Pathways

CONFIDENTIALITY AND PRIVACY

UPDATED 4.13

Privacy Practices

- **<u>What are the Pathways Privacy practices?</u>**
- The Pathways Privacy Practices are a compilation of three different laws which protect the confidentiality of recipient information and apply to all classifications of staff members associated with Pathways. These statutes are:
- **45 CFR Part 164 (HIPPA)**
- **Michigan Mental Health Code Section 748**
- **42 CFR Part 2 (Substance Abuse)**

Similar, yet different

- All people who receive services through Pathways have a right to confidentiality – the laws that protect this right are HIPAA and the Michigan Mental Health Code.
- Those who receive co-occurring services (mental health and substance abuse) are protected by HIPAA, the Mental Health Code and the federal substance abuse confidentiality law and regulations – 42 CFR Part 2.

42 CFR Part 2

- To be protected by 42CFR Part 2, the substance abuse diagnosis must be made for the purpose of alcohol/drug treatment or referral for treatment.
- Diagnosis alone does not trigger 42CFR2.
- Anyone who has ***applied for*** or ***received*** any sort of individual service relating to drug or alcohol abuse – treatment, counseling and/or diagnosis is protected.

What information is protected?

- All information and communication concerning the recipient including but not limited to the following:
- The name of the recipient.
- The fact that a person is receiving mental health services.
- Information related in confidence.
- Information in the designated record set (any item, collection, or grouping of information that includes protected health information).
- Observation of the recipient.
- Other information received while providing services.

When May Information be Released?

- When it is **authorized** by the recipient (or guardian if applicable) or it is **mandatory** under state or federal laws.
- Examples of mandatory disclosure are:
- Court orders
- Reporting Abuse or Neglect
- Referrals to Protective Services

When can information be exchanged within Pathways

- If staff **need to know** the information to do their job they are given access to the **minimum necessary** amount of information according to their job classification.

What is a QSOA/BAA

- Qualified Service Organization (42CFR Part 2)
- Business Associate (HIPAA)
- A written agreement that allows programs to disclose information without the recipient's consent to an outside organization that provides services to the program or to the program's recipients.

Examples of QSOA/BAA

- Data processing
- Laboratory analyses
- Patient transportation
- Attorney
- CPA
- Medical/health care
- BUT!!! If two substance abuse providers contract with each other, protected health information can not be shared unless the recipient authorizes it.

Special Consideration with co-occurring recipients

- All recipients must sign the specific consent to release information regarding substance abuse information.
- Recipients age 14 and older must sign for themselves. The rule of thumb is – if the parent/guardian signs for service, have both the child and the parent sign authorizations to release information.
- Clinicians must make sure that recipients understand their rights specific to releasing substance abuse information.

Revocation of Release

- Co-occurring recipients can revoke consent orally or in writing.
- Other recipients must revoke in writing.

Exceptions

- Limited exceptions to confidentiality apply when:
  - Crime on Premises/Threats to staff
  - Medical Emergencies
  - Initial report of Suspected *Child* Abuse or Neglect
  - Vulnerable Adult Abuse/Neglect – if it's a co-occurring recipient, contact the Office of Recipient Rights for assistance.

Exceptions

- Even without consent, patient-identifying information may be disclosed to certain persons in the event of a medical emergency that.....
  - Poses an immediate threat to the health of an individual
  - Requires immediate medical intervention
- The release is to medical personnel only -- those who need the information in order to treat the threatening medical condition
  - But NOT family members (unless there's a release)
  - NOT "emergency contacts" (only if there's a release)

Subpoena

- You are served with a subpoena that directs you to appear in court with your entire file on a particular recipient and testify about the records in the file.
- You get a subpoena in the mail that directs you to turn over your entire file on a particular patient to an attorney.
- Should you turn the records over and testify? NO
- The agency attorney must be contacted prior to responding to a subpoena.

Duty to Warn

- The following elements, at a minimum, need to be present for the Duty to Warn to take effect:
- A threat of physical violence;
- Against a reasonably identifiable third person;
- With apparent intent;
- And ability to carry out the threat;
- In the foreseeable future

Duty to Warn

- If, in the judgment of the worker, there is a Duty to Warn, the following steps must be taken:
- Notify potential victim(s) and notify appropriate police authorities.
- Notify your supervisor. The supervisor will be responsible for notifying the CEO or designee.
- Evaluate for involuntary or voluntary hospitalization.
- Document everything in the client's progress notes, giving rationale for every decision.

Duty to Warn

- If the third party who is threatened is a minor or is considered incompetent by other than age, the worker must also:
- Communicate with the Department of Human Services.
- Communicate with the parent or legal guardian.

- FOR CO-OCCURRING RECIPIENTS, CONTACT THE OFFICE OF RECIPIENT RIGHTS.

Search Warrants

- If the search warrant is for a program or individual protected by 42 CFR Part 2, the law requires a specific court order - contact the agency attorney.
- Staff are not expected to resist police officers, however, an attempt should be made to notify the officer that the search may be improper.

How to protect confidentiality

- Develop good habits. Some examples are:
- Do not discuss recipient information at home
- Never identify an individual as a recipient
- Verify that there is a valid authorization in the recipient's chart before releasing information
- Review the agency Privacy Practices
- Lock all documents that contain protected health information

Breach Notification

- It is imperative that staff immediately notify their supervisor, ORR (Privacy Officer) and the Security Officer if there has been a breach of privacy or security.
- A breach is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under NorthCare Privacy Practices which compromises the security or privacy of the protected health information.

If there is a breach…

- we need to mitigate the risk,
- we need to do a risk assessment,
- we need to analyze if it is a reportable breach.

- If we have to report, it may be to the individual, or it could mean reporting it through the press. We also, have to report to Health and Human Services.
- We could have to pay a fine.

Privacy Rights

- It is important that you let Clinical Records/Privacy Officer know if someone asks:
- To receive a copy of their record;
- To amend their record;
- To learn who has received information from their record;
- To restrict who has access to their record

ORR

- This has been a brief review of Pathways Privacy Practices.
- The Privacy Practices are available on the Pathways Policy/Procedure Forum.
- Your local Office of Recipient Rights will assist you if you have questions regarding confidentiality.