Unlimited Services, Inc.
Agency Policies & Procedures

POLICY #: **25.0**

SUBJECT: Confidentiality and HIPAA
(Health Insurance Portability and Accountability Act)

POLICY: All Unlimited Service's records and information relating to the individuals served, employees and the agency are confidential, and the agency ensures the privacy and security of these records as outlined in the Health Insurance Portability and Accountability Act (HIPAA). Employees must, therefore, treat all matters accordingly. No US, Inc. or US, Inc.-related information, including without limitation, individual's files, documents, notes, files, records, health records, oral information, computer files or similar materials (except in the ordinary course of performing duties on behalf of US, Inc.) may be removed from US, Inc. premises without ~~written~~ permission from US, Inc. Additionally, the contents of US, Inc. individual records or information otherwise obtained in regard to business may not be disclosed to anyone, except where required for a business purpose and a "*Consent to Obtain and Release Information*" is signed by the individual. Employees must not disclose any confidential information, purposefully or inadvertently (through casual conversation), to any unauthorized person inside or outside the agency. Employees who are unsure about the confidential nature of specific information must ask their supervisor for clarification.

PROCEDURE: Kelly Meyers, ~~Quality Assurance Coordinator~~ Director of Quality Assurance & Enhancement, is the designated HIPAA Privacy/Security Officer. Joy Allyn, ~~Finance Manager~~ Finance Director is the HIPAA Privacy/Security Officer backup.

This position oversees the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe use and handling of protected health information (PHI) in compliance with federal and state HIPAA regulation.

Newly hired staff will read and sign a Confidentiality Agreement and will be trained on HIPAA, PHI, Confidentiality, Member Rights and Rights Restrictions as part of their New Hire Training and Annual Review. New Hires will receive their Notice of Privacy Practice on date of hire.

Questions on policies and procedures, staff training, safeguards and complaints must be addressed to the Privacy/Security Officials.

Inappropriate disclosure of client data may result in termination of employment and/or the imposition of fines up to $250,000 and ten years imprisonment per incident.

Unlimited Services will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information (PHI).

Unlimited Services will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action: (1) against any individual for the exercise by the individual of his or her rights

under the privacy regulations; or, (2) any individual or other person for filing a complaint with the government, assisting and investigation, or opposing any act or practice made unlawful by the privacy regulations.

Unlimited Services may not require individuals to waive their right to file a complaint with the Secretary of HHS as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

Documentation of privacy policies and procedures are located in the Agency Policy Manual. Communication is required in writing and will be maintained by the Privacy/Security Official. Documentation will be retained for six years from the date of its creation or the date when it was last in effect whichever is later.

Disclosure of confidential information: can be released only through the following channels:

All requests for individual's served information must not be handed out until the consent to release information form has been identified and signed correctly. The director/supervisor and Service Manager or other direct care staff, will ensure that the "Consent to Release Information" is signed and dated appropriately.

In Accordance with the Health Insurance Portability and Accountability Act (HIPAA), employees are strictly prohibited from taking photographs or videos of individuals served without prior written consent.

Personnel information requests must be routed to the Human Resources staff.

Media requests must be directed to the Community Relations Coordinator.

Business Associate - Prior to Unlimited Services disclosing any electronic protected health information to a business associate or allowing a business associate to create or receive electronic protected health information on its behalf, Unlimited Services shall require the execution of a Business Associate Agreement setting forth the relative responsibilities of the parties as they relate to the protected health information disclosed by the County.

The Minimum Necessary Standard

The minimum necessary standard applies to all of Unlimited Service's uses and disclosures of PHI except: (1) disclosures to or requests by a health care provider when the PHI will be used for treatment purposes; (2) disclosures to the individual who is the subject of the PHI; (3) uses or disclosures made pursuant to an authorization requested by the individual; (4) disclosures made to the Secretary under HIPAA; (5) uses or disclosures that are required by law under 45 C.F.R. 164.512(a); and (6) uses and disclosures that are required for compliance with the Privacy Rule.

Unlimited Services employees shall follow proper procedures to ensure that only the minimum amount of PHI necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed. Unlimited Services employees shall request only the minimum amount of PHI necessary to accomplish the specific purpose of the request.

Snooping means intentionally accessing or viewing anyone's confidential information when you do not have a job-related reason to do so. Snooping is a HIPAA violation under the minimum necessary standard and is subject to disciplinary action, up to and including termination.

Electronic Transactions: Unlimited Services is protected by a firewall and all emails are encrypted. Electronic transactions used by US, Inc. are activities involving the transfer of health care information through the use of computers for email, ~~Edoc for~~ documentation, payroll and billing purposes. Unlimited Services will follow the HIPPA requirements for transactions, code sets and identifiers according to HIPAA Administration Simplification.

Password Management: The HIPAA Privacy/Security Officer shall consult with management staff on the procedures for creating, changing and safeguarding passwords. The password management is designed to ensure a secure environment for all employees and protect sensitive information. Adhering to these guidelines will reduce the risk of unauthorized access and enhance the organization's security. All administration employees, SCL Assistants and Vocational Assistant devices will have multi factor authentication. A valid password for administration employees, SCL Assistants and Vocational Assistant shall contain a minimum of 25 characters with a mix of the following Uppercase letters)A-Z), lowercase letters (a-z), numbers (0-9), and special characters (e.g. !@#$%^&*). ~~at least one non-alphabetic or non-alpha-numeric character.~~ A valid password for non-administration (excluding SCL Assistant and Vocational Assistant) devices shall contain a minimum of 16 characters with a mix of the following Uppercase letters)A-Z), lowercase letters (a-z), numbers (0-9), and special characters (e.g. !@#$%^&*). ~~at least one non-alphabetic or non-alpha-numeric character.~~ Our documentation system for all employees will contain a minimum of 16 characters along with two factor authentication. Names, birth dates, and words appearing in any English language dictionary are not valid passwords. Employees must immediately report any suspected or known password compromise to the Operations Manager. If compromised, employees will be required to reset their passwords within 24 hours. Employees are responsible for creating passwords that comply with this policy. Employees must not share passwords with others. Accessing systems with another person's credentials is strictly prohibited.

Additional device management information can be found in Agency 39.0 Technology and Security Policy.

Data Backup & Disaster Recovery: Please see Unlimited Service's – Disaster Management Plan by location, in the Safety & Health Policy Manual, # 5.0

Employee Health Insurance Benefits: The Human Resources staff may disclose protected health information to the organization that sponsors and maintains the group health insurance. Any summary health information will be stripped of all individual identifiers other than the five-digit zip code. All other summary health insurance information will only be kept by the health insurer.

Workstation/Office Security: All staff with workstations are required to lock PHI in files anytime they are away from their workstation and ensure that computers ~~hibernate~~ are equipped with a screen saver with lock after two minutes of inactivity and are password protected. For

those staff that have offices with locks on the door, they may utilize cabinets without locks as long as the office door remains locked anytime they are not occupying their space.

Staff are also required to position their work area and monitor so that people walking into their area cannot directly see their computer screen.

Confidentiality and HIPAA – Page 4

System Access Revocation/Termination Procedure: The program supervisor of each department will notify HR on a "change of status" form, of each employee whose employment is being terminated and whether or not the termination is voluntary or involuntary.

HR will update the employee's status and coordinate the revocation of access rights to the computer system immediately upon the employee's last day of employment.

In the event of an involuntary termination, the supervisor shall immediately notify HR of the employee's termination and HR will take appropriate action to terminate that employee's access to any company computer system.

Protected Health Information: By law: all employees and people served have the right to review and obtain a copy of their medical information in the property of Unlimited Services (this includes paper or information stored electronically). Employees will be subject to appropriate disciplinary action, up to and including dismissal, for knowingly or unknowingly revealing information of a confidential nature.

Reporting of Suspected Breach: If you suspect that there has been a breach of confidential information or PHI, you will be required to fill out an incident report submitted electronically (type of incident will be marked as Questionable incident). The report will describe the event you are reporting. Follow-up with a phone call to the supervisor and privacy officer to alert them of the possible breach. The supervisor will complete the "Privacy or Security Event Reporting" form based off of your information within 2 business days and forward all reports to the Privacy Officer. The privacy officer will review the incident, conduct an investigation and complete the "Breach Notification Risk Assessment" Form, The Privacy Officer will have 5 business days from the date of receiving information from the supervisor to conduct their investigation and determine if a breach occurred. The Privacy Officer will determine if a breach occurred and do the necessary reporting.

Compatible forms with policy:

- Privacy or Security Event Reporting Form
- Breach Notification Risk Assessment Form

Revised: 10/16/09, Revised: 11/26/12, Revised: 4/24/13, Revised: 5/22/17, Revised: 12/19/19
Revised: 1/20/21av (added Business Associate & Minimum Necessary Standard)
Revised: 3/30/21av (added new hires will receive this policy at orientation)
Revised: 4/16/21av (add reporting procedure & paper & electronic PHI requests)
Revised: 6/28/21av (add see attached for reporting forms) Revised: 3/31/22av (added names of compatible forms)
Revised: 8/30/22av (added snooping) Revised: 9/19/22av (added Questionable Incident as category)
Revised: 11/21/23av (KM changes: laptops to hibernate at 2 min.& removing ref. to Edoc)
Revised: 12/30/24km (added no photograph/video, updated password management & screen saver)