Unity House of Troy, Inc.
Policy and Procedure: HIPAA/HITECH Compliance

Topic: Safeguards for Confidentiality

For NYS Mental Hygiene, Article 27-F HIV/AIDS, VAWA, FERPA/IDEA and other special population-specific confidentiality requirements, please also refer to the corresponding UH Program's Policies and Procedures.

Policy Description:

It is the policy of **Unity House** (Organization) that all employees, interns, volunteers, and contractors ensure the confidentiality and privacy of participants and others for whom we create, store, or send private information. The very fact that a participant is served by this organization must be kept private or confidential; disclosures can be made only under specified conditions and/or with the appropriate authorization of the participant, the participant's personal representative, or an appropriate Organization representative.

All disclosures of protected health information (PHI & ePHI, except for disclosures made for treatment purposes), Personally Identifying Information (PII), and NY Resident Private Information (NPI) must be done limited to the minimum amount of information needed to accomplish the purpose of the disclosure.

It is also the policy of the Organization that all requests for PHI (except requests made for treatment purposes), PII, and NPI must be limited to the minimum amount of information needed to accomplish the purpose of the request.

For purposes of this policy:

- **PHI**[i] is defined as any information that is created or maintained by the Organization that relates to the past, present, or future physical or mental health condition of a participant, the provision of care to a participant, or the past, present, or future payment for the provision of care to the participant. It includes any information that identifies the participant or provides a reasonable basis to believe the information can be used to identify the participant. PHI may include, but is not limited to, the participant's name, address, birth date, social security number, benefit information, medical information, service plans, records of treatment or service delivery, and photographs or other images.
- **PII**[ii] means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

- **NPI**[iii] means personal information in combination with one or more of the following data elements:
    - social security number;
    - driver's license number or non-driver identification card number;
    - account number, credit or debit card number, with or without additional identifying information, security code, access code, or password that would grant access to a financial account;
    - biometric information (i.e. fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data); or
    - a username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

The Organization has identified the following safeguards to protect participants from unauthorized disclosure of PHI, PII, and/or NPI.

Verbal Communication
Details concerning participants, their health information, or information related to service provision should not be discussed in a public area where others may overhear the information. Public areas may include but are not limited to hallways, parking lots, rest rooms, break rooms, and public facilities.

Employees, volunteers, or contractors may not discuss information about participants served with any unauthorized person, whether on- or off-duty.

Participant Records/Information
Each employee or contractor is granted access to PHI, PII, and/or NPI based on the assigned job functions of the employee or contractor. Such access privileges should not exceed those necessary to accomplish the assigned job function.

All records containing PHI, PII, and/or NPI or pertaining to participants served must be maintained in a secure area, accessible only to employees or contractors authorized for such access.

Any records stored in general areas must be locked at all times when authorized employees are not in attendance.

Information stored in file rooms, offices, or program areas must be appropriately secured and accessible to authorized personnel only.

Employees must maintain a clean desk practice; no PHI, PII, or NPI may be left unattended on desks or other areas in a manner that is visible to others. Desks and surfaces must be cleared of PHI, PII, and NPI at the end of the shift/day. Records should be secured in locked drawers or cabinets, behind locked doors as required.

Information pertaining to participants may not be visibly posted on walls, bulletin boards, etc. This includes but is not limited to rosters, schedules, service needs, and health or medication needs.

Confidential information to be reviewed at meetings shall not be routinely distributed prior to meetings. If it is necessary to distribute confidential information prior to meetings, the following precautions

should be observed:

- Documents or information is sent via encrypted email;
- The material should be clearly marked as confidential;
- Distributed hard copies of the confidential information should be numbered or otherwise tracked;
- Each hard copy should be retrieved at the meeting at which it is reviewed;
- All hard copies should be destroyed; and
- The original should be retained in a secure location as needed.

Employees or committee members who maintain records of the meetings must assure that the records are safeguarded at all times and that any records are returned to the Organization for destruction or upon separation from the committee or function.

Removal of Records from Organization Premises
Records or information pertaining to participants may not be removed from the facility without the prior approval of a supervisor with authority over the records.

Employees or contractors will be responsible to sign out any records removed from the facility and complete the documentation upon return of the records.

Employees or contractors are responsible for the safeguarding of records in their possession. No records may be left unattended or unsecured in a manner that will allow access by unauthorized parties. Employees or contractors are prohibited from leaving records in their unattended vehicle for any amount of time. If necessary, records must be secured in the locked trunk of a locked vehicle.

Electronic records that contain PHI, PII, and/or NPI may not be stored on portable storage devices.

Employees and contractors must immediately report the loss or destruction of any records to the supervisor with authority over the records. The supervisor must then immediately notify the Compliance Officer.

Computer/Mobile Device Use and Access
Computer use and access is determined by job functions. Only authorized persons may access the Organization's computers, network, and databases. Network and database permissions are assigned and managed by the appropriate administrator.

Employees or contractors may not share passwords or identity with any other person or allow another person access to a computer with their password.
Information Technology personnel must be notified immediately upon the separation of or decision to terminate an employee or contractor in order to initiate access restrictions.

Information pertaining to participants served may not be loaded onto other computer systems without the approval of the Compliance Officer and the application of appropriate safeguards to prevent unauthorized access or disclosure.

Computer screens should be shielded or located in a manner that prevents access by unauthorized persons.

Employees or contractors must exit any programs or files containing PHI, PII, and NPI before leaving the computer unattended. A password protected screensaver should be utilized when computers are unattended.

Missing or stolen laptops or cell phones or other portable devices must be immediately reported to the IT Manager, who will promptly work with the Compliance Officer to assess risks, locate or remotely wipe the device, or initiate breach protocols.

Email Protocol
PHI, PII, or NPI emailed outside of the Organization's network must be encrypted. To send an encrypted email to a non - unityhouseny.org email domain, include **[encrypt]** (type: *bracket character, the word* encrypt, *bracket character*) on the subject line of the email. The email sender will then receive an email from Proofpoint Essentials confirming the message encryption.

Any employee who lacks the ability to encrypt emails containing PHI, PII, or NPI should instead fax the information or seek assistance from a supervisor.

All e-mail messages from Unity House employees must contain a confidentiality statement. This can be added using Outlook's signature feature. Below is an acceptable sample confidentiality statement:

CONFIDENTIALITY NOTICE: The contents of this message, including any attachments, are confidential and are intended solely for the use of the person or entity to whom the message was addressed. If you received this message in error, please immediately notify the sender and permanently delete all copies of the original message and any attached documentation from your system. Thank you for your cooperation.

Fax Protocol
All fax transmissions must include a cover sheet including the name and phone number of both the sender and the recipient. All fax cover sheets must include a confidentiality statement. If you need a fax cover sheet that meets these requirements, please contact your supervisor.

Employees or contractors who transmit confidential PHI, PII, or NPI should confirm receipt of the information by the recipient.

Fax machines should be located in a supervised area to prevent unauthorized access or disclosure of confidential information.
Authorized personnel should remove faxes and deliver to the recipient directly or place the document in an interdepartmental envelope for delivery.

Fax machines should be monitored on a routine basis for the receipt of messages.

Printer Protocol
Employees or contractors are responsible for retrieving print jobs containing confidential information promptly upon printing or using locked, password protected printing options.

Authorized personnel who remove print jobs from a shared printer should deliver the material to the recipient directly or place the information in an interdepartmental envelope.

Mail Protocol
Personnel are designated by job function to distribute mail within the Organization.

All interagency mail must be placed in an interdepartmental envelope and include the name and department of the recipient and the name and department of the sender.

Employees and contractors are responsible to remove mail from mailboxes on a regular basis. During absences, other personnel should be assigned the responsibility for retrieving and securing the mail.

Employees or contractors should not open the mail of others unless authorized to do so by an appropriate supervisor.

Cellular Phones and Mobile Devices
Mobile devices should not be used to email PHI, PII, or NPI unless the device has been encrypted and the Organization has authorized such use. Unencrypted email by its very nature uses an unsecure protocol, creating several risks, including the possibility of data interception.

Missing or stolen mobile devices must be reported immediately to the IT Administrator, who works with the Compliance Officer to assess risks, locate or remotely wipe the device, or initiate breach protocols.

Do not take photos or videos of participants on your personal devices-do not share them with others or on social media. Personal cell phone use with participants is not permitted.

Electronic Communications with Participants
Participants have the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. However, reasonable safeguards **must** be applied to any accommodations that include electronic communication of PHI, PII, or NPI.

Emailing of PHI, PII, or NPI **must** be encrypted, and additional precautions should be applied to avoid unintentional disclosure of confidential information such as checking the e-mail address for accuracy before sending or calling or sending an e-mail alert to the participant, provider, or other email recipient for email address confirmation prior to sending the encrypted message.

If encrypted email is not available to communicate with the participant, the participant **must** be made aware of the risks. When a participant opts to communicate via unencrypted email, additional safeguards **must** be applied to reasonably protect privacy such as de-identifying the information/limiting the amount or type of information disclosed through the unencrypted e-mail.

Texting of PHI, PII, and NPI **must** be de-identified and limited, even with participant informed written consent. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages. However, participants may authorize text message communications regarding reminders for prescription refills and other medication management, housing, and/or appointments. Safeguards to protect privacy **must** be applied during authorized text communications such as de-identifying and limiting the information shared via text message to the absolute minimum required to provide the reminder. More detailed communications that include PHI,

PII, and/or NPI should be relayed in person or via telephone or encrypted email.

Table. Personal Identifiers Under the HIPAA Safe Harbor Privacy Rule That Should Be Removed in Text Messages

Personal names or initials (pertaining to patient, providers, family etc.)
Geographic locations smaller than a state (exception: initial 3 digits of zip code
Elements of dates except years. Ages should be coded as "XX and above"; years as "on or before"
Telephone numbers
Fax numbers
Email addresses
Social security numbers (not even the last 4 digits)
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Vehicle identifiers and serial numbers including license plates
Device identifiers and serial numbers
Web URLs
Internet protocol addresses
Biometric identifies (ie, retinal scans, fingerprints)
Photos
Any unique identifying number, characteristic, or code.

Source: Based on reference 4.

Sample emails or text messages that are deidentified and limit information to the minimum necessary:

> Hi! Reminder: your scripts will be ready this afternoon at 3:00 for pick up at your pharmacy. Please confirm you have received

> Hi! Just a reminder that I will be picking you up at 1:45 tomorrow for your Dr.'s appointment. Please confirm you have received this message. Thanks!

> Hi! Don't forget we have an office visit tomorrow at 10:00! Please confirm you have received this message. Thanks!

If more specific information is requested by the participant or authorized provider or other recipient, Unity House employees **must** provide the identifying PHI, PII, or NPI by phone, fax, or in person.

If a participant has requested electronic communications, an ***Electronic Communications Authorization Form*** (which is attached to this policy) **must** be completed and kept on file. Unity House employees

must review the form, including information related to the risk of communicating over unsecured email or text messaging, with the person in detail before the participant signs the authorization. Any subsequent unencrypted electronic communications must remain within the confines of the participant authorization and content must be de-identified and limited as described above. Whenever possible, the Unity House employee should confirm the email/cell phone number by sending a test email and/or text message at the time the participant signs the Authorization form, before the participant leaves the office.

Participants may text their personal, private, or protected information to employees. In such instances, employees **must** respond using the guidelines above and immediately delete from their cell phone any participant texts that include PHI, PII, or NPI.

Social Media

Employees and contractors are prohibited from posting or including PHI, PII, NPI or any information about participants on social media (i.e., Facebook, YouTube, Twitter). We cannot communicate with participants and/or families via social media nor accept "friend" requests. Staff are required to **not** respond to all such requests.

Authorization for Electronic Communications

Name of Participant:

_____

Date of Request:_____Date of Birth:

_____

It may become useful during the course of service to communicate by email, text message (e.g. SMS) or other electronic methods of communication. Be informed that these methods, in their typical form, are not confidential means of communication. If you use these methods to communicate with staff, there is a reasonable chance that a third party may be able to intercept and eavesdrop on those messages. The kinds of parties that may intercept these messages include, but are not limited to:

- *Email communication containing my personal, private, or protected information will be encrypted, and so I will need to follow the prompts to open the encrypted email.*
- *Text messages from Unity House staff may <u>not</u> be secure and therefore any text message communication from Unity House staff <u>cannot</u> contain any of my personal, private, or protected information. This means text message communications will be broad and <u>not</u> include information about types of prescriptions or name a specific pharmacy, the provider's name for an upcoming appointment, or other specific personal, private, or protected information.*
- *People in your home or other environments who can access your phone, computer, or other devices that you use to read and write messages.*
- *Your employer, if you use your work email to communicate with staff.*
- *Third parties on the Internet such as server administrators and others who monitor Internet Traffic.*

If there are people in your life that you don't want accessing these communications, please talk with Unity House of Troy, Inc. staff about ways to keep your communications safe
And confidential. Use of more secure communications, such as phone or fax, are always alternatives that are available to you if you elect not to give consent to the following forms
*of communication**. I understand that electronic communications will be responded to only during working hours, and are not an appropriate means of communication during an***
***emergency.** 911 should be used for emergency situations.*

I request that the following communications from Unity House of Troy be delivered to me by the indicated electronic means.

Communication(s). Please check <u>all</u> that apply and check the type of communication(s) you'd like, and note any restrictions within each indicated category:

____Prescription refill and other medication management reminders via • Email and/or • Text

____Appointment reminders via • Email and/or • Text

____Housing related reminders via • Email and/or • Text

____Other via • Email and/or • Text (list specifically):

*Indvidual use of email may vary by program.

Restrictions:

My email address is: My cell phone number is:

Time period authorized:

Acknowledgment and Agreement

I understand and agree that Unity House staff may communicate with me using the requested communication method(s) indicated above. I also understand that if I respond to an encrypted email or to a text message from Unity House staff, my message may not be secure and, therefore, I should not email or text staff any information I want to keep protected. I have been informed of the risks; including, but not limited to my confidentiality in services provided, of transmitting my protected health information (PHI) by unsecured means. I understand that I am not required to sign this agreement in order to receive services. I also understand that I may terminate this consent at any time.

Signed: Date:

Printed Name:

Address:

Personal Representative: Date:

Request Received By: Date:

Original filed in the participant's file; offer copy to participant

A Child's Place at UNITY HOUSE

435 4th Street
Troy, NY 12180
(518) 271-6777
Fax (518) 274-5438

50 Philip Street
Albany, NY 12207
(518) 434-0815
Fax (518) 512-3984

achildsplace.unityhouseny.org

Authorization for Electronic Communication(s)

Name of Child: _____

Child's Date of Birth:_____Date of Request: _____

Parent or Legal Guardian's Name: _____

I understand that my signature below authorizes A Child's Place at Unity House to communicate personally identifiable information concerning my child and my child's program by encrypted e-mail. I understand that I will need to follow the prompts to open an encrypted email. I understand that any information that I send to Unity House via email may not be secure and that sending personally identifiable information by e-mail has several risks, which include, but are not limited to, the following:

- E-mail can be forwarded and stored in electronic and paper format easily without prior knowledge of the parent.
- E-mail senders can misaddress an e-mail and personally identifiable information can be sent to incorrect recipients by mistake.
- E-mail sent over the Internet without encryption is not secure and can be intercepted by unknown third parties.
- E-mail content can be changed without the knowledge of the sender or receiver.
- Backup copies of e-mail may still exist even after the sender and receiver have deleted the messages.
- Employers and online service providers have a right to check e-mail sent through their systems.
- E-mail can contain harmful viruses and other programs.
- People in your home or other environments who can access your phone, computer, or other devices that you use to read and write messages.
- Third parties on the Internet such as server administrators and others who monitors Internet Traffic.

I understand text messages from Unity House staff may not be secure and, therefore, any text message communication from Unity House staff cannot contain any specific information about my child or my child's program. This means text message communications must be broad and will typically be used to schedule a call where specific information about my child may be discussed.

Communication(s) between school and parent/guardian

_____Topics related to my child's specific needs/services via • Email and/or • Text

_____Appointment scheduling and reminders via • Email and/or • Text

_____Other via • **Email** and/or • Text (list specifically):

My email address is:_____ My cell phone number is:

_____

****Please note: Childcare staff do not have access to cell phones/computers in the classroom during the school day. ****