Knox County Community Health Center

Patient Healthcare Information Privacy Policies and Procedures

Adopted: August 2023

Revisions/Updates:

_____

_____

_____

_____

_____

_____

HIPAA PRIVACY POLICIES & PROCEDURES

This packet includes the following HIPAA policies, procedures, and model forms:

HIPAA GENERAL OPERATING POLICY

POLICY:

This HIPAA Privacy Compliance Plan is adopted by Knox County Community Health Center (hereinafter referred to as the "Center") as part of our commitment to comply with all applicable laws and regulations enacted by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and each of its subsequent enactments, amendments, and interpretations, including the HITECH Act and 42 CFR part 2 (or "Part 2"), and all laws governing the confidentiality of substance use disorder patient records, as a part of our overall mission. This plan is intended to assist our organization to offer industry best practices for the privacy, confidentiality, and maintenance of Protected Health Information ("PHI").

Privacy Officer

The Center shall designate a Privacy Officer who will be responsible for the development and implementation of HIPAA policies and procedures and oversee the Center's and employees' compliance with the HIPAA Privacy Rule.

Policies and Procedures

The Privacy Officer shall draft HIPAA policies and procedures to protect the patient's PHI from improper use or disclosure by the Center. Changes to these policies and procedures are strictly prohibited without prior written consent of Center legal counsel.

Notice of Privacy Practices

The Center shall provide a copy of its "Notice of Privacy Practices" to all patients as described in the Notice of Privacy Practices Policy.

Authorizations

Except for as specified in the Center's policies and procedures, a patient's authorization on a HIPAA compliant Authorization Form is required to use or disclose a patient's PHI.

Treatment, Payment, & Health Care Operations

The Center shall implement policies and procedures consistent with the HIPAA Privacy Rule and 42 CFR part 2 allowing for the use and disclosure of PHI for treatment, payment, or health care operations when appropriate.

Business Associates

The Center shall have business associate agreements in place with all persons or entities that provide services for the Center and, in doing so, will need access to, or may create, health information regarding patients ("Business Associates").

Training

The Center shall train all members of the Center's workforce on the HIPAA Privacy Rule requirements and its policies and procedures related to the privacy of a patient's PHI annually. New employees will receive HIPAA training as part of their employee orientation.

Safeguards

The Center shall have appropriate administrative, technical, and physical safeguards in place to reasonably safeguard a patient's PHI from intentional or unintentional unauthorized use or disclosure.

Mitigation

The Center shall mitigate, to the extent feasible, any known harmful effect resulting from a use or disclosure of PHI in violation of this policy or HIPAA requirements, by itself or a Business Associate.

Complaints & Reporting

The Center shall implement a policy and procedure giving individuals the ability to make complaints concerning potential violations of their privacy rights and providing workforce members with a process for reporting potential privacy violations.

Sanctions

The Center shall discipline workforce members of the Center who fail to comply with this policy, the HIPAA Privacy Rule, the HIPAA Security Rule, and related policies and procedures.

Minimum Necessary

The Center shall make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary amount to accomplish the purpose of the use, disclosure, or request.

Access, Amendments & Accountings

The Center shall implement policies and procedures to allow individuals access to their PHI for inspection and/or copying, to make amendments to their medical record, and to receive an accounting of the disclosures of their PHI.

Definitions

In addition to the definitions contained herein, any capitalized terms that are defined under HIPAA, whether or not defined separately in this policy, also have the meaning defined under HIPAA or 42 CFR part 2. The following terms also have the meaning ascribed to them below:

Disclosure means the communication of any information identifying a patient as being or having been diagnosed with a substance use disorder, having or having had a substance use disorder, or being or having been referred for treatment of a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person.

Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services, and auditing functions, business planning and development, and general business and administrative activities.

HIPAA for purposes of this Compliance Plan, "HIPAA" encompasses the Health Insurance Portability and Accountability Act of 1996, as amended, including the HITECH Act, the HIPAA Privacy Rule and HIPAA Security Rule, and the federal statutes and regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, as codified at 42 USC § 290dd-2, and the regulations thereunder, codified at 42 CFR § 2 *et seq.*

HIPAA Privacy Rule means the provisions the Health Insurance Portability and Accountability Act of 1996, as amended, ("HIPAA") regarding appropriate safeguards to protect the privacy of PHI, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization, found in 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule means the provisions of HIPAA regarding appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI, found in 45 CFR Part 160 and Subparts A and C of Part 164.

Minimum Necessary means the minimum necessary amount of a patient's PHI to accomplish the purpose of the use, disclosure, or request.

Patient means any individual who has been treated, diagnosed, or referred for services by the Center for the purposes of HIPAA. Patient means any individual who has applied for or been given diagnosis, treatment, or referral for treatment for a substance use disorder at a Part 2 program for the purposes of Part 2. Under Part 2, patient further extends to any individual who, after arrest on a criminal charge, is identified as an individual with a substance use disorder in order to determine that individual's eligibility to participate in a Part 2 program. This definition includes both current and former patients.

Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations, and utilization review.

Personal Representative means a person who has the authority under applicable law to make health-care related decisions for an individual.

Psychotherapy notes are notes by a health care provider who is a mental health professional documenting his or her discussions with the patient during a counseling session that *are separated from* the rest of the patient's medical record. These notes generally capture the therapist's impressions.

Protected Health Information ("PHI") means information that is created or received by Center and identifies an individual, is transmitted or maintained in any form, and is protected from improper use or disclosure under the HIPAA Privacy Rule.

Substance use disorder ("SUD"), as it relates to Part 2, means a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal.

Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care. This definition also includes the care of a patient suffering from a substance use disorder, a condition which is identified as having been caused by the substance use disorder, or both, in order to reduce or eliminate the adverse effects upon the patient.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Withdraw management, for purposes of Part 2, means the use of pharmacotherapies to treat or attenuate the problematic signs and symptoms arising when heavy and/or prolonged substance use is reduced or discontinued.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Center, is under the direct control of the Center regardless of whether they are paid by the Center.

AUTHORIZATION TO USE OR DISCLOSE HEALTH INFORMATION

POLICY: Except for uses and disclosures of health information as allowed under HIPAA, 42 CFR Subpart D, 42 CFR part 2, ORC § 5119.28, these policies and procedures, and as described within the Center's Notice of Privacy Practices, the Center shall obtain a HIPAA Authorization Form signed by the patient or his or her legal representative before using or disclosing the individual's PHI.

PROCEDURE:

1. Authorization Needed. Complete the HIPAA Authorization for Release of Information form ("Authorization") before using or disclosing a patient's health information for reasons other than those uses and disclosures allowed under HIPAA, 42 CFR Subpart D, ORC § 5119.28, and these policies and procedures and as described within the Center's Notice of Privacy Practices.

   For PHI and other information protected by 42 CFR part 2, the standard Authorization form is not sufficient for purposes of releasing protected information. As such, complete the Authorization for Release of SUD Information Pursuant to 42 CFR part 2 before using or disclosing a patient's health information for reasons other than those permissible uses and disclosures. Under federal law, the Authorization for Release of SUD Information Pursuant to 42 CFR part 2 must be accompanied by the Notice to Prohibit Redisclosure.

2. Psychotherapy Notes. An authorization is also needed to release psychotherapy notes, except as follows:

   a. For the use by the originator of the notes.

   b. Use or disclosures by the Center in training programs in which trainees in mental health learn to improve their counseling skills.

   c. Use to defend a legal action brought by the patient who is the subject of the notes.

   d. When required by the Secretary of Health and Human Services.

3. Disclosures to Agencies. The custodian of the patient's records must attempt to obtain the patient's consent before disclosing information to the ADAMH Board to provide services for patients involuntarily committed to other hospitals within ODMH, and to the Department of Rehabilitation & Correction.

4. Form Requirements. The respective "Authorization for Release of Information" forms contain language required by the HIPAA Privacy Rule & 42 CFR part 2. Thus, it may not be revised without consulting legal counsel. The forms must be completed in its entirety, dated, and signed by the patient or his or her legal representative.

   a. You must provide a copy of the signed authorization to the patient/legal representative.

   b. The authorization form may not be combined with another document.

   c. A patient may revoke his or her authorization at any time in writing. When the authorization is revoked, you must stop making further uses and disclosures pursuant to the authorization.

   d. Federal regulations require that you retain signed authorization forms for at least seven (7) years from the date signed, or the date last in effect, whichever is later.

e. You cannot deny a patient treatment on the basis of his or her refusing to sign an authorization.

f. For purposes of information and records protected by 42 CFR part 2, any information and/or records released following lawful and compliant completion of the "Authorization for Release of SUD Information Pursuant to 42 CFR Part 2" must be accompanied by the "Notice of Prohibited Redisclosure of SUD Information Pursuant to 42 CFR Part 2."

5. No Authorization Needed.

You do not need a patient's authorization for the following uses or disclosures pertaining to the identity, diagnosis, or treatment of any person seeking or receiving services that are maintained in connection with the performance of any Part 2 drug treatment program:

a. Disclosures among providers who are treating co-occurring mental health and substance use disorders within the same entity, when such information is shared for legitimate treatment, payment, or health care operations.
b. Disclosures to a researcher, or for research purposes, so long as the research project meets the research requirements in the HIPAA Privacy Rule or the Health and Human Services regulations regarding the protection of human subjects, as applicable. Redisclosure of protected information is not permissible under these circumstances.
c. Disclosures to qualified personnel (including authorized governmental agencies, HIPAA-covered entities or business associates) for the purpose of conducting management, financial audits, or program evaluation. However, the personnel may not identify, directly or indirectly, any individual person in any report of the research, audit, or evaluation. Under 42 CFR part 2, the qualified personnel may not copy or remove patient records from the premises.
d. There is no blanket authorization for SUD information to be used or disclosed for public health purposes; however, there are exceptions in the case(s) of: reporting vital statistics; investigating cause of death; and reporting child abuse or neglect as discussed further below.
e. Disclosures to a court of competent jurisdiction may be permissible under certain circumstances and pursuant to a valid, compliant court order. The court must limit disclosure to those parts of the patient's record considered to be essential, require that all information be disclosed in chambers if necessary, and include all other measures necessary to keep disclosure to a minimum. For disclosures to investigate or prosecute, warrants and subpoenas are not sufficient to compel disclosure of Part 2 protected records.
f. Disclosures for the purposes of reporting a crime are permissible under limited circumstances including when the crime occurs at the Part 2 program or against the Part 2 program's staff. Information disclosed must be limited as provided in 42 CFR 2.12(c)(5).
g. Disclosures to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained. Documentation pursuant to this disclosure should include who made the disclosure, who received the information, when information was disclosed, and the reason information was disclosed.
h. Disclosures required by federal or state law, including disclosure of child abuse or neglect. However, the restrictions continue to apply to the original substance use disorder patient records maintained by the part 2 program including their disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect.

In cases of a patient's mental health or other health information not related to their status as an alcohol or drug user, you do not need a patient's authorization for the following uses:

a. Disclosures required to obtain payment for goods and services provided to the patient from third-

party payers and insurers responsible for processing and authorizing payment. The Center must attempt to get permission from the patient before disclosure in this case.

b. Disclosures required by federal or state law, including disclosure of child abuse or neglect.
c. Disclosure pursuant to a court order signed by a judge.
d. Disclosures for public health activities and health oversight activities.
e. Disclosures to authorities for abuse, neglect, and domestic violence.
f. Disclosures to the executor or the administrator of an estate of a deceased person when necessary to the administration of the estate.

Because the Center may not exclusively provide SUD treatment but, instead, may provide mental health services as well, the applicability of 42 CFR part 2 will depend on the services rendered on a case by case basis. 42 CFR part 2 applies to patient records which pertain to SUD services. This includes, however, records that demonstrate co-occurring mental health and SUD treatment. However, 42 CFR part 2 will not apply to information only pertaining to mental health services.

6. Minor Patients.

In Ohio, minors may give consent for the diagnosis or treatment of any condition which it is reasonable to believe is caused by drugs, beer, or liquor by a licensed physician. If a minor patient acting alone has the legal capacity under state laws to seek and obtain substance use disorder treatment, written consent for disclosure may only be given by the patient. Under federal law, relevant facts to reducing a substantial threat to life or physical well-being of a minor applicant may be disclosed to a parent or guardian if the Center Director judges that the minor lacks capacity to grant disclosure consent due to extreme youth, mental or physical conditions, or the minor applicant's situation poses a substantial threat to the life or physical well-being of the minor applicant or another individual.

KNOX COUNTY HEALTH CENTER
11660 Upper Gilchrist Road, Mount Vernon, OH 43050

MEDICAL RECORDS RELEASE FORM

NAME OF PATIENT_____ DOB_____

ADDRESS_____

CITY_____STATE_____ZIP_____

RELEASE OF RECORDS FROM:	RELEASE OF RECORDS TO:
_____	_____
NAME OF PHYSICIAN	NAME OF PHYSICIAN
_____	_____
NAME OF HEALTH CARE FACILITY	NAME OF HEALTH CARE FACILITY
_____	_____
ADDRESS	ADDRESS
_____	_____
CITY, STATE, ZIP	CITY, STATE, ZIP

INFORMATION TO BE RELEASED:

(CIRCLE ONE) MEDICAL, DENTAL, BEHAVIORAL RECORDS

_____LAB REPORTS
_____ER/URGENT CARE REPORTS
_____IN PATIENT RECORD
_____IMMUNIZATION RECORDS
____DIAGNOSTIC IMAGING
____OUTPATIENT RECORDS
____OTHER (SPECIFY) _____

List other facilities records to be included when releasing for the purpose of continuing medical care: _____
_____.

Purpose or need for disclosure (check applicable categories)

_____Further medical care
_____Application for insurance
_____Disability determination
_____Payment of insurance claim
_____Vocational rehabilitation evaluation
_____Legal investigation
_____Personal
_____Other

I understand that this authorization shall be valid for one (1) year unless revoked through written notice to the Knox County Health Department Clinic.

I AUTHORIZE RELEASE OF MY MEDICAL RECORDS IN ACCORDANCE WITH THE SPECIFICATIONS LISTED ABOVE. I UNDERSTAND WRITTEN NOTICE IS NECESSARY TO CANCEL THIS REQUEST.

SIGNATURE OF PATIENT_____DATE_____

If signed by a legal representative, please provide your relationship to the patient (i.e. guardian, power of attorney, executor) and any required documentation to support this relationship.

Signature of witness _____Date _____

Behavioral Health Authorization for Release of Information

11660 Upper Gilchrist Road, Mount Vernon, Ohio 43050
740-399-8008 ● FAX 740-399-8012

Client Name: _____ Date of Birth: _____
First Name MI Last Name

I Authorize the Knox County Community Health Center (KCCHC) to:
□disclose to, □receive from, or □exchange with

_____
(Organization/ Individual to Whom Disclosure providing TO) (Primary Contact/ Relationship)

_____
(Street Address) (City) (State) (Zip Code)

_____ _____
(Telephone) (Fax Number)

Purpose of Disclosure:

☐Continuity of care/coordination of treatment, ☐To invite to a family program, ☐Feedback/Follow-up to referral source

☐At the request of client, ☐Assistance in evaluation and treatment, ☐Other purposes:_____

Type of Information to be Disclosed: Mental Health (MH) / Substance Use Disorder (SUD)

MH *I* SUD: (Copies of Record)
- ☐ ☐ Diagnostic Assessment
- ☐ ☐ Treatment Plans
- ☐ ☐ Progress Notes
- ☐ ☐ Discharge Summary

MH / SUD
- ☐ ☐ Clinical Interpretive Summary
- ☐ ☐ Treatment Dates/Attendance/Compliance
- ☐ ☐ Progress in Treatment
- ☐ ☐ Other: _____

MH / SUD
- ☐ ☐ Diagnosis
- ☐ ☐ Recommendations
- ☐ ☐ Urinalysis Results

Amount of Information to be Disclosed: Information will be released from the most recent or current treatment episode to the agency unless otherwise noted: ☐ Other (specify dates or time frame)_____

Authorization: I hereby authorize disclosure of information as designated above. This authorization has been explained to me and I understand that my information cannot be disclosed without my expressed written consent unless otherwise provided for in law or regulations.
Revocation: I also understand that this release can be revoked by me at any time except to the extent that the program which is to make the disclosure has already taken action in reliance on it. If not previously revoked, this consent will terminate in one year from date of execution of this Authorization.

I will not be denied services if I refuse to sign this. Having read the above, I understand and agree to all terms.

Signature of Client: _____ Date: _____

If applicable, Signature of Parent/Legal Guardian: _____ Date: _____

Witness: _____ Date: _____

Prohibition Against Redisclosure: This information has been disclosed to you from records protected by federal confidentiality rules. The federal rules prohibit you from making any further disclosure of this information unless further disclosure: is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The federal rules restrict any use of Information to criminally investigate or prosecute any alcohol or drug abuse client. Drug abuse patient records are also protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR , parts 160 and 164.

STAFF USE ONLY:
Consent was revoked by client on: _____ Staff signature/date:_____

Knox County Community Health Center
Notice of Prohibited Redisclosure of SUD Information Pursuant to 42 CFR Part 2

This record, which has been authorized for disclosure pursuant to 42 CFR Part 2, is protected by federal confidentiality rules and regulations including, in relevant part, the Health Insurance Portability and Accountability Act of 1996 including HIPAA Part 2 (42 CFR part 2). Federal law prohibits the recipient of this record from making any further disclosures of this record unless further disclosure is expressly permitted by the written consent of the individual to whom this record pertains, or is otherwise permitted by 42 CFR part 2.

A general authorization for the release of medical records is not sufficient for purposes of satisfying the requirements under 42 CFR part 2.

Federal law restricts any use of this record, including any information contained therein, for the purpose of investigating and/or prosecuting any crime related to any patient with a substance use disorder, as defined by 42 CFR part 2, except as provided therein.

RIGHT TO ACCESS AND/OR COPY HEALTH INFORMATION

POLICY: The Center shall afford individuals the right to access, inspect, and obtain a copy of their health information in accordance with the provisions of the HIPAA Privacy Rule as well as, where applicable, 42 CFR part 2.

PROCEDURE:

1. Request for Access and/or Copying Form. An individual (or their authorized representative) who seeks to access and/or copy his or her health information, must complete the form entitled "Request to Access and/or Copy Health Information" and submit it to the Privacy Officer. The individual can obtain the form from the Privacy Officer.

   The completed form should be forwarded to the Privacy Officer, who will then decide whether to grant or deny the individual's request in accordance with the rules set forth in this policy.

2. The Privacy Officer shall respond to the request within thirty (30) days. The Privacy Officer may extend the deadline once for no more than thirty (30) days by providing the patient with a written statement of the reasons for the delay and the date in which the Privacy Officer will complete the request.

   The Privacy Officer will notify the individual of where to direct his or her request for access if the Center does not maintain the information sought but knows where it can be obtained.

3. Granting Access. If the Privacy Officer grants access, he or she will provide the individual with access to the records in the form requested (unless not producible in such a form) and the chance to copy the records. If the individual's health information is maintained electronically and the individual requests an electronic copy of such information, the Center must provide the individual with access to the health information in an electronic form. The Privacy Officer may provide the individual with a summary of the information requested if the individual agrees in advance to this method and the fees associated with the summary.

   Federal law does not prohibit the Center from providing a patient access to their own records, including the opportunity to inspect and copy records; however, the same must be navigated in accordance with the protocols herein.

4. Denying Access

   The patient/legal representative is entitled to written notice of a denial. The patient/legal representative may request a review of some denials, others are not reviewable.

   a. Unreviewable — An individual has no right to access the following information and the Privacy Officer does not have to provide the individual with a chance for review:

      i. Psychotherapy notes.

      ii. Information compiled in anticipation of civil, criminal, or an administrative action or proceeding.

      iii. Health information that is subject to CLIA to the extent the provision of access to the individual would be prohibited by law.

iv. Health information that was obtained from another person (other than a health care provider) under a promise of confidentiality and granting access would likely reveal the source's identity.

b. Reviewable — The Privacy Officer may deny access for the following reasons but must give the individual a chance to seek a review of the denial:

i. A physician chosen by the Center has determined that access is likely to endanger the life or safety of the patient or another individual.

ii. When the health information sought refers to another person and a physician chosen by the Center determines that access is likely to cause harm to that person.

iii. When the request for access is made by a personal representative and a physician chosen by the Center determines that providing access to the representative is likely to cause harm to the patient or another person.

If the patient/legal representative requests a review, a physician chosen by the Center who was not involved in the original denial must determine, within a reasonable period of time, whether the denial was proper and provide written notice of the determination to the requestor.

c. Restricted Access — Pursuant to 42 CFR part 2 (§2.23), the Center disclosed to a patient may be subject to restrictions including the restriction on use of this information to initiate or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patient.

d. Denial Notice — If you deny access *for any reason*, you must provide the patient with a written denial using the form entitled "Response to Request to Access and/or Copy Health Information," which includes (a) the basis for the denial, (b) a statement of the individual's right to have the denial reviewed and how such right may be exercised, and (c) a description of how the individual can file a complaint with the Center and the Secretary of Health and Human Services. The description must include the name (or title) and telephone number of the person or office responsible for receiving complaints.

5. You must document and retain (a) the records that are subject to access and (b) the title of the person or office responsible for processing the request for access for seven (7) years.

6. Restriction on use of information. Information obtained by patient access to his or her patient record is subject to the restriction on use of this information to initiate or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patient as provided for under 42 CFR §2.12(d)(1).

7. Sending Health Information to a Third Party. If an individual's request for access to health information directs the Center to transmit the copy of protected health information directly to another person designated by the individual, the Center must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

REQUEST TO ACCESS AND/OR COPY HEALTH INFORMATION

Please complete the following:

1. Name of Requestor (Print): _____
2. Patient's Name (If Different): _____
3. Patient's Date of Birth: _____
4. Address: _____
5. Phone: _____
6. If you are not the patient, your relationship to the patient: _____
7. Do you wish to ❒ access (e.g. review) the health information, ❒ copy or receive an electronic copy of the health information, or ❒ both.
8. Describe the information you want to access (e.g., payment information, test results, physician notes):
   _____
   _____
9. Identify the date(s) of information you want access to: _____

Do you wish to send your requested health information to a third party? ❒ YES ❒ NO
If YES, where do you wish to send your requested health information?

Third Party's Name: _____

Address: _____

City, State, Zip Code: _____

There is no charge to access your health information. If you would like a copy of the information, we will charge a reasonable fee for the copying, postage, and to prepare a summary (if you request a summary). We will inform you by ❒ phone ❒ letter (pick one) of the cost of your copy before we make the copy and verify that you agree to pay for the copy. We will require you to pay for your copy before you receive it. We will notify you in writing within thirty (30) days of your request if and when your health information will be available for access, where you will need to come to access your health information to read and review it, or where to come to pay for and pick up your copy. We will notify you within thirty (30) days if we need one additional period of thirty (30) days to respond to your request. In specific circumstances, we may deny access to your health information, or to a portion of your health information. If we deny access we will return this form to you with our written reasons for our denial and explain your right to review the denial, if applicable. The Center reserves the right to supervise your access.

Signature of Patient (or Patient's Representative):	Date:
Print Name of Patient (or Patient's Representative):	
If you are the representative of a patient, check the scope of your authority to act on the patient's behalf:	
❒ Power of Attorney ❒ Legal Guardian ❒ Surrogate Decision-Maker ❒ Executor or Personal Representative ❒ Parent ❒ Other: _____	

RESPONSE TO REQUEST TO ACCESS AND/OR COPY HEALTH INFORMATION

Your request to ❒ access, ❒ copy, or ❒ both access and copy your health information is:

❒ **Approved.** Your health information will be available for access on _____ between the times of _____.

❒ A copy of your health information will cost $_____ plus postage if we mail the copy to you. If you wish to have the information mailed to you, please send a check or money order for $_____ to _____. You may save the postage cost by picking up your copy on the date and time listed above. Please bring a check or money order for the copying costs.

❒ **Denied**

❒ Your request was denied because the health information sought includes the following information that is exempt from access. You may not seek a review of the denial.

❒ Psychotherapy notes;

❒ Information that was compiled in anticipation of, or for use in, civil, criminal or administrative legal actions or proceedings;

❒ Health information that relates to the Clinical Laboratory Improvement Amendments of 1988 (CLIA), to the extent that CLIA would prohibit individual access, or other information that is exempt from CLIA.

❒ The health information was obtained from another person (other than a health care provider) under a promise of confidentiality and granting access would likely reveal the source's identity.

❒ Your request was denied because the health information you sought was reviewed by a physician chosen by the Center who determined that the following circumstances exist:

❒ Access is reasonably likely to endanger the life or safety of the patient or another person.

❒ Access is reasonably likely to cause substantial harm to another person.

❒ Access is sought by the patient's legal representative and access is reasonably likely to cause substantial harm to the patient or another person.

If your access request was denied for one of these three reasons, you may seek a review of the decision by submitting a written request for review to the Privacy Officer. The Privacy Officer will provide you a written answer within thirty (30) days.

❒ **Extension of Deadline.** The Center will require an additional thirty (30) days to process your request.

Reason for extension: _____

Your health information will be available for access on _____ between the times of _____.

Complaints. If you disagree with our decision concerning access to your health information, you may send a written complaint to our Privacy Officer at Knox County Community Health Center at 11660 Upper Gilchrist Road, Mount Vernon, Ohio 43050, ATTN: Lane Belangia, or contact the same at telephone no. (740) 399-8015. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services at 200 Independence Avenue, SW, Washington D.C. 20201 or call 1-877-696-6775. There will be no retaliation for filing a complaint.

Privacy Officer's Signature: _____ Date: _____

RIGHT TO AN ACCOUNTING

POLICY: Upon request, the Center shall provide individuals with an accounting of the uses and disclosures of their health information in accordance with the HIPAA Privacy Rule.

PROCEDURE:

1. A patient has the right to receive an accounting of disclosures of his or her PHI made in the six (6) years prior to the date on which the patient requests the accounting. All requests for an accounting will be handled by the Privacy Officer. Patients must request an accounting in writing by completing the Request for Accounting form and submitting it to the Privacy Officer.

2. The Privacy Officer does <u>not</u> need to account for the following disclosures:

    a. Disclosures for treatment, payment, or health care operations.
    b. Disclosures made pursuant to the patient's authorization.
    c. Disclosures made to the patient.
    d. Disclosures to persons directly involved in the patient's care.
    e. Disclosures that are incidental to an otherwise permitted disclosure.
    f. Disclosures for national security or intelligence purposes.
    g. Disclosures to correctional institutions or law enforcement officials concerning persons in custody.
    h. Disclosures pursuant to a limited data set.

3. Examples of disclosures that must be accounted for include:

    a. To a governmental authority required by law for abuse, neglect or domestic violence.
    b. For health oversight activities required by law to audit and investigate.**
    c. To a governmental authority required by law for child abuse or neglect.
    d. To a law enforcement official concerning crime victims or criminal conduct.**
    e. To a coroner or medical examiner required by law for a decedent.
    f. To a public authority required by law for disease reporting.
    g. To an employer, where we have been requested by the employer to conduct an evaluation of the patient.
    h. To the Food and Drug Administration.
    i. To a public health authority required by law to collect information regarding injury or disability (trauma, gunshot).
    j. For organ procurement.
    k. For research purposes (except if the patient signed an authorization).
    l. Pursuant to a subpoena, discovery request, or a court order.
    m. For aversion of threats to public health or safety.
    n. For administration of the Department of Veterans Affairs.
    o. To a public health authority required by law to collect vital statistics.

    * Please note that disclosures pursuant to #3(a)-(o) do not need to be included in an accounting if the patient signed an authorization for the disclosure.

    ** If you are disclosing a patient's health information to law enforcement officials or a health oversight agency, and the agency or official provides you with a statement indicating that disclosure in the accounting would impede their investigation, then you must exclude this disclosure from the accounting.

4. An accounting must include the following information:

    a. The date of the disclosure.
    b. The name of the entity or person who received the patient's health information and, if known, their address.
    c. A brief description of the health information disclosed.
    d. A brief statement of the purpose of the disclosure that informs the patient of the basis for the disclosure or, in lieu of this statement, a copy of the written request for a disclosure from the patient.

5. You must provide an accounting no later than sixty (60) days after receiving the patient's request. If you cannot meet the sixty (60) day deadline, you may extend the deadline by thirty (30) days if you inform the individual of the extension in writing within the original sixty (60) day deadline. Your extension notice must state the reason for the delay and the date in which you will provide the requested accounting. You may only extend the deadline once.

6. The first accounting in any twelve (12) month period must be provided free of charge. You can charge a reasonable fee for a subsequent accounting in the same period.

7. You must document and retain the information included in the accounting to an individual, a copy of the written accounting that was provided to the individual, and the title of the person or office responsible for receiving and processing the accounting for six (6) years.

8. You can deny a request for an accounting when made by the personal representative of a patient if:

    a. The patient has been or may be subject to domestic violence, abuse, or neglect by the person requesting the information and the accounting could endanger the patient; or

    b. The Privacy Officer decides that it is not in the best interest of the patient to treat the person as the patient's representative.

NOTICE OF FEE FOR AN ACCOUNTING

Patient Name: _____

Address: _____

City, State, Zip Code: _____

Knox County Community Health Center is in receipt of your request for an accounting of disclosure involving your medical information on _____. We will charge a fee to process accounting requests when more than one request is received within any 12-month period. This is your _____ request for an accounting since _____, and accordingly, if you wish to continue with your request, then you will be charged $_____ for processing your request.

Please notify us immediately if you wish to withdraw your request for an accounting. If you have not advised us of a withdrawal within 10 days of your receipt of this notice, we will process your request and bill you accordingly or you may enclose your check and return this notice.

❒ I wish to have the accounting and my fee is enclosed.

❒ I am withdrawing my request for an accounting.

Checks may be made out to: _____ and mailed to the following address:

_____
Name

_____
Address

_____
City State Zip

Individual Responsible for processing request:

_____
Name

_____
Title

_____
Phone Number

Signature: _____ Date: _____

NOTICE OF STATUS OF REQUEST FOR ACCOUNTING

Date: _____

Patient Name: _____

Address: _____

City, State, Zip Code: _____

Knox County Community Health Center is in receipt of a request of an accounting involving disclosure of your medical information on _____. We are required to take action on your request within 60 days of receipt of your request unless there are reasons why we are unable to act within that time period.

This is to notify you that we are unable to respond to your request within the 60-day time period. As required by the HIPAA regulations, we are requesting an extension and your request will be acted upon no later than 30 days from the date of this notification.

The reason for this extension is: _____

_____

_____

_____

If you have questions about this notice, you may contact the individual responsible for processing your request:

Print Name: _____

Signature: _____

Title: Center Privacy Officer Phone Number: _____

REQUEST FOR ACCOUNTING

If you are the patient or his or her legal representative, you have the right to receive an accounting of certain disclosures of the patient's health information. Please complete the following information so that we may process your request.

Patient's Name: _____

Address to receive accounting: _____

_____

_____

Telephone number: _____

Period of time requested: _____

The following disclosures will not be provided in an accounting:

- Disclosures made pursuant to an authorization signed by the patient or his or her legal representative;
- Disclosures to carry out our treatment, payment and health care operations;
- Disclosures made to the patient or his or her legal representative;
- Disclosures made to persons directly involved in the patient's care;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials about persons in custody;
- Disclosures that occurred more than six (6) years prior to the date of this request; or
- Disclosures pursuant to a limited data set.

If you request more than one accounting in any twelve (12) month period, we will charge you a reasonable fee for the accounting.

Name of Person Requesting the Accounting: _____

Signature: _____

Date: _____

If personal representative, your relationship to patient: _____

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

POLICY: To allow individuals the opportunity to request communications from the Center by alternative means or at alternative locations through a "Confidential Communication Request" Form in accordance with the HIPAA Privacy Rule.

PROCEDURE:

1. Individuals have the right to request to receive communications from the Center by alternative means or at alternative locations through a "Confidential Communication Request" form. For example, individuals may ask that appointment reminder calls be made to them only at work rather than at home. All reasonable requests should be accommodated.

2. Upon receipt of a written request for a confidential communication, the Privacy Officer shall review the request to determine whether the request is reasonable and can be accommodated.

3. The Center will not inquire why the individual is requesting communications on a confidential basis.

4. If a request cannot be reasonably accommodated, then the Privacy Officer shall contact the individual, in writing or by telephone, to explain why the request cannot be accommodated.

5. All confidential communication requests that are approved must be documented. Before communicating with any individual, the Center workforce member should determine whether a confidential communication restriction exists.

REQUEST FOR CONFIDENTIAL COMMUNICATIONS

You have the right to request that the Center communicates with you on a confidential basis by requesting an alternative means or alternative location to receive Center communications. All reasonable requests will be accommodated for internal operations.

If you wish to be contacted at an address or phone number other than your home address or home telephone, please provide the following information:

Patient's Name: _____

Address to receive communications: _____

_____

_____

Telephone number to receive communications: _____

Please describe in as much detail as possible any other alternative means you request the Center uses in communicating with you or any other alternative location not detailed above.

_____

_____

_____

Print Name: _____

Signature: _____

Date: _____

If legal representative, relationship to patient: _____

****

FOR CENTER USE ONLY: Date Received: _____

Request Approved ❒ Denied ❒ If denied, reason: _____

Patient notified by: ❒ Telephone ❒ Letter Date: _____

Center representative (print): _____

Signature: _____ Date: _____

- PROVIDE COPY TO THE PATIENT AND MAINTAIN A COPY IN THE RECORD -

CONFIDENTIALITY OF CLIENTS

POLICY: It is the policy of Knox County Community Health Center that all employees maintain and protect the confidentiality of clients. Knox County Community Health Center adheres to the following confidentiality as outlined below in accordance with 42 CFR part 2 and HIPAA.

In brief overview, HIPAA protects any health information that identifies an individual, whereas 42 CFR part 2 protects only information that identifies an individual as being a patient in a drug or alcohol abuse program or as having a drug or alcohol abuse problem. It is possible for some information to be protected by only one of these provisions, and for some information to be protected by both. Center employees are responsible for understanding the distinguishment between these two laws and for applying HIPAA and/or Part 2 where necessary to ensure compliance.

Confidentiality of information is the right of the client. All information, verbal and written, obtained in the process of caring for the client or his/her family is considered confidential information and may not be disclosed without the written authorization of the client.

All Knox County Community Health Center employees, contractors, interns, volunteers, and all other individuals with access to client information are informed of the privileged and confidential nature of such information during initial employment processing.

The right of privacy, a tradition in medicine and protected by law, is necessary for effective behavioral health treatment; therefore, we have a clear obligation to safeguard any confidential data about the client acquired from any source. To ensure client confidentiality, a staff member provides information and guidelines to client and family members about prohibitions against the use of tape recorders or video/tape recorder combinations in the facility.

The concept of confidentiality has ethical, as well as legal implications. Individuals who may be responsible for providing care for friends, relatives, or acquaintances shall discuss immediately with their supervisor issues or circumstances that may present a potential conflict or breach of confidentiality.

All employees of Knox County Community Health Center, contractors, volunteers, and other individuals who have access to client information will indicate an understanding of the rules governing client information and prohibition of re-disclosure. This understanding, the dismissal policy for disclosure of data, and the legal penalties for unauthorized disclosure of data and information is acknowledged by a signed statement indicating that he/she recognizes individual responsibility to hold such data in confidence.

Any employee, contractor, volunteer or other individual may be subject to immediate termination of their employment/relationship with Knox County Community Health Center for violation of the company's policies regarding confidentiality. They may, in addition, be subject to federal/state regulations and laws, which include fines and/or imprisonment and/or reporting breach of confidentiality to professional licensing boards.

Questions or concerns regarding legal obligations or duty to disclose information, i.e., communicable diseases, gunshot wounds, child abuse are referred to primary counselors or practitioners and to the Clinical Director for follow-up and/or reporting of the incident.

<u>Confidentiality of Client Records</u>:

Federal and state laws protect the confidentiality of the clients' records maintained by Knox County Community Health Center. Staff will not divulge or confirm a client's treatment status to any person or entity, nor disclose

any information identifying the client as having associated alcohol or drug abuse problems, unless:

1. The client/guardian consents in writing.
2. The disclosure is allowed by a court order signed by a judge.
3. The disclosure is made to medical personnel in a medical emergency or to qualified staff.
4. For research, audit or treatment center evaluation purposes in compliance with applicable law.
5. Federal and state laws require "Duty to Report" information about suspected child abuse or neglect, disabled person, and/or elder abuse, and the treatment center staff will adhere to these regulations. Suspected violations must be reported.
6. Federal laws and regulations do not protect information about a crime committed by a client or any threat to commit such a crime.
7. The disclosure is otherwise explicitly permitted by governing federal or state law.

See 42 U.S.C. 290dd-2 for federal laws and 42 CFR part 2 for federal regulations.

PROCEDURE:

1. The Human Resources Director shall inform employees, contractors, volunteers or other individuals of confidential nature of information related to patients at Knox County Community Health Center.

2. The Human Resources Director shall discuss sanctions imposed related to breach of confidentiality which may include:
   - Immediate termination
   - Fines/Imprisonment — Subject to rules and regulations of State/Federal statutes.
   - Reports of breach of confidentiality to professional licensing board by company management.

3. The Human Resources Director assures compliance and understanding of policy related to confidentiality by having individual(s) sign statement of agreement during employment/service processing. The Center uses health information only for purposes permitted by law and regulation or by further limitations of its policy on privacy. The Center discloses health information only as authorized by the individual served or as otherwise consistent with law and regulation. The Center monitors compliance with its policy on the privacy of health information. The compliance officer is responsible for monitoring privacy safeguards within the organization and externally with vendors who have access to protected health information. Access to the electronic medical records is controlled by user ID and password login. No protected health information is permitted to be removed without the prior authorization of leadership.

4. Security and integrity of health information is accomplished by limiting access use and disclosure. Access to protected health information is determined by leadership on a need to know basis. All electronic health information will be maintained for seven (7) years prior to destruction by complete erasure via overwriting of hard drives containing said info.

5. It is the responsibility of the Clinical Director to designate a responsible staff member of the Center to orient patient/family members to the Center rules and regulations and ensures compliance with prohibition against patient possession of tape recorder/cameras at of Knox County Community Health Center.

6. It is the responsibility of the Clinical Director to discuss with an employee, a potential conflict of interest and/or potential breach of confidentiality related to prior relationship with patients and/or family members.

7. All information pertaining to a patient is considered confidential and is therefore "privileged" information and protected according to state laws.

8. A practitioner must never release any information regarding a patient without their proper written consent, even if the request is just to see if the client is being seen at the Center.

9. The standard response to anyone requesting information should be: “it is state law and the policy at our Center that we cannot release any information regarding whether or not someone is a patient without the proper legal consent.”

10. There are some instances in which confidentiality can be breached including: (1) court orders signed by a judge, (2) a client's report that he wishes to harm himself or someone else, and (3) a client's report that he is being abused/hurt by someone else, and (4) duty to report situation is achieved. More detailed scenarios are listed below.

11. In cases where OHMHAS is conducting an investigation, by law the Practitioner is required to cooperate. However, therapeutic updates regarding progress would require a valid Release of Information.

12. Practitioners should never store patient confidential information in their offices. All patient information must be stored in the medical record.

13. Practitioners should never take patient information off-site unless there is a school or home visit, an off-site meeting regarding the client, or court.

14. Any breaches of client confidentiality will be taken seriously and may be cause for termination. Any breach of confidentiality shall be documented on an Incident Report form and reported to the Clinical Director.

15. All employees must sign a Pledge of Confidentiality upon hire. If staff is uncertain about the legality or appropriateness of Releases, they shall seek guidance from the Office Manager, Clinical Director and/or Knox County Community Health Center’s attorney. Only the Office Manager shall provide documented or verbal information to external sources regarding clients. If other staff receives written or verbal requests, they shall contact the Office Manager who may release the information if a valid release is on file.

16. New Employees: Each new employee shall be oriented on the first day of employment about the rules and laws of confidentiality and organizational policies and procedures. The orientation and training events shall be documented in the individual's Human Resources file.

17. Specific disclosures:

    a. Child Abuse: When complying with State Child Abuse reporting requirements, the general rule is to report the child abuse, but to limit the information to what is absolutely necessary. The Department of Children and Families' representatives will be allowed to interview and receive information relating only to the abuse issue.

    b. Infectious Disease Reporting: State reporting statutes mandate the Center to report and comply with requests in prevention of disease and promotion of health efforts. The 80 Rule is to limit

the information to only what is necessary to fulfill the reporting requirements.

i. Exception: If the request for information from the medical record is used as a personal document (i.e., the identity of the client is released) then a signed authorization is necessary to release the information.

c. Insurance Companies or Third Party Payers: The Office Manager will release information only with a written receipt of authorization under Title 42 of the Code of Federal Regulations Part 2, which applies to drug and alcohol.

i. Exception: If a client commits a crime while in active treatment, the authorities may be notified and the name released, but no other information from the record shall be released in such instances.

d. Attorney Requests: An attorney's request for information must be accompanied by the client's written authorization whether the attorney represents the client or opposing party. This also holds when the requestor desires a copy of the record or an appointment to view the record (with a clinician). If the authorization cannot be obtained, legal proceedings may be an alternative, The Center's legal counsel has immediate access to records if a legal action is brought against the Center.

e. Information Released to Police: Information released to police will only be to the extent that would be found in the police register (i.e., nature of an accident). No specific medical data will be given without valid consent of the client or a court order.

f. Deceased: When information is requested regarding a deceased client, the administrator or executor of the estate has the right to authorize disclosure. This person must present proof of eligibility (i.e., court document, letter of authorization by an attorney for the estate, guardianship papers) before release or inspections of records.

g. Persons Declared Legally Incompetent: Legally incompetent individuals must have authorization signed by a parent, guardian, or legal representative.

h. Release Under Emergency Situations: Relevant information may be released to providers in the event of an emergency that will assist in the treatment of the specific emergency, but an entire record shall not be released for this purpose. Only the relevant information shall be given.

The following would be of interest to the emergency care service personnel:

i. Previous history of symptomatology.
ii. Current medications, dosages, last time taken.
iii. Allergies or reactions to medications.
iv. Current diagnosis.
v. Recommendations for follow-up care (if applicable).

When information has been released under Emergency Situations, the staff member responsible for the release of information must enter all pertinent details of the transaction into the client's medical record including:

i. The date the information was released.
ii. The person to whom the information was released.
iii. The reason why the information was released without a written consent.
iv. The specific information that was released.

v. The client will be informed as soon as possible that the information was released and he/she will be requested to sign a written consent.

18. Release of Information Policy: Knox County Community Health Center will always require an authorization to release information, signed by the client or other responsible party when personal, confidential information is to be released in the absence of any specific law to the contrary.

19. In general, the following releases of information should be obtained from clients upon admission to the program:
    a. Parents of adult children
    b. Non-Knox County Community Health Center practitioners or physicians.
    c. The client shall be informed in a manner to assure their understanding of the specific type of information that has been requested.
    d. The client shall give consent voluntarily.
    e. The client shall be informed that the provision of services is not contingent upon the decision concerning release of information.
    f. The consent is acquired in accordance with all applicable Federal, State, and Local Laws.

    All consents shall be dated with the actual date the information was released and the signature of the staff who released the information. This document will be filed in the medical record.

20. The written consent of the client or their authorized representative will be considered valid only if the following conditions are met:
    a. Specific details the scope of the information requested.
    b. The date of signature of the consent.
    c. The name of the individual to whom the records are to be released to.
    d. The purpose of its uses.
    e. The individual has been informed that their record may contain information of alcohol and substance abuse information, medical, psychiatric and/or psychological, HIV Antibody testing.
    f. The termination date or the following event/condition of the release form.
    g. The client or representative is informed in a manner to assure their understanding of the specific type of information that has been requested.
    h. The client/representative gives consent voluntarily by signature.
    i. The client/representative is informed that the provision of services is not contingent upon the decision concerning release of information.
    j. The consent is acquired in accordance with all applicable Federal, State, and Local Laws.
    k. The consent states Prohibition of Redisclosure or is accompanied by the specific notice prohibiting redisclosure.
    l. A copy of the cover letter, accompanying the information released with the signature of the staff that released the information, will be filed in the medical record.

21. Criminal Penalty: Any person who willfully discloses health care information in violation of this act, and who knew or should have known that disclosure is prohibited, is guilty of a misdemeanor and, upon conviction, is subject to a fine, not to exceed $2000.00, and/or imprisonment of a period not to exceed one (1) year.

22. Consent To Release of Information: As a general rule, a person who can consent to treatment can also consent to the release of information. Therefore, a conservator can sign to release a conservator's information if he/she has the power to admit. In cases of group therapies, or information generated by others rather than the client, the information may not be released without the consent of the party

originating the information, unless Court Order has been issued. The requesting party will be informed that such information has been deleted from the record. There is no special access to records for police officers, school officials/representatives, employers, probation officers, or social workers that do not have the right to consent for the client's treatment, nor for clinical staff not specifically involved with the client's treatment.

23. Revocation of Authorization for Disclosure: A client may revoke a disclosure authorization to a health care provider at any time unless disclosure is required to effectuate payments for their treatment.

24. Limits of Confidentiality: The limits of confidentiality are at one (1) year intervals. After each year a new Release of Information form shall be initiated if the Client so desires.

HIPAA PRIVACY TRAINING

POLICY: The Center will train all new and existing workforce members (which includes volunteers and students) on the requirements of the HIPAA Privacy Rule and related policies and procedures. The Privacy Officer will develop and implement the training program.

PROCEDURE:

1. The Privacy Officer shall provide HIPAA training for all existing Center workforce members within a reasonable time after a material change to these Policies and Procedures and all new workforce members as part of their orientation within sixty (60) days of being hired. The Privacy Officer shall provide HIPAA training for all workforce members annually thereafter.

2. Workforce members are required to sign the "HIPAA Training and Confidentiality Pledge" indicating that they have received HIPAA privacy training and agree to protect the confidentiality of the patient's health information. Documentation of the type, amount, and date the training will be retained for seven (7) years.

HIPAA TRAINING AND CONFIDENTIALITY PLEDGE

I acknowledge that, on the date below, I received training on the HIPAA Privacy Rule and the Center's policies and procedures for preserving the privacy of a patient's health information.

I understand that I am to consider all patient health information strictly confidential and shall not use or disclose such information in any manner contrary to the HIPAA Privacy Rule or the Center's policies and procedures.

I further understand that I may be subject to discipline, including termination of employment, if I improperly use or disclose patient health information.

Name: _____

Signature: _____

Date: _____

NOTICE OF PRIVACY PRACTICES POLICY

POLICY: The Center will provide patients with written notice of the permitted uses and disclosures of their health information, their rights with respect to the information, and the Center's duties to comply with the HIPAA Privacy Rule and preserve the confidentiality of such information.

PROCEDURE:

1. All Center patients will be provided with a copy of the Center's "Notice of Privacy Practices" as required by law. In addition, the Notice shall be posted on the Center's website, provided to new patients on their first date of service, and provided to all current patients within sixty (60) days of any material revision in the Notice, or, in the case that a patient does not have capacity upon admission to understand his or her medical status, as soon thereafter as the patient attains such capacity.

2. The Center shall notify the patient of the availability of the notice and how to obtain it at least once every three (3) years.

3. The model Notice of Privacy Practices contains language that is required by law. Do not revise the notice without legal counsel.

4. If a patient has a present or past history of a drug/alcohol abuse problems, their records are protected by Titles 42 of the Code of Federal Regulations, Part 2 from disclosure, prior to consent, a court order, or under other limited circumstances. Once the proper authorization is obtained, with the request, each sheet of the requested information will be stamped with either the "Confidential" stamp and a statement of prohibition of re-disclosure will accompany requested information.
    a. Drug & Alcohol Prohibition on Redisclosure: "This information has been disclosed to you from records protected by Federal Confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2." A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse.

5. The notice will indicate that all complaints will be forwarded to the Privacy Officer at Knox County Community Health Center, LLC, Attn: Lane Belangia, 11660 Upper Gilchrist Road, Mount Vernon, Ohio 43050, or by telephone at: (740) 399-8015, or the Secretary of Health and Human Services.

6. All patients receiving a copy of the notice will be asked to sign an acknowledgement of their receipt of the notice. Acknowledgements will be retained for at least seven (7) years. If you are unable to obtain the patient's written acknowledgment, then document your efforts to do so and the reason why the acknowledgement could not be obtained.

7. In the case of an emergency, or where the patient is otherwise unable to acknowledge receipt due to unconsciousness, etc., then the patient's acknowledgment will be obtained as soon as practicable thereafter.

8. All acknowledgments of receipt or documentation of a good faith effort to obtain that acknowledgment shall be maintained in the patient's file.

KNOX COUNTY COMMUNITY HEALTH CENTER NOTICE OF PRIVACY PRACTICES

This notice describes how your medical information and information about your substance use disorder patient records may be used and disclosed and how you can get access to this information. **Please review this notice carefully.**

Your Rights: *When it comes to your health information, you have certain rights.* This section explains your rights and some of our responsibilities to help you.

- Get an electronic or paper copy of your medical record
  - You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
  - We will provide a copy or a summary of your health information in a timely fashion, within 30 days of your request. We may charge a reasonable, cost-based fee.
- Ask us to correct your medical record
  - You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
  - We may say "no" to your request, but we will tell you why in writing within 60 days.
- Request confidential communications
  - You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
  - We will say "yes" to all reasonable requests.
- Ask us to limit what we use or share
  - You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.
  - If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.
- Get a list of those with whom we've shared information
  - You can ask for a list (accounting) of the times we have shared your health information for six years prior to the date you ask, who we shared it with, and why.
  - We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We will provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.
- Get a copy of this privacy notice
  - You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.
- Choose someone to act for you
  - If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
  - We will make sure the person has this authority and can act for you before we take any action.
- Keep your presence at Knox County Community Health Center confidential
  - Presence in the program will not be disclosed to anyone without your written permission.
  - Your condition, progress, or any other information about you in the Knox County Community Health Center programs will not be disclosed to anyone outside of the Center without your written permission.
  - The only exceptions to this rule are disclosures answering judicial court orders and disclosures to medical personnel or to a qualified person for research, audit, or program evaluation.
  - See 42 U.S.C. 290dd-3 and 42 U.S.C. 290ee-3 for Federal laws and 42 CFR part 2 for Federal regulations.
- File a complaint if you feel your rights are violated
  - You can complain if you feel we have violated your rights by contacting us using the information at the end of this notice.
  - You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or by visiting: www.hhs.gov/ocr/privacy/hipaa/complaints/
  - We will not retaliate against you for filing a complaint.

Your Choices: *For certain health information, you can tell us your choices about what we share.* If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

- In these cases, you have both the right and choice to tell us to:
  - Share information with your family, close friends, or others involved in your care
  - Share information in a disaster relief situation
  - Include your information in a hospital directory

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

- In these cases we never share your information unless you give us written permission:
  - Marketing purposes
  - Sale of your information
  - Sharing of psychotherapy notes
- In the case of fundraising:
  - We may contact you for fundraising efforts, but you can tell us not to contact you again.

Our Uses and Disclosures: *How do we typically use or share your health information?* We typically use or share your health information in the following ways.

- Treat you
  - We can use your health information and share it with other professionals who are treating you.
  - *Example: A doctor treating you for an injury asks another doctor about your overall health condition.*
- Run our Center
  - We can use and share your health information to run our practice, improve your care, and contact you when necessary.
  - *Example: We use health information about you to manage your treatment and services.*
- Bill for your services
  - We can use and share your health information to bill and get payment from health plans or other entities.
  - *Example: We give information about you to your health insurance plan so it will pay for your services.*

How else can we use or share your health information? We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes.

- Help with public health and safety issues
  - We can share health information about you for certain situations such as:
    - Preventing disease
    - Helping with product recalls
    - Reporting adverse reactions to medications
    - Reporting suspected child abuse, neglect, or domestic violence
    - Preventing or reducing a serious threat to anyone's health or safety
    - Reporting your commission of a crime on the premises of the Center or against personnel of the Center
- Do research
  - We can use or share your information for health research.
- Comply with the law
  - We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we are complying with federal privacy law.
- Respond to organ and tissue donation requests
  - We can share health information about you with organ procurement organizations.
- Work with a medical examiner or funeral director
  - We can share health information with a coroner, medical examiner, or funeral director when an individual dies.
- Address workers' compensation, law enforcement, and other government requests
  - We can use or share health information about you:
    - For workers' compensation claims
    - For law enforcement purposes or with a law enforcement official
    - With health oversight agencies for activities authorized by law
    - For special government functions such as military, national security, and presidential protective services
- Respond to lawsuits and legal actions
  - We can share health information about you in response to a court or administrative order, or in response to a subpoena.

To the extent that your records contain information related to your receipt of drug and/or alcohol treatment programming, additional limitations apply as to our disclosure.

For more information see:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We may not acknowledge your presence at Knox County Community Health Center unless we receive your written consent or if there is a court order.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html**.**

Applicable Privacy Statutes

- 42 CFR part 2
- ORC § 5119.28
- 45 CFR part 164

Changes to the Terms of this Notice

This Notice describes how Knox County Community Health Center may use and disclose your protected health information. The terms of this Notice of Privacy Practices are effective June 2023. We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Contact Information:

If you have any questions about this Notice, or have a complaint, then please contact the following Privacy Officer:

Lane Belangia
11660 Upper Gilchrist Road
Mount Vernon, Ohio 43050
Phone: (740) 399-8015

ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

Notice to Patient:

The Center is required to provide you with a copy of our Notice of Privacy Practices, which states how we may use and/or disclose your health information. The Center also acknowledges that violation of your privacy by a Part 2 program is a crime and that suspected violations may be reported to the Privacy Officer or appropriate federal authorities. Please sign this form to acknowledge receipt of the Notice. You may refuse to sign this acknowledgement, if you wish.

I acknowledge that I have received a copy of this office's Notice of Privacy Practices.

_____

Signature

_____

Print name

_____

Date

****

We have made every effort to obtain written acknowledgment of receipt of our Notice of Privacy from this patient, but it could not be obtained because:

□ The patient refused to sign.
□ Due to an emergency situation it was not possible to obtain an acknowledgement.
□ We weren't able to communicate with the patient.
□ Other (Please provide specific details)

Employee Signature: _____

Date: _____

BUSINESS ASSOCIATE POLICY

POLICY: To secure business associate contracts with all persons or entities that provide services for or on behalf of the Center who will have access to or create a patient's health information. Business associate agreements are required by HIPAA to ensure that each business associate takes appropriate steps to safeguard a patient's health information.

PROCEDURE:

1. Identify business associates. Complete the appropriate fields of the model Business Associate Agreement for each business associate and obtain a signed agreement. If you are unsure whether a Business Associate Agreement is needed, contact the Privacy Officer for guidance. Examples of business associates include collection agencies, billing companies, consultants, accrediting bodies, legal counsel, The Joint Commission, etc.

2. A Business Associate Agreement is NOT required for disclosures to:

    a. Treatment providers involved in the patient's care are not considered business associates and therefore no business associate contract is necessary.

    b. The departments/functions that are designated as part of the Center's health care component.

    c. Member of the Center's workforce, janitorial and housekeeping staff (since they are not expected to have access to patient's health information as part of their job duties).

3. The model Business Associate Agreement contains statements that are required by law. Changes to the Agreement must be approved by the Center's legal counsel.

4. In you learn that a business associate is misusing a patient's health information, you must report the violation to the Privacy Officer. The Privacy Officer will contact the business associate to take steps to cure the violation. If the steps are unsuccessful, the Privacy Officer will terminate the Business Associate Agreement or, if it cannot be terminated, contact the Secretary of HHS.

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made and is effective as of the _____ day of _____, 20___ by and between Knox County Community Health Center ("Provider") and _____ _____ ("Contractor").

WHEREAS, Provider and Contractor have a business arrangement whereby Contractor provides goods or services to Provider, and during the course of providing such goods or services, Contractor may receive medical records or other information about patients including the identity of patients ("Protected Health Information," as that term is more fully defined below); and

WHEREAS, Protected Health Information is subject to protection both under Provider's policies and under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including 42 CFR part 2 ("Part 2") and Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009 42 USC §§17921-17954 ("HITECH") and their respective, implementing regulations; and

WHEREAS, Contractor may be a business associate of provider as that term is defined in HIPAA; and

WHEREAS, HIPAA requires that each Business Associate of provider, as a condition of doing business with Provider, agree in writing to certain provisions, including the use and disclosure of Protected Health Information; and

WHEREAS, the parties further desire to comply with the provisions of the Fair and Accurate Credit Transaction Act of 2003 ("FACTA") and the Identity Theft Prevention Regulations issued in Part 681 of Title 16 of the Code of Federal Regulations.

NOW THEREFORE, in consideration of the mutual covenants and promises contained herein, the parties agree as follows:

I. Definitions

Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in Part 2, the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E ("Privacy Rule") and Security Rule Standards at 45 CFR part 160 and part 164, subparts B ("Security Rule").

"Protected Health Information" shall mean any information which relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or payment for the provision of healthcare to an individual and that identifies the individual or that can be used to identify the individual. For purposes of substance use disorder treatment, this definition extends to any information, whether recorded or not, created by, received, or acquired by a Provider relating to a patient (*e.g.,* diagnosis, treatment and referral for treatment information, billing information, emails, voice mails, and texts).

"Electronic Protected Health Information" or "ePHI" means Protected Health Information or "PHI" that is stored in electronic media. Electronic media means: (1) Electronic storage media, including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dialup lines,

private networks, and the physical movement of removable/transportable electronic storage media.

II. Use and Disclosure of Protected Health Information

The parties acknowledge that during the course of their Agreement, Contractor may receive Protected Health Information from Provider or may obtain or create Protected Health Information on behalf of Provider. The parties acknowledge that Protected Health Information is subject to protection both under Provider's policies, Ohio state law, and the privacy and security standards of HIPAA, HITECH, the Privacy and Security Rules, and other implementing regulations promulgated thereunder.

Contractor agrees that neither it nor any of its directors, officers, employees, contractors, or agents shall use or disclose Protected Health Information in any manner other than for the proper administration of its obligations under the underlying Services Agreement that it has with Provider, for Contractor's own necessary administrative purposes, or as required by law. Federal regulations prohibit any further disclosure of this information without specific written consent of the person to whom it pertains or as otherwise permitted by such regulations. Federal Law prohibits the use of this information to criminally investigate or process any alcohol or drug abuse treatment client. Contractor further agrees that neither it, nor any of its directors, officers, employees, contractors, and agents shall use or disclose Protected Health Information in any manner that would violate the HIPAA regulations if used or disclosed by the Provider in the same manner, or that would violate the minimum necessary policies and procedures of Provider.

Within five (5) days of a request by Provider, Contractor shall make available to Provider any Protected Health Information that is maintained by Contractor.

III. Safeguards for the Protection of Protected Health Information

Contractor shall implement and maintain such safeguards as are necessary to ensure that the Protected Health Information maintained by Contractor is not disclosed or used except as provided in this Agreement. Contractor warrants and represents that it has the agreement from each of its officers, directors, employees, and contractors that such person or entity shall not disclose any Protected Health Information to any person not directly involved in providing goods or services pursuant to this Agreement and who has a need to know the information. Contractor shall permit Provider to review and inspect its policies and procedures to safeguard Protected Health Information upon reasonable request by Provider.

IV. Reporting of Unauthorized Use or Disclosure

Contractor shall report to Provider any use or disclosure of Protected Health Information of which Contractor becomes aware that is not provided for or permitted pursuant to this Agreement. Such report shall be made by Contractor to Provider within five (5) days of Contractor becoming aware of the use or disclosure.

V. Reporting of Breach

Contractor shall report to Provider within five (5) days of Contractor becoming aware of the Breach or unauthorized acquisition, access, use, or disclosure of Protected Health Information that compromises the security or privacy of the Protected Health Information (a "Breach").

VI. Use of Subcontractors/Release to Third-Parties

To the extent that Contractor uses one or more subcontractors or agents to fulfill Contractor's obligations to Provider, and such subcontractors or agents receive or have access to Protected Health Information, and to the

extent that Contractor releases Protected Health Information to any third party, whether or not such third party is a subcontractor or agent of Contractor, Contractor shall require each subcontractor, agent, or third party to be bound by the same restrictions, terms, and conditions that apply to Contractor pursuant to this Agreement.

VII. Access to Information

Contractor acknowledges that pursuant to HIPAA, an individual has certain rights to examine his or her Protected Health Information that is maintained by Contractor. In the event that any individual requests access to his or her own Protected Health Information directly from Contractor, Contractor shall, within two (2) days of such request, forward such request to Provider. Provider shall in good faith determine whether such information is to be provided to the individual and shall so notify Contractor. If requested by Provider, Contractor shall provide the information to Provider, and Provider shall make the disclosure to the individual. Any denials of access to the Protected Health Information requested shall be the responsibility of the Provider.

VIII. Amendment of Protected Health Information

Contractor acknowledges that pursuant to HIPAA, an individual has certain rights to amend his or her Protected Health Information or a record about the individual maintained in a Designated Record Set. Within ten (10) days' notice by Provider that any record or Protected Health Information regarding an individual is to be amended, Contractor shall incorporate any amendments provided by Provider into the record or Protected Health Information. In the event the individual notifies Contractor directly that any Protected Health Information regarding such individual is to be amended, Contractor shall notify Provider within five (5) days of such request, and if Provider notifies Contractor that such information is to be amended, Contractor shall incorporate any amendments provided by Provider into the record or Protected Health Information.

IX. Accounting of Disclosure

Contractor agrees to document disclosures of Protected Health Information and information related to such disclosures in accordance with Provider's policies and procedures regarding accounting for disclosures. Contractor agrees to provide individuals with an accounting of disclosures of the individual's PHI in the event an individual requests such accounting directly from Contractor. Contractor agrees to provide the individual with the accounting in accordance with Provider's policies and procedures regarding accounting for disclosures.

Contractor acknowledges that pursuant to HIPAA, an individual has certain rights to an accounting of disclosures of Protected Health Information. Within ten (10) days of notice by the Provider to Contractor that Provider has received a request for an accounting of disclosures of Protected Health Information regarding an individual, Contractor shall make available to the Provider, at a minimum, the following information with respect to Protected Health Information that is subject to accounting pursuant to 45 CFR 164.528: (1) the date of each disclosure of Protected Health Information by Contractor; (2) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person; (3) a brief description of the Protected Health Information disclosed; and (4) a brief statement of the purpose of such disclosure that includes an explanation of the basis for such disclosure. The accounting of disclosures must be for the lesser of six (6) years prior to the date the request for an accounting is made, or the effective date of the privacy provisions of HIPAA. In the event the request for an accounting is delivered directly to the Contractor, Contractor shall within two (2) days forward such request to the Provider. It shall be the Provider's responsibility to prepare and deliver any such accounting requested. Contractor hereby agrees to implement an appropriate record-keeping process to enable it to comply with the requirements of this Section.

X. Electronic Protected Health Information

To the extent Contractor uses, discloses, creates, receives, maintains, or transmits ePHI on behalf of Provider, Contractor agrees that:

- Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits on behalf of Provider, as required by the HIPAA Security Rule.
- Contractor shall promptly report to Provider any "security incident" of which it becomes aware, as such term is defined in the HIPAA Security Rule. Security incidents must be reported by Contractor as soon as practicable, but in no event later than forty-eight (48) hours of discovering the incident. At the request of Provider, Contractor shall identify: (1) the date of the security incident; (2) the scope of the security incident; (3) the Contractor's response to the security incident; and (4) the identification of the party responsible for causing the security incident, if known. In addition, Contractor agrees to mitigate, at its own expense, any harmful effect imposed by the security incident.
- Contractor shall ensure that any agent, including subcontractors, to whom it provides ePHI agrees in writing to implement reasonable and appropriate safeguards to protect ePHI.

XI. FACTA

Representation. Business Associate acknowledges that it is familiar with FACTA and the implementing regulations. Business Associate further acknowledges that it has adopted an Identity Theft Prevention Program to protect and mitigate identity theft in accordance with those regulations related to any patient's information received from the Provider.

Compliance. Business Associate agrees that it will fully comply with the obligations imposed by FACTA and the implementing regulations and will take appropriate compliance steps to monitor, review, and report any "Red Flags" to Provider or patients of the Provider, as appropriate.

Coordination. In the event Business Associate becomes aware of circumstances that it believes may be a Red Flag, Business Associate, within the scope of its responsibilities, will investigate and attempt to verify the circumstances. In the event Business Associate is unable to do so, it will contact the Compliance Officer for Provider to coordinate advising the patient, making notations or corrections in medical or billing records, and taking other reasonable steps as may be appropriate under the circumstances.

XII. Availability of Books and Records

Contractor hereby agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Contractor on behalf of, Provider, available to the Secretary of Health and Human Services for purposes of determining Provider's and Contractor's compliance with HIPAA.

XIII. Term and Termination

The term of this Agreement shall be effective as of the date noted above and shall terminate when all of the Protected Health Information provided by Provider to Contractor, or created or received by Contractor on behalf of Provider, is destroyed or returned to Provider, or if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the provisions set forth in Section XII.

A material breach or violation of any requirement relating to the Protected Health Information shall give Provider

the right to terminate the relationship existing between the parties, or, if such breach or violation is minor, Contractor may be given an opportunity to cure or end such breach or violation. Provider may terminate this Agreement immediately if Contractor does not cure or end the breach or violation within the time specified. Provider shall be entitled to any damages permitted by law due to Contractor's breach or violation.

XIV. Effect of Termination

Except as provided in the following paragraph, upon termination or expiration of this Agreement for any reason, Contractor shall return to Provider, or at Provider's direction destroy, all Protected Health Information received from Provider, or created or received by Contractor on behalf of Provider. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the Protected Health Information.

In the event that Contractor determines that returning or destroying the Protected Health Information is not feasible, Contractor shall provide to Provider notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of the Protected Health Information is not feasible, Contractor shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return and destruction infeasible, for as long as the Contractor maintains such Protected Health Information.

XV. Notices

All notices, requests, demands, approvals, and other communications required or permitted by this Agreement shall be in writing and sent by certified mail (return receipt requested), by personal delivery, or by overnight delivery (such as Federal Express). Such notice shall be deemed given when received, except delivery by mail will be deemed given on any date of delivery by the United States Postal Service. Any notice shall be sent to the address noted above.

XVI. New Agreement/Compliance with HIPAA and FACTA

Contractor agrees to modify this Agreement or enter into a new agreement to comply with any additional provisions of HIPAA or FACTA that become applicable to Contractor, including any additional requirements regarding the privacy or security of Protected Health Information or other patient information.

Notwithstanding anything contained in this Agreement to the contrary, the parties shall comply with HIPAA, HITECH, the Privacy and Security Rules, and FACTA, and in the event any such corresponding standards, laws, rules, or regulations are amended, the terms and conditions of this Agreement shall be deemed amended to comply with such provisions.

IN WITNESS WHEREOF, the Parties agree to the foregoing:

Knox County Community Health Center	_____
By: _____	By: _____
Print: _____	Print: _____
Title: _____	Title: _____
Date: _____	Date: _____

RIGHT TO AMEND HEALTH INFORMATION

POLICY: Individuals shall have the right to amend their protected health information in accordance with the HIPAA Privacy Rule as described in this policy.

PROCEDURE:

1. Role of Privacy Officer. If a patient requests to amend his or her medical records, he or she should complete the "Request for Amendment" form and submit it to the Privacy Officer. The Privacy Officer is responsible for receiving and processing requests for amendments.

2. The Privacy Officer shall decide whether to grant or deny the request within 60 days of receiving the request. If they are unable to do so in this time period, the Privacy Officer may extend the deadline once by 30 days by providing written notice to the individual of the reason for the delay and when the request will be completed.

3. The Center should only permit amendments to its original documents. Except as provided below, patients should be directed to their health care providers for other amendments. The Center is not required to delete information contained in the medical record. It may attach information as necessary to ensure that the record is accurate and complete.

Denying a Request to Amend

1. The Privacy Officer may deny an individual's amendment request if:

    a. The individual's health information is accurate and complete;
    b. The individual's health information is not part of the applicable designated record set;
    c. The individual's health information was not created by the Center, unless the individual provides you with the basis to indicate that the originator of the health information is no longer available to act on the request for amendment; or
    d. The individual's health information is not available for inspection under the rules allowing an individual access to his or her information (such as psychotherapy notes).

2. Denial Notice — If the Privacy Officer denies a request, he or she must provide the individual with a written denial indicating:

    a. The reason for the denial;
    b. The individual's right to submit a written statement of disagreement with the denial and how to file the statement;
    c. A description on how the person can file a complaint with the Center (including the title and telephone number of the person responsible for processing complaints) and the Secretary of Health and Human services; and
    d. A statement that, if the individual does not submit a statement of disagreement, he or she may ask that you include their request for amendment and the denial with future disclosures of their health information.

4. Statement of Disagreement — If the individual files a statement of disagreement, the Privacy Officer may prepare a written rebuttal and send a copy to the individual. The Privacy Officer must identify the record that is subject to the dispute, attach the patient's request for the amendment, the denial notice, the statement of disagreement, and rebuttal (if any), and forward this information with subsequent disclosures. If the

request for amendment is denied and the patient does not file a statement of disagreement, you do not need to include the request for amendment and denial with subsequent disclosures unless the patient requests. The Center may include its own rebuttal statement to the patient's statement of disagreement, so long as a copy of the rebuttal is provided to the patient.

Granting a Request to Amend

1. To amend the record, attach the Request for Amendment form to the applicable portion of the medical record being amended. Notify the individual that the amendment has been accepted within the 60-day timeframe and make efforts to obtain the individual's agreement to contact the following persons or entities concerning the amendment:

    a. Persons identified by the individual as having health information needing amendment; and
    b. Persons, including Business Associates, that are known to have health information that is subject to the amendment.

KNOX COUNTY COMMUNITY HEALTH CENTER
REQUEST FOR AMENDMENT

The Center is not required to delete information contained in the patient's record. Please complete the following. You may attach a separate piece of paper if you need more room.

1. Date: _____
2. Patient's name: _____
3. Address: _____
4. Birth Date: _____

5. Please describe the information you want amended: _____
_____
_____

6. Date(s) of information you want amended (e.g., date of office/clinic visit, treatment, or other health care services) _____

7. State your reason for making this request: _____
_____
_____

8. Describe how the entry is incorrect, incomplete, or outdated: _____
_____
_____

9. What should the entry say to be more accurate or complete: _____
_____
_____
_____

10. Do you know of anyone who may have received or relied on the information in question such as your doctor, pharmacist, health plan, or other health care provider? □ Yes □ No
If yes, please specify the name(s) and address(es) of the organization(s) or individual(s)
_____
_____

11. If your request for amendment is granted, do you give us permission to contact the persons identified in item 10 above so that they may amend the information also? □ Yes □ No

Signature of Patient (or Patient's Representative):	Date:
Print Name of Patient (or Patient's Representative):	
If you are the representative of a patient, check the scope of your authority to act on the patient's behalf:	
❒ Power of Attorney ❒ Legal Guardian ❒ Surrogate Decision-Maker ❒ Executor or Personal Representative ❒ Parent ❒ Other: _____	

- Please forward this Request to the Privacy Officer -

****

FOR CENTER'S USE ONLY

Amendment has been: □ Accepted □ Denied
If denied, check the reason(s) for denial:

□ the health information was not created by this organization.
□ the health information is not part of the patient's record.
□ the law forbids making the health information in question available for inspection (e.g., psychotherapy notes).
□ the health information is accurate and complete.

Comments _____

_____

_____

Privacy Officer's Signature: _____ Date _____

- Privacy Officer: Attach this form to the portion of the record being amended and provide a copy to the patient. -

STATUS OF REQUEST FOR AMENDMENT

Name: _____

Address: _____

City, State, Zip Code: _____

Knox County Community Health Center has received a request for an amendment to your medical information on _____. We are required to take action on your request within 60 days of receipt of your request unless there are reasons why we are unable to act within that time period.

This is to notify you we are unable to respond to your request within the 60 day time period. As required by the HIPAA regulations, we are requesting an extension and your request will be acted upon no later than 30 days from this notification.

The reason for this extension is: _____
_____
_____
_____

If you have questions about this notice, you may contact the individual responsible for processing your request.

Print Name: _____

Signature: _____ Date: _____

Title: Privacy Officer Phone Number: _____

VERIFICATION POLICY

POLICY: To establish reasonable means to verify the identity and authority of an individual requesting access to a patient's health information.

PROCEDURE:

1. If the identity or authority of a person requesting a patient's health information is not known, then you must verify their identity and authority and document your actions.

2. The requestor's identity can be verified by knowing the requestor or by asking for his or her driver's license, passport, or state identification card with photograph. If the request is made by fax or phone, call the requestor back from the main switchboard.

3. The requestor's authority can be verified by, for example, obtaining a copy of a power of attorney, or court guardianship papers, or asking questions to determine that an adult acting for a young child has the requisite relationship to the child.

4. Public Officials

   Identity - You may rely on the following information to verify the identity of a public official seeking the patient's health information:

   a. If the request is made in person, the requestor provides an ID badge, official credentials, or other proof of government status.

   b. If the request is in writing, the letter is written on the appropriate governmental letterhead.

   c. If the disclosure is to a person acting on behalf of a public official, their identity may be verified by a written statement on government letterhead that the person is acting on the government's behalf or other documentation establishing the same.

   Authority - You may rely on the following information to verify the authority of a public official seeking the patient's health information (a) a written or oral statement of the official's authority to request the information; or (b) if the request is made pursuant to a subpoena, order, warrant or other legal process you may presume authority.

MINIMUM NECESSARY POLICY

POLICY: It is the Center's policy that all uses and disclosures of a patient's health information shall be limited to the minimum amount of information that is reasonably necessary to accomplish the intended purpose of the use or disclosure, unless otherwise permitted by law. This extends to, without limitation, protected information pursuant to 42 CFR part 2.

PROCEDURE:

1. The Privacy Officer shall identify the persons, as appropriate, who need access to the patient's health information to carry out their duties and the types of health information to which access is needed. The following types of uses are NOT subject to the minimum disclosure requirements:

    a. Uses to prepare information to give to a patient or to the patient's representative;
    b. Uses and disclosures that the patient has authorized in a signed Authorization;
    c. Disclosures to a treatment provider;
    d. Disclosures to a covered entity for non-treatment purposes;
    e. When disclosure is requested by a business associate who represents that the information is the minimum necessary;
    f. Disclosures to public officials who represent that the information sought is the minimum necessary;
    g. Disclosures to the Secretary of HHS for compliance or enforcement activities; and
    h. Disclosures for any purpose required by law.

2. Each determination of what information constitutes the minimum necessary must be individually evaluated on a case-by-case basis to ensure that the information disclosed is the minimum necessary to accomplish the purpose of the disclosure. You may develop standard protocols for routine and recurring disclosures.

3. As a general rule, you may not disclose the patient's entire record except in those instances when the entire record is justified as the amount that is reasonably necessary.

COMPLAINT AND REPORTING POLICY

POLICY: To establish a process for individuals and workforce members to make complaints regarding suspected privacy violations. The intent of this policy is to promptly resolve complaints and mitigate the harmful effects of any privacy violation.

PROCEDURE:

1. Role of Privacy Officer. The Privacy Officer is responsible for receiving and investigating all suspected privacy violations. The Privacy Officer shall log all complaints on a complaint log indicating the date, time, name of the individual making the complaint, and a description of the complaint. The Privacy Officer shall investigate the complaint and take all appropriate steps to mitigate the effects of any privacy violation. The Privacy Officer shall notify the individual who made the complaint of the outcome of the investigation and how the complaint was resolved.

2. Notice of Privacy Practices. The Center's Notice of Privacy Practices shall inform individuals of how to file complaints with the Privacy Officer and/or the Secretary of HHS.

3. Documentation. The Privacy Officer shall document all complaints, their resolution, and any actions resulting from the complaint. The documentation must be retained for a minimum of seven (7) years from the date of the final resolution.

4. No Retaliation. At no time shall any individual who makes a complaint to the Privacy Officer be retaliated against.

How to file a Complaint

1. Individuals should file a privacy complaint using the "Reporting Form for Privacy Violations." The form should be submitted to the Privacy Officer. The form allows the complainant to remain anonymous and may be placed in the anonymous reporting box for privacy violations. However, individuals may make complaints directly to the Privacy Officer in accordance with the complaint process in the Notice of Privacy Practices.

2. The Privacy Officer will educate workforce members of their reporting obligation and how to file a complaint.

KNOX COUNTY COMMUNITY HEALTH CENTER
REPORTING FORM FOR PRIVACY VIOLATIONS

Name: _____ (unless you wish to remain anonymous)

Date: _____

Are you a patient □, member of the workforce □, or other □. If other, please describe:_____

Description of possible violation: _____
_____
_____

When did this occur? _____

Person(s) involved: _____

How did you come to learn of the incident? _____
_____

Do you have any evidence to prove the above allegations? If so, please describe: _____
_____
_____

Would you be willing to discuss the above allegations with the Privacy Officer? □ YES □ NO
If yes, what is the best way to contact you: _____

Have you discussed the above allegations with anyone else? If so, who? _____
_____

Do you have any further information to provide or any suggestions for verifying the allegations described above?
_____
_____

Are you aware of any other individuals who may be able to provide further information regarding the above allegations? If so, who? _____
_____

If you need more room, attach a separate piece of paper to this form. Please forward this form to the Privacy Officer or place in the Anonymous Reporting Box for suspected privacy violations.

BREACH NOTIFICATION

POLICY: Under the HIPAA Privacy Rule, the Center and its Business Associates are required to notify individuals in the event there is a breach of the individual's PHI. The Center will promptly notify all individuals of any breach in accordance with this policy.

DEFINITIONS:

Breach. The acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule and that compromises the security or privacy of the PHI. A breach does not include the following occurrences:

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

- Any inadvertent disclosure by a person who is authorized to access PHI at the Center or a Business Associate to another person authorized to access PHI at the Center or a Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

- A disclosure of PHI where the Center or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Unsecured PHI. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons.

PROCEDURE:

Upon identifying a breach, the Center must conduct a risk assessment to determine whether any potential breach actually constitutes a breach as defined under the Privacy Rule. If so, then the Center must take the following actions:

- The Center must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or HIPAA requirements.

- The Center must issue notification of the breach to the individual, or legal representative, within 60 calendar days after discovery by first class mail or, if specified by the individual, by email.

- The notification must include the following information:

    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - 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);
    - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
    - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

- If the Center lacks contact information, or the contact information is out-of-date, for fewer than 10 individuals, then the Center must send substitute notice to the individual through some form that is reasonably calculated to reach the individual.

- If the Center lacks contact information, or the contact information is out-of-date, for 10 or more individuals, then notification must be on the homepage of the Center's website, if any, for a period of 90 days or via conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The Center must include a toll-free number on the website that remains active for 90 days.

- If the breach involves more than 500 individuals, the Center must notify prominent media outlets within Ohio and the Secretary of the Department of Health and Human Services ("HHS").

- All breaches requiring notification, regardless of the number of individuals affected, must be reported to the Secretary of HHS within 60 calendar days of the end of the calendar year.

DISCIPLINARY POLICY FOR PRIVACY RULE VIOLATIONS

POLICY: The Center shall take appropriate disciplinary action against members of the workforce (employees, volunteers, trainees, etc.) who fail to comply with the HIPAA Privacy Rule and the Center's policies and procedures for protecting the confidentiality of a patient's PHI. The Center also acknowledges that violation of the federal law and regulations by a Part 2 program is a crime and is subject to federal penalties.

PROCEDURE:

1. During their HIPAA training sessions, workforce members will be made aware of the potential sanctions for violating HIPAA policies and procedures, including possible termination.

2. The employee may be subject to discipline, taking into account:

    a. the severity of the violation;

    b. whether the violation was accidental or intentional;

    c. whether the violation was part of a pattern of violations; and

    d. the Center's standard disciplinary process.

3. Disciplinary action may range from a verbal warning to termination.

4. A workforce member who reports suspected HIPAA violations to a governmental agency, accreditation organization, an attorney, or other agency or body under applicable whistleblower laws or regulations will not be disciplined for making the report.

5. Documentation of investigation and discipline shall be maintained for 6 years following the date of completion of the investigation or implementation of discipline.

DISCLOSURE TO FAMILY AND FRIENDS

POLICY: To establish a process for disclosing a patient's PHI to family members, relatives, or friends who are involved in the patient's care. Each client will be asked to sign an Authorization to Release Emergency Information form prior to the beginning of all treatment to ensure that the client gives consent to the facility to contact family or significant others in cases of emergency.

PROCEDURE:

1. If the patient is present (or otherwise available) and is capable of making decisions, then you must obtain the patient's agreement (can be oral), or provide the patient with an opportunity to object to the disclosure, or reasonably infer from the circumstances that the patient does not object to the disclosure before making any disclosure to the patient's family members or friends.

2. In the case of a patient who has been adjudicated as lacking the capacity, for any reason other than insufficient age, to their own affairs, any consent which is required under the regulations in this part may be given by the guardian or other individual authorized under state law to act in the patient's behalf.

3. In the case of a patient, other than a minor or one who has been adjudicated incompetent, that for any period suffers from a medical condition that prevents knowing or effective action on their own behalf, the Knox County Community Health Center program director may exercise the right of the patient to consent to a disclosure for the sole purpose of obtaining payment for services from a third-party payer.

4. If you suspect that an incapacitated individual is a victim of domestic violence and that the person seeking information about the individual may have abused the patient, do not disclose the information to the suspected abuser. Consult legal counsel.

5. Upon receipt of written authorization, the facility administrator or designee will contact the patient's family or significant other in the following cases/circumstances: (which shall be entered in the patient's clinical record):
   a. Patient injury requiring medical care;
   b. Accidents or incidents involving the patient;
   c. Patient transfer; and
   d. Patient death (in certain circumstances only the Medical Examiner's Office may contact the family or next of kin about death).

DISCLOSURES TO PERSONAL REPRESENTATIVES

POLICY: To allow for disclosures of a patient's PHI to the patient's personal representative as permitted under the HIPAA Privacy Rule.

PROCEDURE:

1. "Personal representatives" include individuals designated as the patient's attorney-in-fact under a durable power of attorney for health care, parent (or guardian) of a minor, court-appointed guardian, or the executor or administrator of a deceased patient's estate.

2. The Center shall treat a personal representative the same as the patient with respect to disclosing the patient's PHI.

3. The Center must verify the personal representative's identity and authority to act on behalf of the individual according to the Verification Policy.

4. Abuse, Neglect and Endangerment Situations - Do not disclose an individual's PHI to his or her personal representative if you have reason to believe that:

    a. the patient has been or may be subjected to domestic violence, abuse, or neglect by the personal representative, or treating such individual as the personal representative could endanger the patient; and

    b. you determine, in the exercise of professional judgment, that it is not in the best interest of the patient to treat the individual as the patient's personal representative.

RIGHT TO REQUEST RESTRICTIONS

POLICY: To allow patients to restrict the use or disclosure of their health information in accordance with the HIPAA Privacy Rule.

PROCEDURE:

1. An individual has the right to request a restriction on the use or disclosure of his or her health information: (a) for treatment, payment, or health care operations, and (b) to family and friends involved in the individual's care.

2. When an individual requests a restriction, the person receiving the request should complete the "Request for Restrictions" form and obtain the individual's signature. Place the completed form in the patient's medical record.

3. Although the Center does not generally have to honor restriction requests (subject to Section 4, below), it shall honor all reasonable requests, except that the individual may not restrict information disclosed to HHS for compliance purposes and other disclosures required by law.

4. The Center must agree to the request of a patient to restrict disclosure of PHI about the patient to a health plan if: (a) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (b) the health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

5. In emergency situations, where the individual needs emergency care and the restricted information is needed to provide the care or disclose information to another health care provider, you do not have to follow the agreed-upon restrictions. If restricted information is disclosed to a health care provider for emergency treatment, you must request that the health care provider not further use or disclose the information.

6. The Center may terminate a restriction that it was not legally required to agree to under Section 4 if:
   a. the individual agrees or requests the termination in writing; or
   b. the individual orally agrees to the termination and the oral agreement is documented; or
   c. you inform the individual that you are terminating its agreement to a restriction, except that the termination is only effective with respect to health information received after you have informed the individual.

7. Document and retain agreed-upon restrictions (in written or electronic form) and an individual's oral agreement to terminate a restriction for 6 years from the date created or last date of use, whichever is later.

8. Denying Restrictions. If, within your professional judgment, a request for restriction should be denied, please contact the Privacy Officer for guidance. If denied, please notify the individual requesting the restriction of the denial.

9. Notifying Others. Business Associates of the Center who use or disclose the patient's PHI must be notified of and abide by any agreed to restrictions.

KNOX COUNTY COMMUNITY HEALTH CENTER
REQUEST FOR RESTRICTIONS

Please indicate below the restrictions you are requesting on the use and disclosure of your health information. Attach a separate page if needed. We do not have to honor any request other than a request not to send information to an insurer for a claim paid out of pocket. If we agree to the restriction, then we are bound to follow it. If we deny the restriction, we will notify you of the denial. We reserve the right to terminate an agreed-to restriction if we feel that the termination is appropriate, and you have the right to terminate, in writing, any restriction by sending a termination notice to the Center.

Requested Restriction:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Print Name: _____

Signature: _____

Date: _____

If legal representative, relationship to patient: _____

****

FOR CENTER USE ONLY:

Restriction □ Accepted □ Denied

Print Name: _____

Signature: _____

Date: _____

-Place this form in the patient's record-

DISCLOSURES TO HEALTH OVERSIGHT AGENCIES

POLICY: To allow for the disclosure of a patient's health information to agencies involved in health oversight activities as permitted or required by the HIPAA Privacy Rule.

PROCEDURE:

1. Contact the Privacy Officer if you receive a request for a patient's PHI from a health oversight agency.

2. The Privacy Rule allows you to disclose a patient's PHI to a health oversight agency for oversight activities authorized by law, including audits, civil, administrative, or criminal investigations, inspections, licensure or disciplinary actions, civil, administrative, or criminal proceedings or actions, or other activities necessary for appropriate oversight of the health care system.

MARKETING/SALE USES AND DISCLOSURES

POLICY: The Center shall limit the use and disclosure of PHI for marketing activities to that permissible under the HIPAA Privacy Rule. The Center does not sell PHI. If the Center decides to sell PHI, it shall limit the use and disclosure of PHI for sales activities to that permissible under the HIPAA Privacy Rule. Per ORC §5119.27(A), the Center will not disclose records or information for marketing purposes pertaining to the identity, diagnosis, or treatment of any person seeking or receiving services that are maintained in connection with the performance of any drug treatment program or services licensed by, or certified by, the director of mental health and addiction services.

PROCEDURE:

1. Marketing means a communication about a product or service that encourages recipients to purchase or use the product or service.

2. Marketing General Rule - Authorization is Required. The Center may not use or disclose an individual's health information for marketing unless the individual first signs a HIPAA Authorization Form specifically allowing the use or disclosure.

3. Marketing Exceptions – When Authorization is not Required. Patient authorization is not required for the following:

    a. Face-to-face disclosures.

    b. A promotional gift of nominal value provided by the Center.

    Patient authorization is also not required to make the following communications to individuals because they are not considered marketing:

    a. Communications about a participating provider and health plans in a network, the services offered by a provider, or the benefits covered by a health plan;

    b. Communications about the individual's treatment; and

    c. Communications about case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual.

4. Sale Rule - Authorization is Required. The Center may not sell an individual's health information unless the individual first signs a HIPAA Authorization Form specifically allowing the sale. In addition, the Authorization must notify the individual that the Center will receive remuneration for the sale.

FUNDRAISING USES AND DISCLOSURES

POLICY: The Center does not do any fundraising. If the Center decides to fundraise, the Center shall limit the use and disclosure of patient health information for fundraising activities to that which is permissible under the HIPAA Privacy Rule as described in this policy. Per ORC §5119.27(A), the Center will not disclose records or information for fundraising purposes pertaining to the identity, diagnosis, or treatment of any person seeking or receiving services that are maintained in connection with the performance of any drug treatment program or services licensed by, or certified by, the director of mental health and addiction services.

PROCEDURE:

1. Fundraising means any appeal for money or other donations, sponsorship of events, etc. that is undertaken on behalf of the Center.

2. No Authorization Needed. The only information the Center may use or disclose for fundraising activities is (a) the individual's demographic information (e.g. name, address, other contact information, age, and date of birth); (b) dates of care provided; (c) department of service; (d) treating physician; (e) outcome of treatment; and (f) health insurance status if this information does not violate ORC §5119.27(A). The Center does not need to obtain the individual's authorization to use or disclose this information to a Business Associate or related foundation raising funds for the Center.

3. Authorization Needed. If the Center wishes to use or disclose an individual's health information for fundraising activities other than as described in Section 2, above, it must first obtain a signed HIPAA Authorization Form from the individual specifically allowing the use or disclosure.

4. Required Notice to Individual. The Center's Notice of Privacy Practices shall include a statement that it may contact the individual to raise funds and how the individual can opt-out of receiving fundraising materials.

   The Center will also include the following statement in any fundraising materials it sends to an individual of how the individual may opt-out of receiving further information:

   > You have the right to request that we not send you any future fundraising materials and we will use our best efforts to honor such request. You may make the request by sending your name and address to the Center's Privacy Officer at: 11660 Upper Gilchrist Road, Mount Vernon, Ohio 43050, together with your request to be removed from our fundraising mailing and contact lists. Treatment or payment will not be conditioned on your choice with respect to receipt of fundraising communications.

5. The Center shall not send any fundraising materials to an individual who has indicated that he or she does not want to receive this information (e.g. opted-out).

6. The Center may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications in the future. Please note, an individual must take an affirmative step to opt back into receiving fundraising communications. Making a donation is not, in and of itself, sufficient to opting back into receiving fundraising communications.

RESEARCH USES AND DISCLOSURES

POLICY: The Center does not perform research. If the Center decides to perform research, the Center shall limit the use and disclosure of patient health information for research to that which is permissible under this policy. Disclosure of a patient's record may be made without the person's consent to qualified personnel for the purpose of conducting scientific research, as long as the personnel does not identify, directly or indirectly, any individual person in any report or otherwise disclose a person's identity in any manner.

PROCEDURE:

1. Center may use or disclose PHI for research, regardless of the source of funding of the research, provided that:
    a. Center obtains documentation that an alteration to or waiver, in whole or part, of the individual authorization required by the HIPAA Privacy Rule has been approved by a privacy committee of the Governing Body that has:
        i. Members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
        ii. Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
        iii. Does not have any member participating in a review of any project in which the member has a conflict of interest.
    b. Reviews preparatory to research: Center obtains from the researcher representation that:
        i. Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
        ii. No PHI is to be removed from the Center by the researcher in the course of the review; and
        iii. The PHI for which use or access is sought is necessary for the research purposes.
    c. Research of decedent's information: Center obtains from the researcher:
        i. Representation that the use or disclosure sought is solely for research on the PHI of decedents;
        ii. Documentation, at the request of Center, of the death of such individuals; and
        iii. Representation that the PHI is necessary for the research purposes.

2. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation must include all the following:
    a. A statement identifying the privacy committee and the date on which the alteration or waiver of authorization was approved;
    b. A statement that the privacy committee has determined that the alteration or waiver, in whole or part, of authorization satisfies the following criteria:
        i. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
            A. An adequate plan to protect the identifiers from improper use and disclosure;
            B. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
            C. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted
        ii. The research could not practicably be conducted without the waiver or alterations; and
        iii. The research could not practicably be conducted without access to and use of the protected health information
    c. A brief description of the protected health information for which use or access has been determined to be necessary by the privacy committee has determined;

d. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as follows:
    i. The privacy committee must review the proposed research at convened meetings at which a majority of the privacy committee members are present, including at least one member who satisfies the criterion mentioned above, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy committee elects to use an expedited review procedure;
    ii. The privacy committee may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy committee elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy committee as designated by the chair; and
e. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the Governing Board or the privacy committee, as applicable;
f. Statements that the patient received information to help determine whether or not to participate in the data study and that the patient was informed that refusing to participate or to discontinue his or her participation in the study will in no way jeopardize their access to care, treatment & services unrelated to the data study; and
g. The name of the staff that provided the form and the date that the form was signed.

3. Patient authorization required. Patient authorization is required where compensation received for research involving disclosure of PHI is greater than a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes. The authorization must include a statement that disclosure will result in remuneration to the Center.

4. Research under 42 CFR part 2. Notwithstanding the provisions otherwise contained herein, the Center recognizes that, under certain circumstances, federal law requires additional and/or different disclosure requirements and limitations when the subject information is governed by 42 CFR part 2. Specifically, information can be disclosed to a researcher as provided herein so long as the research project meets the research requirements in the HIPAA Privacy Rule or the Health and Human Services regulations regarding the protection of human subjects, as applicable. Disclosure may be:
    a. To a HIPAA-covered entity or business associate that has obtained and documented authorization from the patient, or a waiver or alteration of authorization, consistent with the HIPAA Privacy Rule;
    b. Subject to the HHS regulations regarding the protection of human subjects, with a requirement that the researcher comply with 45 CFR part 46, including the requirements related to informed consent or a waiver of consent (45 CFR 46.111 and 46.116) or that the research qualifies for exemption under the HHS regulations;
    c. Subject to the FDA regulations regarding the protection of human subjects, with a requirement that the researcher comply with FDA regulations, including the requirements related to informed consent or an exception to, or waiver of, consent (21 CFR part 50); or
    d. Any combination of the foregoing as provided in 45 CFR part 2, §2.52.

As provided in 42 CFR part 2, any individual or entity conducting scientific research using patient identifying information protected by Part 2:
    a. Is fully bound by the regulations of Part 2;
    b. May not redisclose PHI except back to the Center;
    c. May include Part 2 data in research reports only in aggregate form in which patient identifying information has been rendered non-identifiable;
    d. Must maintain and destroy patient identifying information in accordance with the security policies and procedures established Part 2; and
    e. Must retain records in compliance with all federal and state record retention laws.

GENERAL HIPAA SECURITY POLICY

POLICY: It is the policy of the Center to: (1) ensure the confidentiality, integrity, and availability of all electronic PHI created, received, maintained, or transmitted by the Center; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule; and (4) ensure compliance with the HIPAA Security Rule by its workforce.

PROCEDURE:

1. The Center has implemented and will continue to implement all required security standards, measures, and implementation specifications contained in the administrative, physical, and technical safeguard sections of the HIPAA Security Rule and 42 CFR part 2. These include:

    a. Transferring and removing paper or electronic records;

    b. Destroying paper records, including sanitizing the hard copy media or electronic media associated with the paper printouts or on which the records are stored, to render the patient identifying information non-retrievable;

    c. Maintaining paper records in a secure room, locked file cabinet, safe, or other similar container, or storage facility when not in use;

    d. Using and accessing electronic records or other electronic media containing patient identifying information; and

    e. Using and accessing workstations, secure rooms, locked file cabinets, safes, or other similar containers, and storage facilities that use or store such information; and

    f. Rendering patient identifying information non-identifiable in a manner that creates a very low risk of re-identification (e.g., removing direct identifiers).

2. In implementing security standards, measures, and implementation specifications, the Center has taken into account the following factors:

    a. the size, complexity, and capabilities of the Center;

    b. the Center's technical infrastructure, hardware, and software capabilities;

    c. the costs of security measures; and

    d. the probability and criticality of potential risks to electronic PHI.

3. With respect to those addressable (but not required) implementation specifications in the HIPAA Security Rule that the Center has not implemented, the Center has:

    a. assessed whether such specifications would be reasonable and appropriate safeguards (when analyzed with reference to the likely contribution to protecting electronic PHI); and

    b. determined that implementation of said specifications is not reasonable and appropriate based on the 4 factors listed above in #2.

In addition, the Center has determined that there are not any reasonable or appropriate equivalent alternative measures available to implement.

CLIENT RECORDS MAINTENANCE PROCEDURES

POLICY: It is the policy of Knox County Community Health Center to maintain, retain and dispose of client records in accordance with the Ohio Department of Mental Health & Addiction Services regulations and federal, state and/or local laws. The privacy of each client will be protected at all times to maintain confidentiality. It is the policy to secure client records from unauthorized access and to maintain records in accordance with Ohio State Regulations.

PROCEDURE:

To maintain integrity against loss, damage, unauthorized alteration, unintentional change, and accidental destruction the client /participant records will be kept secure from unauthorized access and maintained in accordance with Code 42 of the Federal Regulations, part 2.

The facility has record management procedures regarding content, organization and use of records. The record management system meets the following additional requirements:

1. The Clinical Director has been designated as the keeper of the Medical Records and is responsible for the Medical Records System.

2. To protect against unauthorized access, use and disclosure of health information client records shall be kept secure. The client records shall be password protected and each therapist or staff member who needs access will have their own identifier code to permit entry into the system.

3. The EMR system shall remain locked at all times unless in use.

4. No client shall ever have access to the EMR.

5. No client records will ever be kept open in clinicians' or any staff office.

6. The organization will use health information only as authorized by the individual or otherwise consistent with law and regulation.

7. Records will not be released unless the organization is responding to law and regulation.

8. Original client records will be signed through electronic signatures.

9. In the event of an unforeseen power outage or the need for routine maintenance of the EMR System the organization will utilize a legible hard copy record system that will be stored in a locked file cabinet when not in use in accordance with HIPAA and any other relevant privacy laws until the backup system is up and running.

10. In those instances where records are maintained electronically, a staff identifier code will be accepted in lieu of a signature.

11. Documentation within records will not be deleted.

12. Amendments or marked-through changes will be initialed and dated by the individual making such changes.

13. Electronic clinical records are audited on a consistent basis for completeness, accuracy, and integrity by designated clinical staff members. The results of compliance rates with electronic chart audits are reported monthly to the Performance Improvement Committee by the Clinical Director.

    a. Audits may be conducted by any federal, state, or local government Center which provides financial assistance to the Center or is authorized by law to regulate its activities; or any individual or entity who provides financial assistance to the Center, which is a third-party payer covering patients in the Center, or which is a quality improvement organization performing a utilization or quality control review; or Is determined by the Part 2 program to be qualified to conduct an audit or evaluation of the Center.
    b. Auditors may only remove patient identifying information from the Center’s premises

if the auditor agrees in writing to maintain and destroy the patient identifying information, retain records in compliance with applicable federal, state, and local record retention laws, and disclose patient identifying information back to the program from which it was obtained.

RECORDS RETENTION AND DISPOSITION

POLICY: It is the policy of Knox County Community Health Center that in the case of individual client/participant records, records will be retained for a minimum of seven years. The disposition of client/participant records will be carried out in accordance with Title 42, Code of Federal Regulations, part 2.

PROCEDURE:

1. Medical records, clinical records and will be retained for a minimum period of seven (7) years.

2. All clinical records will remain in a secure area of the facility for a period of three (3) years of inactivity. If such chart has no activity in three (3) years, the chart will be moved to storage or e-storage for at least four (4) additional years.

3. If at any time within those seven (7) years, the client returns, the record will be pulled and incorporated into Knox County Community Health Center's paperless charts and the count begins over again from the most recent treatment episode.

4. If the chart has remained inactive for seven (7) years after discharge, the chart will then be purged and destroyed.

5. Records will be destroyed by shredding. The Center shall contract with an independent company for destruction of medical records. Destruction of records will include sanitizing the hard copy media associated with the paper printouts, to render the patient identifying information non-retrievable.

6. The facility will maintain a list of all closed medical records kept both on-site and off-site.

7. The facility will maintain a list of destroyed Medical Records.

8. The facility shall inform the Ohio Department of Mental Health & Addiction Services of the secured storage location and the manner in which records are destroyed as soon as that information is available and upon request.

9. If a chart is too thick, a second volume will be started and the volume will be indicated on the outer jacket of the chart.

10. Documentation within records will not be deleted until record is properly destroyed.

RISK ANALYSIS

POLICY: The Center shall conduct, as necessary, an accurate and thorough risk assessment to determine potential threats to the confidentiality, integrity and availability of electronic protected health information as one administrative safeguard implemented to prevent, detect, contain, and correct security violations.

PROCEDURE:

1. The Center has an accurate understanding of the technical and non-technical components of its security environment related to electronic PHI.

2. The Center reviews and implements the standards and implementation specifications of the HIPAA Security Rule.

3. A Risk Analysis Management Report summarizes the findings of the risk analysis.

4. The Risk Analysis Management Report is retained for 6 years from the date completed or last updated, whichever is later.

5. The Risk Analysis Management Report is reviewed periodically to audit the Center's continued compliance with the Security Rule and its effectiveness in reducing security risks.

RISK MANAGEMENT

POLICY: The Center shall select and implement security measures sufficient to reduce risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI to a reasonable and appropriate level as one administrative safeguard implemented to prevent, detect, contain, and correct security violations.

PROCEDURE:

1. An analysis of the data collected during the risk analysis identifies the risks and vulnerabilities of the electronic PHI stored, processed, and transmitted by the Center.

2. Decisions made regarding the implementation of security measures to manage identified risks are based on the security requirements of the standards and implementation specifications of the HIPAA Security Rule.

3. Reasonable and appropriate risk management decisions are made taking into consideration the Center's size, complexity, technical capabilities, risk analysis, and the costs of security measures.

4. Documentation of selected and implemented security measures is included in the Center's Risk Analysis Management Report.

5. The effectiveness of implemented security measures are audited during annual evaluations of the Center's security environment.

INFORMATION SYSTEM ACTIVITY REVIEW

POLICY: Records of information system activity are reviewed on a regular basis as one administrative safeguard designed to prevent, detect, correct and contain security violations.

PROCEDURE:

1. The Compliance Officer is responsible for coordinating the review of records of information system activity.

2. The Center has the following capabilities for reviewing information system activity: (a) audit logs; (b) access reports; (c) security incident logs; (d) paper based logs; and (e) other internal security controls and monitoring tools.

3. A random sample of records of information system activity is reviewed quarterly.

4. Records of information system activity are used as needed and appropriate to investigate root causes of reported or suspected security incidents or security violations.

5. Workplace members are periodically reminded that records of information system activity are reviewed on a regular basis.

INFORMATION ACCESS MANAGEMENT

POLICY: As one administrative safeguard designed to prevent, detect, correct and contain security violations, access to electronic PHI is authorized, established, maintained, and modified based on the minimum amount of PHI necessary for individual members of the workforce to perform their jobs effectively.

PROCEDURE:

1. Authorization to access electronic PHI is consistent with the Center's documented determinations of the minimum amount of PHI needed by a workplace member to perform his or her job effectively under the Privacy Rule.

2. After access privileges have been authorized, a user account is established that enables a workplace member to access electronic PHI and the Center's information systems as appropriate to his or her job function.

3. Documentation is maintained of all user accounts and authorized access privileges.

4. Reviews of access rights and user accounts are conducted quarterly to ensure continued appropriateness of accounts and levels of access.

5. Access privileges are modified or revoked whenever a user's job function or access needs change. Modifications to user accounts are made with appropriate authorization.

6. Access privileges are revoked when a user is no longer employed by the Center. This revocation occurs on the effective date of the user's end of employment or sooner if warranted by circumstances.

7. The Center's Privacy officer and personnel responsible for information technology shall implement periodic security updates, procedures for guarding against, detecting, and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords.

8. This policy and procedure is designed and implemented: (a) to ensure that all members of the workforce have appropriate access to electronic PHI; and (b) to prevent those workforce members who do not have access from obtaining access to electronic PHI.

DISCIPLINARY POLICY FOR SECURITY RULE VIOLATIONS

POLICY: The Center shall take appropriate disciplinary action against members of the workforce (employees, volunteers, trainees, etc.) who fail to comply with the HIPAA Security Privacy Rule and the Center's policies and procedures for protecting the confidentiality of a patient's electronic PHI.

PROCEDURE:

1. During their HIPAA training sessions, workforce members will be made aware of the potential sanctions for violating HIPAA and 42 CFR part 2 policies and procedures, including possible termination.

2. The employee may be subject to discipline, taking into account:

    a. the severity of the violation;

    b. whether the violation was accidental or intentional;

    c. whether the violation was part of a pattern of violations; and

    d. the Center's standard disciplinary process.

3. Disciplinary action may range from a verbal warning to termination.

4. A workforce member who reports suspected HIPAA violations to a governmental agency, accreditation organization, an attorney, or other agency or body under applicable whistleblower laws or regulations will not be disciplined for making the report.

5. Documentation of investigation and discipline shall be maintained for 6 years following the date of completion of the investigation or implementation of discipline.

SECURITY INCIDENT PROCEDURES: RESPONSE AND REPORTING

POLICY: As one administrative safeguard designed to prevent, detect, correct, and contain security violations, the Center addresses security incident procedures as required by the HIPAA Security Rule.

PROCEDURE:

1. Workplace members are trained to report suspected or known security incidents to the Compliance Officer.

2. Security incidents are documented on the Security Incident Report Form.

3. The Compliance Officer conducts an investigation of all security incidents.

4. An appropriate response to the security incident is determined by the Compliance Officer and/or designated personnel based upon the nature and severity of the security incident. Responses may include, but not be limited to, the application of sanctions against personnel, initiation of security reminders, additional training or an evaluation of the adequacy of security measures.

5. Any harmful effects of security incidents that are known to the Center are mitigated to the extent practicable.

6. All security incidents and their outcomes are documented in the Security Incident Log.

7. The Security Incident Log is reviewed on a regular basis and during the security evaluations conducted by the Center to determine and ensure the adequacy of security measures and compliance with the Security Rule.

8. Documentation related to security incidents and their outcomes for 6 years from the date of occurrence of the incident.

CONTINGENCY PLAN

POLICY: As one administrative safeguard designed to prevent, detect, correct, and contain security violations, the Center maintains a contingency plan to respond to emergencies, disasters, and other occurrences that damage systems containing electronic PHI in accordance with this policy and the HIPAA Security Rule.

PROCEDURE:

1. The contingency plan for electronic PHI is a component of the Center's emergency preparedness plan.

2. Copies of the contingency plan for electronic PHI are maintained off-site in secure, accessible locations.

3. Members of the workforce receive training appropriate for implementing the Center's contingency plan procedures.

4. The contingency plan for electronic PHI includes:

    a. an assessment and summary of the results of an applications and data criticality analysis;

    b. a data backup plan that includes procedures for creating, maintaining and retrieving exact copies of electronic protected health information;

    c. a disaster recovery plan that includes procedures for restoring data that may be lost during a major disaster;

    d. an emergency mode operation plan that provides procedures for protecting the security of electronic protected health information while operating in emergency mode; and

    e. procedures for testing and revising the contingency plan to ensure it is effective and kept up to date.

EVALUATION PLAN

POLICY: As an administrative safeguard, the Center shall evaluate its safeguards under the HIPAA Security Rule and perform an annual technical and non-technical evaluation to establish the extent to which its policies and procedures meet HIPAA Security Rule requirements.

PROCEDURE:

1. The Compliance Officer coordinates the resources necessary to evaluate the Center's security environment and compliance with the HIPAA Security Rule annually.

2. An evaluation is conducted whenever there are environmental or operational changes affecting the electronic protected health information created, received, maintained or transmitted by the Center.

3. Evaluations that include a review of the technical and non-technical components of the Center's security environment and compliance with the requirements of the HIPAA Security Rule are conducted annually.

4. The results of the evaluations are documented and retained for 6 years from the date the evaluation was conducted.

PHYSICAL SAFEGUARDS

POLICY: The Center shall implement physical safeguards to prevent, detect, contain and correct any HIPAA Security Rule violations in accordance with this policy.

PROCEDURE:

1. Facility Access Controls.

   a. The Center maintains a Facility Security Plan to document physical security measures intended to prevent unauthorized access to the Center's facility and tampering or theft of its equipment while ensuring that properly authorized access is allowed.

   b. To ensure that only authorized individuals have access to the Center's facility and electronic information systems, access is controlled and validated by:

      i. ID badges;
      ii. Magnetic card readers;
      iii. Security guards; or
      iv. Receptionists.

   c. Visitors to the facility are required to sign a log that records the time of arrival and departure.

   d. Visitors to the facility must be escorted as appropriate and, if working near or with electronic protected health information, have appropriate authorization and/or supervision.

   e. A log is kept to document all facility repairs or modifications that are related to security.

   f. Temporary authorization to access the Center's facility and electronic information systems is granted to repair personnel or technicians during emergencies for the purpose of restoring lost data or repairing damaged equipment.

2. Workstation Use and Workstation Security.

   a. Guidelines for the acceptable use of workstations (including desktops, laptops and hand-held devices) that contain or have access to electronic PHI are provided to workplace members.

   b. Training is provided to workplace members on the guidelines for acceptable use of workstations.

   c. Additional training is provided as needed to ensure authorized users understand necessary procedures for compliance with the guidelines (for example, enabling password protected screensavers or log-off procedures).

   d. Physical safeguards for workstations that are implemented to restrict access to authorized users include:

      i. Secure locations;
      ii. Locking devices;
      iii. Password protection;
      iv. Screen time-outs; and
      v. Shielding monitors from plain view.

3. Device and Media Controls.

   a. An accurate inventory of the Center's hardware and electronic media is maintained and updated by the Compliance Officer.

   b. A log is maintained by the Compliance Officer of the movement of hardware and

electronic media that contain electronic protected health information into, out of and within the facility.

c. A retrievable, exact backup copy of electronic protected health information is created before moving equipment that may result in damage or the loss of data.

d. Electronic protected health information that is stored on the hard drives of computers or other electronic media is removed before the disposal or re-use of the hardware or electronic media.

e. Electronic PHI is removed from hard drives or electronic media by _____ _____ [e.g. examples include but are not limited to scrubbing, purging, and/or disposing of electronic protected health information].

f. The effective removal of electronic PHI from hardware or electronic media is verified by the Compliance Officer prior to disposal or re-use.

TECHNICAL SAFEGUARDS

POLICY: The Center shall implement technical safeguards to prevent, detect, contain, and correct any HIPAA Security Rule violations in accordance with this policy.

PROCEDURE:

1. Technical Access Controls.

   a. Unique User Identification.

      i. Workforce members who are authorized to access electronic protected health information are assigned a unique User ID that enables the Center's information system to identify, authenticate and track user identity.
      ii. User accounts are established that are consistent with administrative policies and procedures that authorize and grant access privileges.
      iii. Access control lists are maintained and updated as needed and technical modifications to user accounts are provided in a timely manner when access privileges are terminated or changed.

   b. Emergency Access Procedure.

      i. Temporary access to electronic protected health information or the Center's information systems are provided in emergencies.
      ii. The Center's Contingency Plan describes the Center's emergency access procedures.

2. Integrity of Electronic Protected Health Information. These HIPAA Policies and Procedures are designed to protect electronic protected health information from improper alteration or destruction.

3. Person or Entity Authentication.

   a. A unique User ID is assigned to workplace members who are authorized to access the Center's information systems and electronic protected health information.

   b. Workplace members may not allow anyone to use their User ID to gain access to the Center's information systems under any circumstance without authorization from the Compliance Officer.

   c. Workplace members may not misrepresent themselves to the Center's information systems by using another person's User ID.

   d. Workplace members are required to follow any password management policies and procedures to create and safeguard their User ID to prevent unauthorized access to the Center's information systems.

4. Transmission Security.

   a. Electronic PHI may only be transmitted to authorized parties.

   b. When electronic PHI must be transmitted in email communications, only the minimum amount of PHI needed to achieve the purpose of the communication may be transmitted.

   c. A compatible encryption method must be coordinated with the recipient of email communications containing PHI that is transmitted over an electronic network.

   d. When transmitting protected health information in email communications, the following statement must be included in the email as an extra precaution:

      Confidentiality: This email message, including any attachment(s), is for the sole use of the intended recipient(s) and may contain confidential information. Any unauthorized review, use, disclosure or distribution is strictly prohibited. If you are not the intended recipient, please immediately contact the sender and destroy all copies of this email.