

## **Web Connect Treatment Management System Policy/Procedures**

The Berks SCA has implemented a web-based client management system, the Care Payer Web Connect System. The Web Connect System allows the Berks SCA to:

- Manage the care of clients in need of Council funded drug and alcohol services
- Administer reimbursement payments to contract treatment programs for drug and alcohol treatment services provided
- Maintain necessary client and financial data in order to provide analysis of client demographic and treatment trends and budgetary spending patterns as well as required reporting to federal, state and local authorities.
- Preserve the security and confidentiality of client services and the financial transactions associated with those services.

Drug and Alcohol treatment providers are required to utilize the Berks SCA's Web Connect System for all clients referred and authorized for services to the provider by the Treatment Access and Services Center (TASC) on behalf of the Berks SCA. The provider is required to use the web connect system for all requests for client funding authorization, reporting of client service encounters and reporting of client discharge from the provider's facility. All treatment providers are required to use the Council's web connect system for client transactions.

The provider will adhere to the following with regard to the Berks SCA's web connect system:

- A. Maintain World-Wide-Web access through Internet Explorer 5.5 or better. This internet access is essential in order for the provider to interact with the Council's web-based application. The Council will issue the provider user identification and password that will be unique for the provider to access the application.
- B. Assure that all provider personnel who will be accessing the Council's web connect system will have been trained by the Council on the use of the system and will be thoroughly familiar with how to use the Council's web connect system.
- C. Submit to the Council the names of those provider personnel who will be using the Council's web connect system. It is the responsibility of the provider to identify necessary personnel who are trained in the use of the web connect system and who require access to the system. The personnel identified by the provider to be given permission to the Council's web connect system is limited to: those who have direct responsibility with the client treatment file and/or billing of services; individuals who supervise those with direct responsibility for the client treatment file and/or billing of services; and management of the provider organization who have the authority to view client treatment and/or billing information.
- D. The Council will create a unique user log-on identification and passwords for each user. An individual will need to use both their own particular user identification and password and the provider's unique user identification and password in order to access the Council's web connect system. The provider must take reasonable measures to assure that each individual's unique user identification and password

remain confidential. The provider representative are not allowed to share their web connect system accounts or permissions with other individuals.

- E. If any individual who was issued a user identification and password to the web connect system terminates his/her employment with the provider, the provider must inform the Council within one (1) working day of that person's termination. In this way, the Council can invalidate that particular persons user log-on identification and password into the web connect system.
- F. The provider will assure that the Council's web connect system will only be accessed from a computer terminal within the facility. Provider personnel are not allowed to access the Council's web connect system from a location (i.e., private residence, public internet access sites, etc.) where unauthorized individuals could view protected client information.
- G. The provider and it's representatives are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, passwords, etc.), or by causing some system component to function incorrectly.
- H. The provider and it's representatives are prohibited from taking unauthorized actions to intentionally modify or delete information or programs associated with the Council's web connect system.
- I. The provider and its representatives are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges.
- J. The providers and it's representatives shall not intentionally introduce or use malicious software (i.e., computer viruses, Trojan horses, worms, etc.).
- K. The providers must notify the Council immediately when they become aware that any of the accounts used to access the web connect system application have been compromised. Additionally, the provider agrees to notify the Council or the Treatment Access and Services Center (610-375-4426) if the provider encounters any problems with the functioning of the web connect system.
- L. The provider acknowledges and accepts full responsibility and liability, and holds the Council harmless, for any breach in client privacy as a result of the provider's (or any of it's personnel's) inappropriate managing of the client information viewed and/or inputted into the Council's web connect system.