Confidentiality

Date of Origin: July 22, 2004
Modification Date(s): 4/14, 2/20/15, 5/13/19
Date of Last Review: 5/14/24
Policies Referenced: Client Records Policy

I. Purpose

To outline the expectations of UCP of Maine employees, volunteers and contractors regarding client and employee confidentiality

II. Definitions

Confidential Information - Information made confidential by law, such as "Protected Health Information" (PHI) under the Health Information Portability and Accountability Act of 1996 (HIPAA) or by UCP of Maine policies.

III. Policy

All information relating to UCP of Maine clients and family members, vendors and all employee records are confidential and must be treated as such. Confidential information may be information in any form including but not limited to written, electronic, oral, overheard or observed. Access to all information is granted on a need to know basis. A "need to know" is defined as information that is required in order to do your job. Access to any information not needed in order to perform your role at UCP is unacceptable.

Provision for the protection of the client's right to privacy shall be maintained at all times within the Agency. The client's right to privacy shall be paramount among staff and information will be shared for professional purposes and on a "need-to-know" basis only.

Employees/Volunteers/Contractors shall not access nor disclose confidential information during his/her employment or thereafter except as required in the performance of his or her job in accordance with law and UCP of Maine policies.

All employees, volunteers and contractors, regardless of job category, should appreciate the importance of maintaining confidentiality and the security of electronic protected health information, and understand that compliance with this and other security policies is required of UCP's Code of Conduct. Violation of UCP's security policies will be grounds for disciplinary action, up to and including termination.

Employees and contractors are not permitted to access confidential and protected health information for any individual that is not receiving services from the employee/contractor

as part of their regular job duties. Employees and contractors who wish to access information on themselves, family members or other individuals that they do not have a work-related need-to-know, must request such information following the Client Clinical Records policy and is never permitted to access such information independently regardless of relationship to the client/person.

All employees, volunteers and contractors will receive a general orientation to basic confidentiality and security training. Training will be updated regularly on an ongoing basis. UCP will maintain documentation on confidentiality and security awareness and training in UCP training files for employees and in volunteer and contractor files.

Basic confidentiality and security training includes but is not limited to:

- Accessing and disclosing confidential information on a need-to-know basis only
- Proper use of the computer system including email and the Internet
- Proper use of Secure Email
- Procedures for saving data to network drives
- Prohibition on improper copying of files and programs, or loading of unauthorized programs on the information system
- Prohibition on attempting access to electronic protected health information without authorization
- Precautions against malicious software, and procedures to follow if the individual suspects that malicious software has been introduced
- Password management

For employees and contractors with access to confidential and protected health information, additional security training will be conducted on the following:

- Proper use of security features of specific applications being used
- The necessity of maintaining the confidentiality of access codes and passwords
- Additional password management policies
- Reporting security incidents
- Reporting access issues
- Prohibition on attempting access to electronic protected health information not required for the job function
- Client Clinical Records policy
- Other electronic security policies

Employees, volunteers and contractors will review and sign UCP's Confidentiality and HIPAA Statement at hire/engagement and annually thereafter.

IV. Confidentiality and Electronic Technology

Employees will be granted access only to electronic systems required for the employee to perform their job. Volunteers will not have access to UCP's electronic systems that include confidential information. Contractors will only have access to UCP's electronic systems that include confidential information as needed to perform contracted services.

Any contractor that has access will receive a full orientation on UCP's confidentiality and IT access policies and will sign a Business Associate Agreement prior to engagement.

The Agency will protect confidentiality of clients and employees by limiting use of cellular phones, facsimile machines, automated information systems and/or technologies when possible. When portable (a.ka. jump or zip) drives are used, the portable drives must always be password protected and must always be a company-issued portable drive.

An employee or contractor who uses a cellular phone for work purposes is required to have a passcode to access information and for use of their phone. Any employee or contractor who uses email or other electronic communication devices is required to send confidential information only via Secure Email unless emails are going from one UCP outlook account to another UCP outlook account, in which case emails are already secure within the same server from employee to employee and secure email is not necessary. Confidential information (information that allows for identification of protected client or employee information) that is shared via email that is not sent via UCP's Secure email is considered a confidentiality breach and must be reported to the Director of Operations, as UCP's Privacy Officer.

Whenever possible, all information/messages need to be carefully considered and "de-identified" regarding client-specific information.

When a staff member ends employment with UCP of Maine, all confidential information must be immediately returned and secured prior to the individual's last day of employment and all client information contained on a personal cell phone must be deleted.

V. Client Records

All information in the client's record is privileged and confidential. Records are kept behind locked doors and are not available to unauthorized persons. Staff are strictly prohibited from accessing records that do not belong to clients they serve in any UCP provided electronic or paper health record, including HealthInfoNet (HIN). Staff must never access their own records or family member records on HIN for any reason, as this is strictly prohibited and may result in termination.

Release of information in a client's record is allowed only with the informed and written consent of the client or client's family/guardian. The expiration date placed on a release of information form should be an appropriate length of time directly related to the purpose of the release form, but never to exceed one year. Signed release of information forms will be updated yearly by the client's worker. In the case of client's inactive status, records will be released only upon presentation of a release with a current date (within one year).

Information in the record is released only after the requesting agency or individual documents the need and right to know.

Specific rules regarding the access, use and dissemination of client records is located in the **CLIENT CLINICAL RECORDS** policy.

It is always the prerogative of the client or parent/legal guardian as to whether or not information is released to another agency or individual, unless by court order, subpoena or statute. If at any time, an Agency worker has concern about this, they may contact the client or family to advise them that a request for information has been received from an agency or individual and ask for their consent to comply with the request.

VI. Use of Client Information in Supervisions

UCP will inform clients that their confidential information may be shared in supervision and consultation to improve the quality of the service(s) being provided.

VII. Reporting of Confidentiality Violations

Any employee, volunteer or contractor who becomes aware of a potential or actual confidentiality or HIPAA violation should immediately report the violation to the Director of Operations, UCP's Privacy Officer.

Scott Tash, CEO

5/20/24
Date

CONFIDENTIALITY & HIPAA STATEMENT

All information relating to UCP of Maine, its clients, vendors and all employee records are confidential and Employees/Volunteers/Contractors must, therefore, treat all matters accordingly. Such information is made confidential by law (such as "protected health information" under the Health Information Portability and Accountability Act of 1996 (HIPAA) or by UCP of Maine policies). Confidential information includes, but is not limited to personally identifiable information such as name, address, social security number, dates of birth, diagnosis, medications, treatment plans, medial history, etc. Confidential information may be information in any form including but not limited to written, electronic, oral, overheard and observed. Access to all information related to UCP of Maine, its clients, vendors and employees is granted on a need to know basis. A "need to know" is defined as information that is required in order to do your job. Such information needs to be properly protected by individuals who have access to the information.

Employees/Volunteers/Contractors shall not, during employment/engagement and thereafter, disclose to others or use any confidential information except as required in the performance of his or her job and in accordance with law and UCP of Maine policies.

If employee or client information is not needed to fulfill a function of your position with UCP of Maine, you should not be accessing this information. Accessing your personal health records, or the records of significant others (spouse, domestic partner, friends, parents or children) is never allowed. Individuals who wish to access such information should formally request copies of records from the Quality Assurance Department as they would as a client receiving services.

Personal employee information is considered confidential and only shared as required with those who have a need to have access to such information for specific purposes. Information relating to an individual's employment must always be kept separate from information related to health care /mental health services provided to an employee or family members, except with specific permission from the individual.

Employees/Volunteers/Contractors who are unsure about the confidential nature of specific information should ask their supervisor for clarification. Confidential information shall never be removed from UCP of Maine premises unless it is required of the employee's/contractors job function. If confidential information is removed for a permitted purpose, the employee/contractor recognizes that the materials must be protected to the greatest extent possible and returned as soon as possible, and that any

unauthorized use or disclosure could render the individual employee and UCP liable for damages on grounds of defamation or invasion of the right to privacy or subject to HIPAA or other sanctions.

Certain employees may be allowed remote access to UCP's network or in accordance with UCP policies and the law. Any individual allowed remote access is legally responsible for the privacy and security of the information.

Any employee/volunteer/contractor who violates the confidentiality of a UCP client, vendor or employee related information is subject to appropriate disciplinary action, up to and including termination of employment/contract.

Health Information Portability and Accountability Act (HIPAA)

HIPAA provides privacy standards for the use and disclosure of personal protected health information by covered entities and gives clients specific rights to that information. HIPAA also provides security standards which require specific security measures to be in place to protect an individual's health information that is sent or stored electronically. Violation of HIPAA carries serious consequences, including civil monetary penalties on covered entities, and criminal fines and imprisonment on persons who obtain or disclose an individual's health information in violation of the privacy standards. Maine law also protects the privacy and security of health information and provides for sanctions.

All employees/volunteers/contractors at UCP of Maine are required to know, understand and strictly adhere to these privacy and security standards, and are asked to sign a statement certifying that he or she understands HIPAA and will comply with all HIPAA requirements including UCP policies and procedures. Violations of HIPAA are extremely serious and may result in disciplinary action up to and including termination.

Please refer to UCP's Confidentiality Policy for additional requirements related to client and employee confidentiality.

_____

Employee/Volunteer/Contractor Name (Print)

_____ _____

Employee/Volunteer/Contractor Signature Date