

**WSC ADVISORY 2020-033**  
**APD SYSTEM ACCESS SECURITY**

**MANDATORY REQUIREMENT**

**EFFECTIVE DATE: SEPTEMBER 30, 2020**

This advisory is to remind all Waiver Support Coordinators (WSCs) and Consumer Directed Care Plus (CDC+) Consultants that APD system account credentials (user name and password) are unique to the WSC or CDC+ Consultant and are not to be shared or used by anyone other than the person assigned to the account. If a WSC or CDC+ Consultant shares his or her login credentials (user name and password) for any APD data system with anyone else, including other employees, the WSC or CDC+ Consultant is in violation of the iBudget Waiver Handbook, Rule 59G-13.070, Florida Administrative Code (F.A.C.) and the Medicaid Waiver Services Agreement.

The iBudget Waiver Handbook Rule requires all providers to comply with APD information security policies, as well as state and federal regulations and laws when using any APD computer systems and data. The Health Insurance Portability and Accountability Act (HIPAA) requires adequate safeguards, including access controls such as passwords, be in place to protect private information. Consistent with Part 164, Subpart C of HIPAA, APD's Passwords Policy, PD 14-004 provides in section 3.b.: "Unless under the direction of the Inspector General, do not share passwords with *anyone*, under *any* circumstances, including administrative assistants. All passwords are to be treated as sensitive, confidential information."

Failure to follow these security requirements poses an unacceptable risk to protected health information and will result in disciplinary action against the WSC or CDC+ Consultant, up to and including termination of Medicaid Waiver Services Agreements.