PURPOSE:

To assure the protection of all client rights to privacy and define the process through which Federal Confidentiality Guidelines are implemented. In addition, Columbus House is committed to protecting the privacy and confidentiality of information collected, maintained, and shared through the Homeless Management Information System (HMIS) in accordance with applicable federal, state, and local laws, HUD HMIS Privacy and Security Standards, the HIPAA Privacy Rule (45 CFR Parts 160 and 164), and 42 CFR Part 2 when applicable.

POLICY:

Confidentiality is a fundamental component of quality services. It is therefore the policy of CH to safeguard the client right to privacy with respect to confidential information disclosed or revealed in the therapeutic setting.

CH recognizes that information entered into the Homeless Management Information System (HMIS) contains sensitive client data used for service coordination, program administration, reporting, and evaluation. All HMIS users shall access, use, disclose, and protect client information in accordance with HUD HMIS Privacy and Security Standards and agency policies. Client information contained within HMIS shall be limited to the minimum necessary to accomplish legitimate business purposes and shall only be accessed by authorized personnel with a demonstrated business need.

All employees, volunteers, interns, contractors, and other authorized users with access to HMIS shall complete required confidentiality, privacy, and HMIS security training prior to being granted system access and annually thereafter. Users must sign confidentiality agreements acknowledging their responsibility to protect client information and comply with all applicable privacy and security requirements.

To ensure that client confidentiality is protected, upon employment all staff members of CH will be required to review Federal Confidentiality Regulations relating to the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2 and other confidentiality laws that may be applicable at that time. After having reviewed said laws and regulations, the employee will be required to sign a statement acknowledging their understanding of this material, the implications contained therein, and that the employee agrees to abide by all applicable confidentiality and privacy regulations. A copy of this signed statement will be included in each employee's personnel file.

PROCEDURE:

Federal Confidentiality Regulations, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164) and 42 CFR Part 2 will define the basic framework within which all operating policies and practices of CH are to be conducted. Any exceptions to the contents of this policy are to be enacted only in accordance with relevant clauses contained within the Federal Confidentiality Regulations, and then only upon approval of the Chief Executive Officer. In the absence of the Chief Executive Officer, the Chief Program Officer will make such determinations as may be necessary.

The full text of the most recent federal confidentiality regulations will be available through the Chief Operating Officer and Chief Program Officer. In summary, these regulations state:

1) Program staff shall not convey to a person outside of the program that a client attends or receives services from the program or disclose any information identifying a client as an alcohol or other drug services client unless the client consents in writing for the release of information, the disclosure is allowed by a court order, or the disclosure is made to qualified personnel for a medical emergency, research, audit or program evaluation purposes.
2) Federal laws and regulations do not protect any threat to commit a crime, any information about a crime committed by a client either at the program or against any person who works for the program.
3) Federal laws and regulations do not protect any information about suspected child abuse or neglect, elder abuse or neglect or abuse and neglect of persons with developmental disabilities being reported under state law to appropriate state or local authorities

HMIS Privacy and Confidentiality

4) Client information collected and entered into HMIS shall be used only for purposes permitted by HUD regulations and agency policies, including the provision of services, care coordination, reporting, data analysis, and program evaluation.
5) Clients shall be informed of the collection and use of their information through the agency's HMIS Notice of Privacy Practices and any applicable HMIS Consent or Authorization forms. Clients shall be given the rights provided under applicable laws and regulations, including the right to request access to, correction of, or an accounting of disclosures of their information where applicable.
6) Access to HMIS shall be restricted through unique user credentials and role-based permissions. Users shall not share usernames or passwords, permit unauthorized individuals to access HMIS, or access client records for any purpose unrelated to their job duties.
7) Electronic client information maintained in HMIS shall be protected through physical, administrative, and technical safeguards designed to prevent unauthorized access, alteration, disclosure, or destruction of data. Such safeguards shall include password protection, secure workstations, encryption where appropriate, automatic logoff features, and regular security monitoring.
8) Any suspected or confirmed breach of HMIS confidentiality, privacy, or security, including unauthorized access, use, disclosure, or loss of client information, shall be reported immediately to the employee's supervisor, the HMIS System Administrator, and agency leadership. The agency shall investigate all reported incidents and take appropriate corrective action, including notification requirements as required by law or HMIS governing policies.
9) HMIS information may only be disclosed to participating agencies or other entities as authorized by applicable law, client consent, data-sharing agreements, court order, or other legal authority. All disclosures shall be limited to the minimum necessary information required to accomplish the intended purpose
10) Printed HMIS reports and documents containing client information shall be stored securely and destroyed in accordance with agency records retention and destruction policies when no longer needed.

Violation of client confidentiality, including HMIS privacy, confidentiality, or security requirements, by a staff member will result in disciplinary action up to and including termination of employment, revocation of HMIS access privileges, and any additional penalties permitted by law.

Except for situations previously referenced in this policy, and more fully described in the federal confidentiality regulations, confidential information held by CH may only be released or disclosed if the client in question has properly executed an Authorization to Use and Disclose Protected Health Information form. Said information to be released or disclosed may include only information accumulated through the client's involvement with CH. Reports from other organizations may be released only by the organization from which the report originated.

Clients who wish to communicate with Columbus House staff via text message must first have it explained that text messaging may be unsecured and as a result at risk of being viewed by a third party. If the client still wishes to use this form of communication, they must sign a Consent to Receive Text Messages form. This form will be placed in the client file.

Clients can refuse or rescind providing an Authorization of the Use and Disclosure of Protected Health Information without the fear of any retribution. If a client refuses to provide authorization, the subsequent consequences will be fully explained. If a client rescinds an authorization, the staff person will put a line through the middle of the release, write Rescinded and the date it was rescinded across the middle.

Authorization to Use and Disclose Protected Health Information forms shall contain the following information:

1) Name of the organization or person to whom information may be disclosed,
2) Extent and nature of the information to be disclosed,
3) Purpose for the disclosure,
4) Date upon which the authorization to disclose information automatically expires,
5) Signature of the client about whom information is to be communicated; or, in the case of a minor client, the signature of a legal guardian,
6) Prohibition on Re-disclosure Statement

Confidential client information may be disclosed among employees of the different departments comprising Columbus House only to the extent necessary for said employees to perform the expected functions of their employment. Graphically illustrated, confidential client information may be disclosed within a department and upwardly within the agency's internal table of organization. All other internal disclosures shall be limited to the extent necessary for the performance of one's position responsibilities.

Information to be released to other organizations must be disclosed only in accordance with this policy, and with the best interest of the client as a paramount factor. Such disclosures will contain only that information necessary to satisfy the professional obligations of Columbus House. Disclosure of incidental information shall be avoided whenever possible.

Authorized disclosures of confidential client information to other organizations will be conducted by the case manager who is primarily responsible for the treatment of said client. If this is not possible or prudent,

the Chief of Programs or Chief Operating Officer shall oversee the disclosure of confidential client information.

Confidential records are to be maintained in locked quarters within the agency at all times.

In accordance with state law with regards to confidentiality, a client may request information pertaining to their clinical record. Said request should be submitted in writing to the Chief Executive Officer.

Information will be released without a client's consent in the following situations:

1) When the client presents an immediate danger to themselves or others.
2) When the Court subpoenas client records.
3) When staff suspects child or elder abuse.