in this policy.

II. GUIDELINES:

Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes-

- KTCH may disclose to a family member, other relative, close friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment for such care.
- KTCH may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.
- Any such use and disclosure of PHI for notification purposes must comply with applicable requirements, depending upon whether the individual is present at the time of PHI is disclosed:
    - **Uses and Disclosures with the Individual Present:** If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, KTCH may use or disclose the PHI if it:
        - Obtains the individual's agreement; or
        - Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
        - Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to such disclosure.
    - **Limited Uses and Disclosures When the Individual Is Not Present or Is Incapacitated, or in an Emergency**

- If the individual is not present, or cannot agree or object to the disclosure of PHI because of his/her incapacity or an emergency circumstance, KTCH may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care.
- KTCH may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual by picking up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

Enforcement
All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.510 (b)

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Uses and Disclosures of PHI Based on Patient Authorizations
Policy Number: 7.12
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Confidentiality of health information is the right of each patient seeking health care through KTCH. All PHI (both verbal and written) is strictly confidential. Where authorization to use or disclose PHI is required, such use or disclosure shall take place only after completion of a valid written authorization

II. GUIDELINES:

Definition-

Authorization: An authorization allows for the use and disclosure of PHI for purposes other than treatment, payment, and healthcare operations.

Core Elements of a Valid Authorization-

A valid authorization must be handwritten by the person who signs it or in typeface no smaller than 8-point type. It must be clearly separate from any other language present on the same page and executed by a signature that serves no other purpose than to execute the authorization. It must contain at least the following elements and must be handwritten in plain language:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful way.
- The name or functions of the persons(s) or class of persons authorized to disclose the medical information.
- The name or specific identification of the person(s) or class of persons authorized to receive the medical information.
- The specific uses and limitations on the use of the medical information to be disclosed. The statement "at the request of the individual" is a sufficient description if the individual has initiated the authorization and does not, or elects not to, provide a statement of purpose.
- A specific date after which the provider is no longer authorized to disclose the medical information.
- A statement advertising the person signing the authorization of the right to receive a copy of the authorization.
- Signature and date by an authorized person
- If a personal representative of the individual signs the authorization, a description of the personal representative's authority to act for the individual

- If the authorization is for marketing, KTCH must include a statement acknowledging whether direct or indirect remuneration is given to KTCH.

The authorization may contain elements or information in addition to the required elements, provided that such additional elements or information are not inconsistent with the required elements.

Compound Authorizations-

An authorization for use and disclosure of PHI may not be combined with any other document to create a compound authorization, except for the following:

- An authorization for the use and disclosure of psychotherapy notes may only be combined with another authorization for use and disclosure of psychotherapy notes.
- Where written authorization is required to disclose the results of an HIV/AIDS test, a separate written authorization is required for each separate disclosure.

An authorization, other than an authorization for a use and disclosure of psychotherapy notes and HIV/AIDS test results (as discussed above), may be combined with any other authorization unless KTCH has conditioned the provision of treatment, payment or enrollment in a health plan.

Defective Authorizations-

An authorization is not valid if the document has any of the following defects:

- The expiration date has passed.
- The authorization has not been filled out completely with respect to one of the core elements listed above.
- KTCH or its employees know that the authorization has been revoked.
- The authorization is combined with another document to create a compound authorization in violation of C.F.R. § 164.508(b)(3).
- The authorization was improperly required as a condition of providing treatment or otherwise violates C.F.R. § 164.508(b)(4).
- KTCH or its employees know that any other information in the authorization is false.

In the event of revoking an authorization, refer to "Revocation of Authorization to Release PHI".

Enforcement:

All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. §164.506; 45 C.F.R. § 164.508; 45 C.F.R. § 164.509; 45 C.F.R. § 164.512; 45 C.F.R. § 164.510

Policy Title: Revocation of Authorization to Release PHI
Policy Number: 7.13
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

An individual may revoke an authorization at any time, provided that the revocation is in writing, unless KTCH has already provided the PHI based on the patient's authorization. KTCH will stop providing information based on the patient's authorization as soon as possible.

The revocation form should be used to ensure the requirements of this section and the request(s) of the patient is met

II. GUIDELINES:

Definition-

- **Revocation:** An individual exercises the right to void a prior authorization to use and disclose PHI. After the revocation, KTCH may no longer use or disclose the patient's PHI without the patient's authorization. However, KTCH will not be liable for a use or disclosure of a patient's PHI after a revocation, if KTCH in good faith based its actions upon prior authorization, and has already acted in reliance upon the authorization.

An initial authorization form is completed and forwarded to the medical records department in accordance with the KTCH policy on *Use and Disclosure of PHI based on a Patient Authorization*.
In the case of a patient seeking to revoke a prior authorization, the revocation form will be forwarded to the Privacy Officer, for proper documentation in the official medical record. It will be the responsibility of the Privacy Officer to notify those authorized to use the patient's PHI that the patient has revoked his/her authorization. Once notified, by the Privacy Officer, of the revocation, all personnel are responsible for ensuring the patient's PHI is no longer subject to further use or disclosure.

Enforcement:
All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. §164.506(b)(5); 45 C.F.R. §164.508(b)(5)

Policy Title: Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object

Policy Number: 7.14

BOD Approval: 12/2009

Effective Date: 05/2008

Responsibility: All Staff

Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) may use or disclose protected health information (PHI), provided that the individual is informed in advance of the use or disclosure and can agree to or prohibit or restrict the use or disclosure. KTCH may orally inform the individual of and obtain the individual oral/ written agreement or objection to a use or disclosure of PHI

II. GUIDELINES:

1. Permitted uses and disclosures (except when an objection is expressed by an individual):

a. A directory of individuals in the facility

b. KTCH may disclose PHI directly relevant to the patient's care, to a member of the patient's family, other relative, or close friend or any other person identified, with verbal or written permission from the patient. (View the section within this policy titled "*Disclosures to Persons Involved with Patient's Health Care or Payment and for Notification*" for further detailed information)

c. KTCH may also disclose PHI in case of an emergency.

d. KTCH staff may use professional judgment and its experience with common practice to make reasonable inferences of the individuals best interest in allowing another person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI.

Disclosures to Persons Involved with Patient's Health Care or Payment and for Notification

KTCH may disclose PHI to a family member, other relative, close personal friend of the patient, or any other person identified by the patient who is involved with the patient's health care or payment. Disclosure is limited to the PHI that is directly relevant to the individual's involvement with the patient's health care or payment. KTCH may also use or disclose PHI to notify--- or assist in the notification of (including identifying or locating) --- a family member, a personal representative, or other person responsible for the care of the patient. This disclosure is limited to providing information about the patient's location, general condition or death.

KTCH's use or disclosure is subject to the following requirements:

- When a patient is present and capable of making health care decisions, KTCH will only use and disclose the PHI if:
    - The patient agrees.
    - The patient is provided with an opportunity to object and does not; or
    - It can be reasonably inferred from the circumstances (based on the exercise of professional judgment) and the patient does not object to the disclosure.

- If either (a) the patient is not present or (b) an opportunity to agree cannot be practically provided because of the patient's incapacity or emergency circumstances, KTCH may exercise personal judgment to determine whether the disclosure is in the best interest of the patient. If so, only the PHI directly relevant to the person's involvement with the individual's health care will be disclosed and made available (for example, information necessary to allow someone to retrieve prescriptions, medical supplies or X-rays for a patient).

Use and Disclosure for Disaster Relief

KTCH may use or disclose basic PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with these entities uses or disclosures for involvement in an individual's care and notification purposes. The following requirements will be adhered to, unless KTCH determines that they will interfere with the ability to respond to the emergency circumstances:

- When a patient is present and capable of making health care decisions, KTCH will only use and disclose the PHI if:
    - The patient agrees.
    - The patient is provided with an opportunity to object and does not; or
    - It can be reasonably inferred from the circumstances (based on the exercise of professional judgment) and the patient does not object to the disclosure.

- If either (a) the patient is not present or (b) an opportunity to agree cannot be practically provided because of the patient's incapacity or emergency circumstances, KTCH may exercise personal judgment to determine whether the disclosure is in the best interest of the patient. If so, only the PHI directly relevant to the person's involvement with the individual's health care will be disclosed and made available (for example, information necessary to allow someone to retrieve prescriptions, medical supplies or X-rays for a patient).

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.510

Policy Title: Handling of Privacy Complaints
BOD Approval: 12/2009
Responsibility: All Staff

Policy Number: 7.15
Effective Date: 05/2008
Distribution: All Departments

I. POLICY:

It is the policy of Katy Trail Community Health (KTCH) to keep a record of all complaints and to investigate all valid complaints to determine the circumstances surrounding any concerns our patients raise regarding privacy. If a patient's privacy right has been infringed upon in any way, or there is evidence that our staff or associates have not adhered to the privacy standards or our policies and procedures, we will take actions consistent with the HIPPA regulations and our policy and procedure on personnel discipline for breach of privacy or confidentiality and document these actions accordingly.

The HIPPA privacy regulations give all individuals the right to file complains to KTCH and the Office of the Secretary of the Department of Health and Human Services. Any privacy-related complaint can be made by a patient, employee, student, trainee, volunteer, business associate, or other internal or external person(s).

Under no circumstances will the fact that an individual has filed a complaint affect the services provided to that individual. Any staff found to be treating any individual differently in the light of a complaint will be sanctioned. Any retaliation is prohibited by law.

II. GUIDELINES:

A complaint may be made by telephone, mail, or in person. Upon receipt of a complaint about a possible breach or in regards to a patient's rights being infringed upon, the Privacy Officer will review the complaint and record the information given by the patient on to the HIPAA event report as well as. The form must describe the acts or omissions the patient believes to have occurred.
The HIPAA privacy complaint must include the following information:

1. The date on which the act or omission occurred
2. A description of the PHI affected and how it was affected; and
3. The name(s) of anyone who may have improperly been provided with the PHI

All complaints received by the Privacy Officer must be dated with a "Received Date".

- The KTCH Privacy Officer will review and act on the complaint in a timely manner and not more than thirty (30) days from receipt of the complaint. If greater time is necessary to review and investigate the complaint, the Privacy Officer shall, within the thirty (30) days, notify the grievant, in writing of the delay, and inform the grievant of the expected time frame for completion of the review.

- The Privacy Officer shall determine what PHI is affected by the complaint and if the PHI was provided to other covered entities and business associates.
- If the affected PHI was created and maintained by a business associate, the complaint will be forwarded to the business associate as outlined in the Business Associate Agreement. Complaints forwarded to business associates will be logged and a notice of the action sent to the patient make the complaint.

The Privacy Officer will determine if there is reason to believe that a violation has occurred, and the recommended course of action to be taken. The Privacy Officer will utilize the Breach Notification Decision Tree and Incident Assessment Form in the evaluation.

- If no violation has occurred the complaint and finding will be dated with "Review Completion Date", the complaint will be considered closed.
- If cause exists to believe that a violation has occurred, the Privacy Officer shall be responsible for determining the risk and harm level to the patient(s). The Privacy Officer will then be responsible for verify the "Breach Notification Rules" to determine what, if any, type of immediate notice should be made.
    - Following the determination of the risk and harm level, the Privacy Officer shall be responsible for determining if:
        a. Performance or training need to be improved.
        b. A recommendation for a change to the KTCH operating regulation or creation/revision of a HIPAA policy.
        c. Conclusion of policy violation is to be reported to implement disciplinary action (sanction).
- The KTCH Privacy Officer shall notify the appropriate administrators of the action needed.
- If disciplinary action must be taken, it must follow the KTCH policies, and is to be initiated by the appropriate administrator on referral of the report from the Privacy Officer.

If the complaint resolution finds that no cause exists to believe a violation occurred, the patient may seek resolution to the Chief Operating Officer (COO).

- The patient, through completion of the Complaint Form, will request that the Privacy Officer or designee forward the complaint to the COO.
- The COO will review and act on the complaint in a timely manner and not more than thirty (30) days from receipt of the complaint form.
- The COO will determine one of the following:
    - That the original determination of the Privacy Officer is accurate
    - That remediation should occur through increased training, or that a recommendation is made appointing authority for possible disciplinary action.
    - That a recommendation for department operating regulations review be initiated.
    - That a recommendation be made for the establishment of a new operating regulation

- The original complaint form, and any other accompanying forms, will be placed in the patient/complaint specific protected folder within the KTCH shared database.

Retention: The Privacy Officer's primary responsibility in the HIPAA Complaint process includes logging and retaining complaints in a retrievable manner for a minimum of six (6) years, and identifying:

a. Person or entity making the complaint.
b. Date complaint was received.
c. A list of what PHI was allegedly affected.
d. Status of complaint.
e. A list of business associates or other facilities affected; and
f. Actions taken or recommendations.

Investigation of Complaints-

The Privacy Officer (or designee) will contact all relevant parties to investigate the alleged privacy violations in consultation with the Chief Operating Officer (COO) and Chief Executive Officer (CEO).

Simultaneously, the Privacy Officer shall request an investigation by the Chief Information Officer of any information technology systems that may be involved to determine if a breach of privacy has occurred. If, during investigation, an individual is found to be in violation of a KTCH policy, he/she will be subject to the disciplinary procedures that apply as appropriate.

-

If the investigation results in a breach, the event will be documented on the Violation Tracking log, as outlined in the procedure above.

Assessing the risk and probability level of the breach- 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 qualify as a potential breach. An "acquisition, access, use, or disclosure in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:

A. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

B. The unauthorized person who used the protected health information or to the disclosure was made.
C. Whether the protected health information was actually acquired or viewed; and Privacy Officer will be responsible for assessing the level of "probability" of the further disclosure of the PHI and the level of "harm" that the disclosure will cause the patient. There are 4 levels-
    - Low Probability, Low Risk
    - High Probability, Low Risk
    - Low Probability, High Risk
    - High Probability, High Risk

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 organization may make breach notifications without completing a risk assessment.

Notice of Breach-

1. Content of the Notice: The notice shall be written in plain language and must contain the following information:
    A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    B. 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).
    C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
    D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
    E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

2. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:
    A. Notice to Individual(s): Notice shall be provided promptly and in the following form:
        1. 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. The 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. Limited examples

a. The organization may send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, if they all reside at a single address and all individuals to which the notice applies are clearly identified on the notice. When a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, however, address a breach notice to the dependent himself or herself.

b. In the limited circumstance that an individual affirmatively chooses not to receive communications from a health care provider at any written addresses or email addresses *and* has agreed only to receive communications orally or by telephone, the provider may telephone the individual to request and have the individual pick up their written breach notice from the provider directly. In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all of the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the ''written notice'' requirement.

2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes 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 precludes written notification to the next of kin or personal representative.

a. 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.

b. 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.

3. 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.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area (of the breached patients) when the breach of unsecured PHI affects 500 or more of the organization's patients of a State or jurisdiction.
   1. The Notice shall be provided in the form of a press release.
   2. What constitutes a prominent media outlet differs depending upon the State or jurisdiction where the organization's affected patients reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State

C. 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 identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.[1]
   1. For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

For breaches involving less than 500 individual, the organization will maintain a log of the breaches. The breaches may be reported during the calendar year or no later than 60 days after the end of that calendar year in which the breaches were discovered (e.g., 2012 breaches must be submitted by 3/1/2013 – 60 days). Instructions for submitting the logged breaches are provided at www.hhs.gov

[1] Note: If the breach involves "secured" PHI, no notification needs to be made to HHS.

Policy Title: Mitigation After Improper PHI Use or Disclosure
Policy Number: 7.16
BOD Approval: 09/2013
Effective Date: 08/2013
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

KTCH has a duty to ensure the proper use/or disclosure of PHI. To the extent practical, KTCH will mitigate (i.e., lessen or alleviate) any harmful effects that becomes known to it as a results of a use or disclosure of PHI in violation of KTCH's policies and procedures or applicable by law.

II. GUIDELINES:

KTCH will take appropriate and reasonable steps to mitigate harmful effects that become known to it as the result of a use or disclosure of PHI in violation to the KTCH policies and procedures.

This may include, but is not limited to, the following:

- Taking operational and procedural corrective measures as warranted to remedy violations.
- Taking employment actions to re-train, reprimand, or discipline employees as necessary, up to and including termination.
- Promptly addressing problems with business associates if KTCH becomes aware of a breach of privacy.
- Incorporating mitigation solutions into the KTCH policies as appropriate.
- Promptly addressing and investigating violations

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.530(f)

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Request Restrictions on Use and Disclosure of Protected Health Information
Policy Number: 7.17
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health (KTCH) will allow a patient the opportunity to request restrictions on release of their protected health information (PHI). KTCH will agree to requested restrictions if the restriction will not limit its ability to provide quality healthcare treatment or manage it healthcare operations, and if it information management procedures and systems will permit it to comply consistently with the requested restrictions. KTCH will also provide confidential communications by alternative means or to an alternative address if it receives specific alternative address or other method of contact.

II. GUIDELINES:

Restriction: An agreed limitation upon the use or disclosure of PHI to carry out Treatment, Payment, or Healthcare Operations (TPO) and/or disclosure for involvement in the individual's care. For instance, KTCH may use and disclose PHI for TPO, but the patient may request that KTCH not use or disclose PHI in other circumstances.

1. When an individual requests restriction, supply the individual with the *Request of Restrictions* form and have patient complete it.
2. It will be the responsibility of the Privacy Officer to receive requests for *Request for Restriction* form. The Privacy Officer will consult with the Chief Medical/Chief Dental Officers and/or the billing specialist prior to agreement to any restrictions on use and disclosure of protected health information.
3. The Privacy Officer will review the *Request of Restriction* form to determine whether KTCH is able to accept the restrictions. The Privacy Officer will complete and sign the form, supply the individual a copy, and place the original in the individual's electronic medical record (EMR) under the *Consent to Treat* category. The Privacy Officer or designee will also make the necessary postings to the individual's health record and/or billing record in the physical chart and/or the practice management system to enable the restrictions to be carried out.
4. KTCH will attempt to complete the *Request of Restriction* form during the time the individual is present in our office, but no later than 30 days after the receipt.
5. It will be the responsibility of the Privacy Officer/billing specialist to monitor any restriction to which the office agrees to.
6. If at any time KTCH finds that it cannot carry out the restrictions requested by an individual, a notice will be sent to the individual indicating same.

7. KTCH will accept a written request from the individual to terminate the restrictions at any time or will document any oral request to terminate restrictions from the individual. If an oral request is received, this will be documented on the original form, a copy of which will be supplied to the individual and placed in the patient's EMR under the *Consent to Treat* category.

Emergency Treatment-
If KTCH does agree to a restriction, however, KTCH may not use or disclose PHI in violation of it, except that, if the individual who requested the restriction needs emergency treatment and the restricted PHI is needed for that, KTCH may use the restricted PHI itself or disclose it to a health care provider to provide emergency treatment.

If restricted PHI is disclosed to another health care provider for emergency treatment, as outlined above, KTCH must request that the health care provider not further use or disclose the PHI.

An agreed restriction is not effective to prevent:

- Uses or disclosures from being made to the individual for inspection and copying their own PHI;
- The individual from obtaining an accounting of disclosures of PHI
- Uses and disclosures for which consent, authorization or opportunity to agree or object is not required.

Terminating a Restriction-
KTCH may terminate its agreement to a restriction if:

- The individual agrees to or requests the termination in writing,
- The individual orally agrees to the termination and the oral agreement is documented, or
- KTCH informs the individual that it is terminating the restriction.

Any PHI created and received after the termination will not be restricted. However, any PHI created or received before the termination will be restricted.

Documentation-
When KTCH agrees to or terminates a restriction, it must be documented as follows:

- A request or termination that is in written form, KTCH shall maintain an electronic copy of it for six (6) years.
- If the request or termination is oral, KTCH will create and maintain an electronic record of the transaction and maintain it for six (6) years.

Alternate Communications-
KTCH must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from KTCH by alternative means or at alternative locations.

KTCH will require the individual to make a request for alternate communication in writing.

KTCH may condition the provision of a reasonable accommodation on receipt of:

- When appropriate, information as to how payment, if any, will be handled; and
- Specification of an alternative address or other method of contact.

Enforcement:

All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.522

Policy Title: Patient's Right to Access Health Information
Policy Number: 7.18
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

Katy Trail Community Health(KTCH) will provide our patients the right to access, amend, or summarize their protected health information (PHI) and to obtain a copy of their health information, for as long as the information is maintained in our designated record set, with exceptions permitted by law, which include, but are not limited to:

a. Psychotherapy notes (notes written by a mental health professional documenting or analyzing the contents of conversation during a private counseling session and that are separated from the rest of the individual's medical record by the mental health professional).
b. PHI compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
c. PHI requested by an inmate, maintained by a correctional institution, or by a provider on behalf of the correctional institution, if obtaining the information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate.
d. In the event that a physician/provider of KTCH believes in their professional opinion that it is reasonably likely that to cause substantial harm to the individual or another person.
e. PHI obtained from someone else, other than a health care provider, under a promise of confidentiality, but only if access would be reasonably likely to reveal the source of the information.
f. PHI maintained by KTCH that is subject to or exempt from certain provisions of the Clinical Laboratory Improvement Act of 1988 (CLIA).

Staff members will who are also patients will only be permitted to access their own medical record or records of family members following the same processes as non-employed patients. Staff should never access these records themselves, for any reason.

II. DEFINITIONS:

Access means that patients may inspect their medical and billing records under the supervision of a staff member or obtain a copy of all or a portion of their medical and billing records for which a copying fee is charged.

Designated record set means medical and billing records used to make health care and payment decisions about patients.

Reviewable grounds meaning that KTCH is required to have another party/provider review a denial to access of a patient who requests their medical or billing records and is denied them.

Unreviewable grounds meaning that KTCH may deny a patient access to their medical or billing records without providing the patient an opportunity for review by another party/provider.

III. GUIDELINES:

Access:

1. Patients may request access to their medical/dental records and/or billing records by submitting a request in writing on the *Request for Access, Amendment, or Summary to Protected Health Information* form to the Privacy Officer. This form specifies that access will be granted or denied within 30 days of its receipt. The request must state the type of access requested (inspection, summary, and/or amendment). A summary will be accepted if there are reasons why a complete inspection or copy cannot be released.

2. When a request for access to the medical/dental record and/or billing record is made by a patient:
    a. Obtain the patient's medical/dental record/billing records and verify the patient's demographic
    information and signature on the *Request for Access, Amendment, or Summary to Protected*
    Health Information form with demographic information and signature on the *HIPAA-Medical*
    Consent form, or other document signed by the patient contained within the medical record.
        i. If the authenticity of the patient cannot be verified, mail a request to the patient to have a new *Request for Access, Amendment, or Summary to Protected Health Information* form notarized.
    b. Review the medical/dental records and/or billing record according to the request, to determine if:
        ii. The request for access is denied due to #3 below.
        iii. The information requested is complete.
            a. If the information is not complete, inform the provider responsible/billing specialist responsible for completion that a request for access has been made by the patient and the record will need to be completed within 30 days in order to comply with the patient's request or be found in non-compliance with HIPPA and subject to fines. If the record is not completed within 30 days, send a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form to the patient indicating that an extension to providing access will be required because the record is in the process of being completed and

indicating the specific date on which access will be granted. This date must not exceed an additional 30 days.

3. Exceptions to access are limited to very specific situations. Certain exceptions are unreviewable and for others we must permit the patient to request a review of our decision not to grant access.

   a. Unreviewable grounds for denial of access include (KTCH does not have to explain to the patient why KTCH has denied them access in the following circumstances):

   i. When the PHI is psychotherapy notes which are specially protected.
   ii. When the PHI was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
   iii. When the request is from an inmate of a correctional institution, and KTCH believes that providing a copy of the information would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or the safety of any person responsible for transporting the inmate.
   iv. When the patient has agreed to the denial of access when consenting to participate in a research study, we are conducting that includes treatment, for the duration of the research study.
   v. When the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

   b. Reviewable grounds for denial of access include (If the patient requests it, KTCH has to explain why KTCH denied them access in the following set of circumstances):

   i. When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person.
   ii. When the information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
   iii. The request for access has been made by the patient's personal representative and a licensed health care professional has determined that access to the personal representative is reasonably likely to cause substantial harm to the patient or another person.

4. Denial of access is a serious matter under the law. Before the Privacy Officer may make such a denial decision, it is our policy to conduct an internal review of that denial. Any such case should be given to the Chief Medical Officer or Chief Dental Officer and Chief Operating Officer who will authorize the denial.

a. If access is denied for one of the unreviewable reasons, return a copy of the authorization for *Request for Access, Amendment, or Summary to Protected Health Information* form to the patient, with a letter, indicating that we are unable to comply with the request for access due to the applicable reason. Retain a copy of the Request *for Access, Amendment, or Summary to Protected Health Information* form and letter sent to the patient in the patient's medical record.
b. If access is denied for one of the reviewable reasons, determine if a summary of the record may be made or portions of the record may be provided such as to prevent the risk associated with denial.

    i. If a summary of a portion of the record would prevent risk, return a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form with a letter to the patient indicating we are not able to comply with the request for complete access for the specified reason, but would be able to provide a summary of the information in the record or access to specific portions of the record.
    ii. If a summary or a portion of the record is not possible, return a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form with a letter to the patient indicating we are not able to comply with the request for access for the specified reason, but that the patient has the right to have this decision reviewed by another licensed health care professional/billing specialist.
    iii. If a request for review is received from the patient, give a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form and the medical/dental record to the Chief Medical Officer or Chief Dental Officer or Billing Specialist who will make a final determination. Upon the review and determination, send a response to the patient indicating the result of the review and if necessary, how the patient may file a complaint with KTCH and/or the Secretary of the Department of Health and Human Services (DHHS).
    iv. If a request for access to the medical/dental record/billing record is made and the person was not a patient of KTCH, return a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form to the individual indicating we have no records. If KTCH does not have records on this individual but knows where the requested information may be maintained (such as at a hospital or other physician's office), return a copy of the *Request for Access, Amendment, or Summary to Protected Health Information* form to the individual and provide the name and address of the location where the records may be maintained.

v. Maintain all documentation in the medical record.

Type of Access:

1. Inspection:

a. If access to the medical/dental/billing record is accepted, the information is complete, and the patient requests inspection of the medical/dental record and/or billing record or any portion thereof, schedule an appointment for the patient to visit the office. The patient's electronic record will be printed out either in its entirety or the requested portion. Patients will not be permitted, even with supervision, to view their chart within the electronic medical record system. The Privacy Officer, a member of administration or a physician/provider must be present with the patient during the time the patient is inspecting the record(s). During this time, the patient may not remove any documents from the record(s) or write any information in the record(s). If the patient has any questions concerning the information in the medical record, inform the patient that an appointment must be made with the physician/provider to discuss the information. If the patient has any questions concerning the information in the billing record, refer the patient to the billing specialist.

2. Amendment:

a. If the patient wishes to make an amendment to the record(s), follow the Policy and Procedure for Patient's Right to Request Amendment of Health Information.

3. Summarize:

a. KTCH may provide a summary of PHI if the patient or legal representative agrees to the summary and the associated fees. If agreed to, a summary must be provided within 30 days. If KTCH is unable to comply within 30 days, an extension of 30 days may be used if the requestor is notified in writing of the reasons for the delay.

4. Copy:

a. If a patient requests a copy of their medical information, they may fill out an *Authorization for Use or Disclosure of Protected Health Information* form. If the request is accepted, make the specified paper copies or electronic copy, if requested, and mail the information to the patient via postal mail or make arrangements for pickup. If the patient requests this information to be mailed to a different address, mailed to a different individual, or be given to someone else who physically presents to our office, this information must be authorized through the *Authorization for Use or Disclosure of Protected Health Information* form. If another individual is designated to physically pick up the copy of the information, verify the individual's identity by requesting a photo identification card or other form of identification and match the name on the card to the name on the authorization form signed by the patient. A copy of the photo ID will be scanned into the HER showing who picked up the document(s).

IV. REFERENCES

This policy/ procedure shall be periodically reviewed and updated consistent with the requirements and standards established by the Board of Directors and by Health Center management, Federal and State law and regulations, and applicable accrediting and review organizations.

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.524

This policy/ procedure shall be periodically reviewed and updated consistent with the requirements and standards established by the Board of Directors and by Health Center management, Federal and State law and regulations, and applicable accrediting and review organizations.

Policy Title: Amendment of Protected Health Information
Policy Number: 7.19
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

An individual has the right to request an amendment of the Protected Health Information (PHI) collected and maintained about them in their designated record set, except in the following set of circumstances:

1. The information the patient is requesting to amend was not created by Katy Trail Community Health (KTCH), unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
2. The information is not part of the designated record set.
3. The information is accurate and complete.
4. The information would not be available for inspection as provided by law, and is, therefore, unamendable. This exception applies to the following:
    a. Psychotherapy notes (notes created by a mental health professional and that are kept separated from the rest of the medical record).
    b. Information compiled in anticipation of a legal proceeding.
    c. Information used in the course of research with treatment, provided that the individual has agreed to that restriction.
    d. Information received from someone else under a promise of confidentiality.

II. GUIDELINES:

Amendment Process-

1. *Patients may request to have their PHI amended by submitting a Request for Correction/Amendment of Protected Health Information Form along with a detailed written request of what they are requesting to be corrected/amended to the Privacy Officer, who shall be responsible for ensuring that the request is properly clarified (if necessary) investigated, and responded to in a timely and appropriate manner.*
2. The Privacy officer will confirm identity of requestor or legal representative. If requestor is legal representative, ask for legal proof of their representation status, copy, and place in the chart, unless this documentation is already in the chart.
3. The Privacy Officer has the authority to amend or correct any PHI that is determined to be a routine revision and would not require a review from a KTCH medical staff member (i.e. patient's name is spelled incorrectly). If an amendment request requires further investigation by a KTCH medical staff member, the Privacy Officer, shall forward the request for amendment to the KTCH Chief Operating Officer (COO).
4. The COO is responsible for reviewing all amendment requests sent by the Privacy Officer for non-routine corrections and amendments to PHI. The COO will determine whether the provider(s) associated with the PHI under review are currently with

KTCH. If so, the COO will forward the request for amendment to the KTCH provider(s) and await a decision by the provider(s) on the request. If the provider(s) are no longer at KTCH, the COO will appoint the Chief Medical/Dental Officer to review the request.

5. If a request for amendment is accepted, the patient will be notified of a specific date that the records will be amended (within 30 days).
    a. If KTCH is unable to act within 30 days, an extension of no more than 30 days may be used if the requestor is notified in writing stating the reason for the delay and the date by which the holder of the medical record will respond to the request.
6. If the originator of the record (provider/physician or billing specialist) agrees with the request for
Amendment:
    a. The originator will amend the record within the EMR/EDR or billing system.
    b. The Privacy Officer will notify the patient/legal representative of the agreement to amend the record and that the amendment has been made.
    c. KTCH must make reasonable efforts to inform and provide the amendment within a reasonable time, to:
        - Persons identified by the individual as having received PHI about the individual and needed the amendment; and
        - Person(s), including business associates, that KTCH knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to detriment of the individual.
7. If the originator denies the request for amendment:
    a. The Chief Medical/Dental Officer (for medical/dental records) or Chief Financial Officer (for billing records) will be notified.
    b. The patient/legal representative that requested the amendment will receive a timely notification of the denial, in whole or in part. The denial must use plain language and contain:
        - The basis for the denial, which must be one of the four permissible grounds described above.
        - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.
        - A statement that, if the individual does not submit a statement of disagreement, the individual may request that KTCH provide the individual's request for amendment and the denial with any future disclosures of PHI that is subject of the amendment; and
        - A description of how the individual may complain to KTCH or the Secretary of the U.S. Department of Health and Human Services (HHS) in accordance with KTCH's Privacy Complaint Process.

Statement of Disagreement-

- KTCH must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. KTCH may reasonably limit the length of a statement of disagreement.
- KTCH may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, a copy of the rebuttal must be provided to the individual who submitted the statement of disagreement.
- KTCH must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set.

Post-Denial Requirements for Future Disclosures-

- If a statement of disagreement has been submitted by the individual, KTCH must include the patient's request for an amendment, the denial of the request, the patient's statement of disagreement and the rebuttal, if any, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
- If the individual has not submitted a written statement of disagreement, KTCH must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.
- When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, KTCH may separately transmit the material required to the recipient of the standard transaction.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.526

Policy Title: Accounting of Disclosure of Protected Health Information
Policy Number: 7.20
BOD Approval: 12/2009
Effective Date: 05/2008
Responsibility: All Staff
Distribution: All Departments

I. POLICY:

All release of information will be kept in the patient's medical record. Individuals shall have the right to receive an accounting of PHI disclosures made by Katy Trail Community Health (KTCH) in the six years prior to the request or three years prior to the request for any disclosures used for treatment, payment, and healthcare operations. The accounting shall also include a listing of business associates acting on behalf of KTCH. KTCH is not required to account for any disclosures that occurred prior to the compliance date of April 14, 2003.

A log will be kept with an accounting of all disclosures of protected health information (PHI). This accounting log will be kept for six years from the date the request was made. The accounting log will include the following:

1. Patient name.
2. Date of disclosure.
3. Name of entity or person who PHI was released to (notating if address, phone number, and fax number are available on request).
4. Purpose of disclosure.
5. Description of the PHI released
6. Means of how the PHI was sent to the requesting facility
7. Name of employee releasing the PHI

Individuals shall also have the right to request an access report cataloguing any access to ePHI (electronic PHI) regardless of whether the access is for use or disclosures, out of a designated record set for any purpose over the preceding 3 years.

II. GUIDELINES:

Right to an Accounting of Disclosures-

All disclosures (excluding disclosures for treatment, payment, and healthcare operation purposes):

KTCH is required to provide the individual or the individual's legal representative with a written accounting that, except as otherwise provided, includes disclosures of PHI that occurred during the six years (or shorter time period, if requested) prior to the date of the request.

All disclosures made for treatment, payment, and healthcare operation purposes:

KTCH is required to provide the individual or the individual's legal representative with a written accounting that, except as otherwise provided,

includes disclosures of PHI for TPO purposes that occurred during the three years (or shorter time period, if requested) prior to the date of the request.

Content Standard-

For each disclosure, the accounting must include:

- The date of the disclosure.
- The name of the entity or person who received the PHI and, if known, the address of such entity or person.
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of the written request for disclosure, if any.

If KTCH has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

- The information required above.
- The frequency, periodicity, or number of the disclosures made during the time period; and
- The date of the last such disclosure during the accounting period.

If KTCH has made a disclosure to a business associate acting on behalf of the organization, KTCH will provide:

- The name of the business associate; and
- A brief description of the PHI disclosed.

When available the following contact information for the business associate must also be provided:

- The address of the business associate.
- The phone number of the business associate.
- The email address of the business associate; and
- Any other contact information.

Accounting of Access:

KTCH is required to provide the individual or the individual's legal representative with a written accounting that catalogues any access to ePHI regardless of whether the access is for use or disclosure, out of a designated record set for any purpose over the preceding 3 years prior to the request.

Content Standard:

For each access, the accounting of access must include:

- User who made the access
- Date (and if available, time) the access was made
- Type of access made (i.e. view, update, print, delete, etc…)

A brief description of what data was accessed **Compliance Standards-**

KTCH must act on the individual's request for an accounting no later than 60 days after receipt of the request, as follows:

- Provide the individual with the accounting requested; or
- If KTCH is unable to provide the accounting with the 60-day period, it may extend the time to provide the accounting by no more than 30 days, provided that:
    - KTCH, within the 60-day time limit, provides the individual with a written statement of the reasons for the delay and the date by which KTCH will provide the accounting; and
    - KTCH may have only one such extension of time for action on any request for an accounting.

KTCH must provide the first accounting to an individual in any 12-month period without charge. KTCH may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that KTCH informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Documentation for Accounting of Disclosures-

KTCH medical records personnel shall account for disclosures by documenting any such disclosures in the *"Accounting of Disclosures"* spreadsheet that is saved in a protected folder on the public KTCH drive. A copy of the request (verbal or written) will be saved in the patient's medical record.

The Privacy Officer shall be responsible for receiving and processing requests for an accounting of disclosures. The Privacy Officer must document and maintain a copy of the following:

- A copy of the written accounting/access report that is provided to the individual requesting the accounting.
- The original request from the individual requesting the accounting of disclosure and/or access report.

Exceptions to the Right to an Accounting of Disclosures-

In an accounting of PHI, KTCH is not required to account for the following disclosures:

- To individuals requesting their own PHI.
- Incidental use or disclosure made during an otherwise permitted or required disclosure.
- For national security or intelligence purposes (see C.F.R. § 164.512(k)(2));
- To persons involved in the individual's care or other notification purposes (see C.F.R. § 164.510);
- To law enforcement officials (see C.F.R § 164.512(k)(5));
- As part of a limited data set (see C.F.R. § 164.512(e));

- That occurred prior to the date of April 14, 2003 compliance date

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.528

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Printing and Copying of PHI
BOD Approval: 09/2013
Responsibility: All staff

Policy Number: 7.21
Effective Date: 08/2013
Distribution: All Departments

I. POLICY:

Katy Trail Community Health and it's staff will protect all forms of patient confidentiality including printed and copied materials.

II. GUIDELINES:

Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise.

- PHI printed should be promptly removed by the user.
- PHI in hardcopy format must be disposed of in accordance with the KTCH's record retention schedule and policy on Disposal of PHI.
- Printers and copiers that are using for printing PHI should be in a secure location. If the equipment is in a non-secure location, the information being printed or copied is required to be strictly monitored.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.530(c)(1)

This policy/ procedure shall be periodically reviewed and updated consistent with the requirements and standards established by the Board of Directors and by Health Center management, Federal and State law and regulations, and applicable accrediting and review organizations.

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Faxing of Protected Health Information
BOD Approval: 12/2009
Responsibility: All staff

Policy Number: 7.22
Effective Date: 12/2009
Distribution: All Departments

I. POLICY:

It is the policy of Katy Trail Community Health (KTCH) to ensure confidentiality in facsimile transmission of protected health information (PHI).

II. GUIDELINES:

Medical records/PHI can be faxed for medical treatment, payment, and healthcare operations, i.e. doctors, hospitals, laboratories, third party payers. Fax will not be used for routine release of information to insurance companies, attorneys, or other non-health entities when served effectively by regular mail.

- PHI will be sent by facsimile only when the original record or mail delivered copies will not meet the needs. For example, personnel may transmit the PHI by facsimile when urgently needed for patient care or required by a third-party payer for ongoing certification of payment for a patient.

Information transmitted must be limited to the minimum necessary to meet the requester's needs.

Except as authorized by the individual's consent to treatment, payment, or healthcare operations (TPO), or federal or state law, a properly completed and signed authorization must be obtained for releasing PHI (see General Uses and Disclosures policy).

The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization, unless required by law.

- Confidential details of:
  - Psychotherapy
  - Other professional services of a licensed psychologist
  - Social work counseling/therapy
  - Domestic violence victims' counseling
  - Sexual assault counseling (42 CFR Part 2)

The Facsimile Cover Letter must be used to send faxes containing PHI. The is a printable Facsimile Cover Letter located on the shared KTCH public drive, as well as built in the facsimile section(s) of the EMR.

Personnel must take reasonable efforts to ensure that they send the facsimile transmission to the correct destination including:

- Preprogramming frequently used numbers into the machine to prevent misdialing errors.
- Periodically and/or randomly checking all speed-dial numbers to ensure their accuracy, validity, and authorization to receive confidential information.
- For a new recipient, the sender must verify the fax number by requesting the recipient; the sender must verify the fax number of the recipients of PHI to notify KTCH if their fax number is to change.

Once a facsimile transmission is completed, the document must be date and time fax stamped. The sender must initial the stamp.

Procedures for Misdirected Faxes (for both TPO and non-TPO purposes)-

If a fax transmission containing PHI is not received by the intended recipient because of a misdial, check the internal logging system of the fax machine to obtain the misdialed number.

If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed.

If the recipient cannot be reached by phone, a fax informing that a misdirected fax was sent should be directed to the recipient requesting that the entire content of the misdirected fax be destroyed.

The sender of the misdirected fax is responsible for forwarding the Letter for Misdirected Fax and the fax confirmation sheet or activity report of its transmittal to the Privacy Officer.

Misdirected faxes will be recorded on the Accounting of Disclosures log by the Privacy Officer, as described in the policy on Accounting for Disclosures.

Incoming faxes for clinical reasons or containing PHI should be directed to the internal EMR secure fax server. If this is not possible and the PHI must be directed to a "hard fax machine" the receiving party should:

- Immediately remove the fax transmission from the fax machine and deliver as appropriate.
- Manage PHI received as confidential in accordance with this policy.
- Destroy, or follow sender's instructions for patient information faxed in error and immediately inform the sender.

Enforcement-

The Privacy Officer, or in his/her absence, the Chief Operating Officer are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.530

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Paper PHI
BOD Approval: 09/2013
Responsibility: All staff

Policy Number: 7.23
Effective Date: 06/2013
Distribution: All Departments

I. POLICY:

Patients seen prior to April 1, 2009 have a paper medical record containing PHI that will be maintained according to the record retention policy.

II. GUIDELINES:

1. Storage-
All paper medical records containing PHI will be stored in an offsite locked storage facility.

2. Access-
Should PHI contained in a paper chart be requested, the only persons having access to the locked storage unit are the privacy officer and the medical records staff. Information from the paper chart may be scanned into the EHR by medical records staff, should this information be requested by a health care provider or his/her designee at any KTCH location. Should information from the paper chart be requested by an outside person(s) including the patient, a copy will be made of the PHI for the person(s) requesting the record. All original PHI will be maintained within the paper record.

3. Transportation-
When transporting paper PHI between the storage facility and the clinical facility, the record will be kept in a locked brief case until the PHI is inside the secure facilities. View privacy policy, "Transporting PHI".

Policy Title: Transporting PHI
BOD Approval: 09/2013
Responsibility: All staff

Policy Number: 7.24
Effective Date: 07/2013
Distribution: All Departments

I. POLICY:

The intention of this policy is to prevent the unauthorized disclosure of PHI as a result of transporting PHI between outside storage and the clinical facility. The logging of removal or transportation of records must be undertaken because it will assist with tracking unauthorized disclosures. Only approved medical records staff will have access to this specific storage facility when approved by the Privacy Officer each time.

II. GUIDELINES:

- When an approved request for medical records/PHI is obtained by the facility and records older than April 1, 2009 are requested, the medical records staff will verify the following:
    1. If the paper records have already been scanned into the EMR
    2. If the paper records have already been scanned onto a disk
        a. This list is in a protected folder on the p://drive, only available to medical records staff.
- If the records are in neither of these two places, the medical records staff will request to obtain the chart from the storage unit. The request will be made to the Privacy Officer. Except in emergency situations, access to the storage until will only be approved for Tuesdays and Fridays of every week. In emergency situations, only the Privacy Officer will be approved access the storage unit.
- If approved, a logging record must be made that includes:
    1. Date & time
    2. Chart number
    3. Reason for needing this PHI
    4. Person(s) possessing the information
- The key to the storage facility will be kept in a lock box at all times. The only person with access to this key is the Privacy Officer. The Privacy Officer must review and sign off on the logging records before the key will be removed from the lock box.
- PHI will only be transported in a personal motor vehicle and only current KTCH employees will be allowed in the personal motor vehicle. All employees in the personal motor vehicle containing PHI must be "clocked-in" or salaried.
- The information must be placed in the KTCH locked briefcase until the employee is secured inside the storage facility or the clinical facility. The locked briefcase should always be kept on the floor of the car, out of general view.
- If at any time there is PHI in the personal motor vehicle, the employee must go directly between the clinical facility and the storage unit. No other stops will be approved; this

includes drive-thru, restaurants, gas stations, hospitals, government agencies, etc. No exceptions will be made to this rule.

Enforcement-

The Privacy Officer, or in his/her absence, the Chief Operating Officer are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Disposal of PHI
BOD Approval: 09/2013
Responsibility: All staff

Policy Number: 7.25
Effective Date: 08/2013
Distribution: All Departments

I. POLICY:

KTCH has a duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethnics, and accreditation requirements. PHI may only be disposed of by means that assure that it will not be accidentally released to an outside party. Managers must assure that appropriate means of disposal are reasonably available and operational. This policy defines the guidelines and procedures that must be followed when disposing of information containing PHI.

All personnel must strictly observe the following standards relating to disposal of hardcopy and electronic copies of PHI:

- PHI must not be discarded in trash bins, unsecured recycle bags or other publicly-accessible locations. Instead this information must be shredded or placed in a secure recycling container.
- Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.

It is the individual's responsibility to ensure that documents have been secured or destroyed. It is the supervisor's responsibility to ensure that employees are adhering to this policy.

II. GUIDELINES:

KTCH management shall provide users with access to shredders or secured recycling containers for proper disposal of confidential documents containing PHI. The user may elect to use either shredding or secure recycle containers for the destruction is in accordance with this policy.

Shredders or secured recycling containers should only be filled to their maximum capacity and should never be "over flowing". If all secured recycling containers in the entire building are filled to their maximum capacity the Privacy Officer should be notified so that the shredding company can be requested make an exception trip to empty the containers or other arrangements can be made.

To ensure that it is in fact performed, KTCH has hired a bonded destruction service to carry out the destruction of PHI. KTCH will keep an up to date contract and business associate agreement with the shredding company.

Enforcement:

All supervisors are responsible for enforcing this policy. Federal regulations require that individuals who violate this policy shall be subject to sanctions.

III. REFERENCES

Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.530(c)(1)

KATY TRAIL COMMUNITY HEALTH
Privacy Policies

Policy Title: Security Auditing Protocol
BOD Approval: 12/15/2016
Responsibility: All staff

Policy Number: 7.26
Effective Date: 09/26/2016
Distribution: All Departments

I. POLICY:

It is the goal of Katy Trail Community Health (KTCH) to perform security audits using audit trails and audit logs that offer a back-end view of system use. Audit trails and logs record key activities, showing system threads of access, modifications, and transactions. The HIPAA Security Rule includes a provision that requires healthcare organizations to perform security audits

II. GUIDELINES:

Performance of periodic reviews of audit logs will be useful for:

- Detecting unauthorized access to patient information
- Establishing a culture of responsibility and accountability
- Reducing the risk associated with inappropriate accesses (Note: Behavior may be altered when individuals know they are being monitored)
- Providing forensic evidence during investigations of suspected and known security incidents and breaches to patient privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied
- Tracking disclosures of PHI
- Responding to patient privacy concerns regarding unauthorized access by family members, friends, or others
- Evaluating the overall effectiveness of the organization's policy and user education regarding appropriate access and use of patient information (Note: This includes comparing actual workforce activity to expected activity and discovering where additional training or education may be necessary to reduce errors)
- Detecting new threats and intrusion attempts
- Identifying potential problems
- Addressing compliance with regulatory and accreditation requirements

PROCEDURE(S):

The audit reports will be ran directly from the EHRs on a monthly basis. A team (Privacy Officer, Chief Operating Officer, and Dental Clinical Coordinator) will review the data paying special attention to:

- Employees accessing their own records
- Employees accessing records of their own family
- Employees accessing records of other employees
- Employees accessing "celebrity" charts
- Employees accessing records of "specially protected" records (including CFR 42, part 2—psychiatry, drug/alcohol abuse, HIV/AIDS—and minors seen as adults).

Each month, two reports will be ran from each EHR. These reports will be:

- A report of all touches from all employees on a specific day during the month
- A report of one medical employee and one dental employee for all touches in a given week.
    - The employee will be randomly selected. Admin personal will be included among medical and dental staff, depend on job duty.

The results of each audit will be saved in a secured folder on the pdrive, stating the date of the audit, any potential findings that may have been discovered, and any follow up.

III. REFERENCES

This provision is found in Section 164.308(a)(1)(ii)(c) – "Information system activity review (required), which states organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."