RECORDS & CONFIDENTIALITY POLICY

This policy covers the policy and implementation procedures for ensuring client confidentiality and maintaining and storing records, both electronic and paper-based, in a secure manner.

RULES & LAWS
The following federal and state laws govern Florida Medicaid:
- Title XIX of the Social Security Act
- Title 42 of the Code of Federal Regulations
- Chapter 409, Florida Statutes
- Rule Division 59G, Florida Administrative Code

Home and community-based services (HCBS) waivers are authorized under section 1915(c) of the Social Security Act and governed by Title 42, Code of Federal Regulations (CFR), Parts 440 and 441. Section409.906, Florida Statutes (F.S.), and Rule 59G-13.070, Florida Administrative Code (F.A.C.), authorize the application for the Florida Medicaid Developmental Disabilities Individual Budgeting Waiver. The iBudget Waiver is referenced in Chapter 393, F.S., and the Agency for Person's with Disabilities' Rule 65G-4.0210, F.A.C. Medicaid providers who create or maintain electronic records pertaining to goods and services paid for by the Medicaid program must develop and implement an electronic records policy to comply with the applicable state and federal laws, rules, and regulations to ensure the validity and security of electronic and paper-based records. Providers must agree to abide by the terms and conditions of use of the APD online iBudget Waiver system or other electronic system providing such access when made available.

Providers will comply with information security policies, and state and federal regulations and laws, in all use of computer systems and data in accordance with:
- Rule 71A-1.006 F.A.C. (http://www.flrules.org)
- Chapter 119, F.S. [Public Records] (http://www.leg.state.fl.us/)
- Title XIX, Section 282.318, F.S. (http://www.leg.state.fl.us/)
- Title XIX, Section 286.011, F.S. (http://www.leg.state.fl.us/)

Medicaid providers' electronic records policies should also address the technical safeguards required by the Code of Federal Regulations (CFR) Title 45, Part 164.312 where applicable. (www.gpoaccess.gov/cfr/index.html)

Confidentiality of Client Information
The provider agrees not to use or disclose any information concerning a client receiving services under this Agreement for any purpose prohibited by state or federal law or regulation, except with the written consent of a person legally authorized to give that consent or when authorized by law. This includes compliance with:
- the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. 1320d (penalties)
- all applicable regulations relating to the disclosure of information concerning Medicaid applicants and clients provided in 45 CFR Parts 160, 162, and 164
- all applicable regulations relating to the safeguarding of client information provided in 42 CFR, Part 431, Subpart F

The WSC will notify the provider of any breach of client's confidential information. Notification must include details of circumstances and information that was involved. The provider will notify the WSC of any breach of client confidential information.

Records Maintenance and Storage
For all services provided to a Medicaid client, Medicaid requires that the provider retain for a period of at least six years after the last date of service (even when the provider surrenders their agreement or when the client chooses another provider):
- all business records as defined in 59G-1.010(30) F.A.C. (https://www.flrules.org/)
- medical-related records as defined in 59G-1.010(154) F.A.C. (https://www.flrules.org/)
- medical records as defined in 59G-1.010(160) F.A.C. (https://www.flrules.org/)

The provider must keep information on file regarding all employees/staff, including but not limited to Medicaid applications, background screening results, reference checks, education, training, experience, licensure, notes and logs, registration or certification as applicable, other documentation as required, etc.

For electronic data storage devices that store confidential iBudget Waiver client data, such data must be encrypted using a minimum of a 128-bit encryption algorithm. **Information stored on physical media, e.g., computer hard-drive, USB drive, which is not encrypted, should be physically safeguarded to prevent loss or theft.**

All enrolled iBudget Waiver providers must promote and maintain confidentiality of information. The provider must:
- have access to a computer
- have a valid active e-mail address
- use a password
- use the Confidentiality Notice in client-related email

The computer must be capable of performing security functions that promote and maintain confidentiality of information and must:
- have internet access which allows for secure transmission to and from APD
- be used exclusively by the provider
- be stored in a secure manner

- have password-protected logins
- have virus/malware detection

Security Manager
The Security Manager is the Program Administrator and must be conferred with regarding any questions or issues about confidential client information or personnel information, including but not limited to, electronic and non-electronic media, storage, portability, security procedures, password, etc. The Security Manager is responsible for ensuring all personal data is secured during any disaster.

Non-Electronic Files
All non-electronic files pertaining to a client must be physically secured so that only authorized persons can access them. Client records can be scanned and saved into individual computer storage devices which must be labeled for content and stored securely.

HIPAA (Health Insurance Portability and Accountability Act)
You are required to successfully complete training on HIPAA relating to safeguarding confidential client information. A rule of thumb is to not discuss anything about your client with anyone exceot with the written consent of a person legally authorized to give that consent or when authorized by law (HIPAA, 42 CFR, and 45 CFR).

Social Connections
Social connections, to include but not limited to blogs, twitter, facebook, tweets, you-tube, and twits, including any form of messaging, are NEVER to be used to discuss clients or client information. Clients are not to be spoken about for any reason with anyone who does not have a need to know and is not involved with the client's care and without permission of the individual.

Secure E-Mail
Secure e-mail must be used to send any client information for any reason.

Email will contain the following **Confidentiality Notice**:

CONFIDENTIALITY NOTICE: This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorized review, use, disclosure, or distribution is prohibited. If you have received this message in error please contact the sender (by phone or reply electronic mail) and then destroy all copies of the original message.

Information Disposal
Disposal of a provider's business computer and portable digital media storage device (flash drive, etc)
- All client information must be removed from the hard drive of the computer or the portable digital media storage device prior to its disposal using a method that permanently destroys the data (simple file deletion is not sufficient)

Disposal of personal information in any format (digital, electronic, paper-based, films, cassette and video tapes, CD's, hard drives, flash drive,etc):
- Submit paper-based ande electronic media to the Security Manager to be shredded or otherwise destroyed
- Maintain in a secure location for disposal (an area that can be locked or an area that is monitored)

Physical and Technical Safeguards
Workspace
- Lock offices, workspaces, offices, storage rooms, and other non-public areas when vacant

Documents in any format
- Keep in an area that is locked or is constantly monitored
- Protect all paper documents in labeled covers
- Transport paper records so that the names cannot be read

Computer
- Position computer screens (or use shields or hoods) so that unauthorized persons cannot read what's on the screen
- Use screensaver
  - Set screensaver to turn on automatically after a period of inactivity
  - Use password to re-enter
- Accessible only by a unique log-in and/or password
  - Passwords may not be shared
  - Passwords must be "strong" and changed often
  - Limited number of log-in attempts
  - No multiple log-ins at the same time
  - Software to detect, contain or remove viruses, trojans, and other malicious software
- Use a secure Email program (SendInc)
- Use encryption software to prevent unauthorized reading or changing of personal information (Glary Utilitites)
- Use software to ensure electronic information is secure (Glary Utilities, Malwarebytes, Kaspersky)

I have read and fully understand the Records & Confidentiality Policy and agree to follow its dictates.

_____ _____
Staff Signature Date