Broward Behavioral
HEALTH COALITION

Broward Behavioral Health Coalition, Inc.	1715 S.E. 4th Avenue Fort Lauderdale, Florida 33316 (954) 622-8121
Policy Title: Confidentiality & Security	
Policy Number: BBHC.0015	**Contract Section (s): Contract No. JH343**
Effective Date: May 16, 2013	**Revision Date:**
Responsible Department: Continuous Quality Improvement (CQI)	

Signature Block *(all necessary Managing Entity (ME) signatures are placed in this section)*

Approved by: Jennifer Holtz, CQI Manager
Signature: _____ Date: 5/17/2013
Title:

Approved by: Silvia Quintana, Chief Executive Officer
Signature: _____ Date: 5/17/13
Title: CEO

Approved by Board of Directors May 16, 2013

Policy: It is the policy of Broward Behavioral Health Coalition (BBHC) that all consumer and personnel information from any source in any form, including paper, records, oral communications, audio recordings and electronic records is strictly protected and confidential. Access to confidential information, including consumer protected health information (PHI), is permitted on a need-to-know basis within the confines of one's job responsibilities as a BBHC employee. Examples of permissible access include, but are not limited to, receipt of & follow up on complaints / grievances, provision of assistance in system access issues, and miscellaneous case issues, data management, administrative support and any additional functions that support BBHC business.

Purpose: To prevent unauthorized disclosure of consumer and employee protected and confidential information.

Procedure: BBHC staff / employees maintain full compliance with The Health Insurance Portability and Accountability Act (HIPAA). BBHC staff / employees will not disclose, divulge, or make accessible confidential information belonging to, or obtained through their affiliation with BBHC, to any person, including relatives, friends, and business and professional associates, other than to persons who have a legitimate need for such information and to whom the BBHC has authorized disclosure.

Staff / employees shall use confidential information solely for the purpose of performing BBHC business. This policy is not intended to prevent disclosure where disclosure is required by law. Conversations that include confidential information are held in a secured setting, i.e. in office with closed doors, to prevent unauthorized disclosure. In addition, staff / employees will ensure all confidential and protected information is secured, i.e. kept in locked drawers / cabinets. Computers will be appropriately logged off or locked when staff / employees leave their work

stations and staff will refrain from phone calls that include discussion of confidential information in public areas.

Upon a staff's employment termination with BBHC, all systems and computer passwords / access will be disabled. Keys to offices, cabinets, etc. shall be returned and all devices, including laptops, cell phones, and other equipment that may contain confidential information are all returned immediately.

BBHC staff / employees shall comply with the following and are required to sign the 'Security and Confidentiality Statement' as a condition of employment (see Attachment I):

1. Comply with the HIPAA rule.
2. Treat as confidential and protected all patient, consumer and employee protected information that is received, either informally or formally, during the course of employment.
3. Only access PHI and protected employee information as required by job responsibilities.
4. Not disclose information regarding consumer / patient PHI, employee protected information and/or any other protected information pertaining to BBHC business and customers to any person, entity, other than as necessary and authorized as part of job duties, or as may be required by law.
5. Not log into any BBHC computer system with any password other than one's own.
6. Safeguard one's computer and systems' passwords and ensure they are not easily seen by others which may lead to improper and unauthorized use.
7. Not permit anyone, including other BBHC employees and affiliates, to use one's passwords.
8. Notify supervisor if computer password has been compromised.
9. Password protects and locks computer when not present at workstation in order to protect confidential information.
10. Not send via email any PHI, employee protected or any other confidential information without using the approved secure email system.
11. Safeguard all PHI, employee confidential and other protected information via storing in locked drawers / cabinets at all times.
12. Upon cessation of employment with BBHC, continue to maintain the confidentiality of any consumer PHI, employee or other protected information accessed while employed and agree to turn in any keys, access cards, computer equipment, cell phone and any other device providing access to BBHC information.

Staff / Employees shall report to their supervisor and/or BBHC Chief Executive Officer any suspected HIPPA violation and/or unauthorized disclosure of protected / confidential information.

Staff / employees will protect information taken off-site, ensure it is fully secured and remains in their physical possession during transit, never leaving it unattended or in any mode of transport (even if the mode of transport is locked). Confidential information will only be taken off-site if accessing it remotely is not a viable option and if removing it from the BBHC offices is necessary for business operations.

Staff / employees will not download, install or run any unauthorized or unlicensed software and will not disable or alter anti-virus or firewall security systems / software on BBHC equipment.

Prior to accessing DCF state databases, all BBHC staff / employees read, agree to and sign the DCF Database Access Request Form & DCF Security Agreement Form (Attachment II) and the DCF Florida Individual Security Information Form (Attachment III).

REFERENCES: 1. The Health Portability and Accountability Act (HIPAA)

ATTACHMENTS: 1. Security and Confidentiality Statement
2. Department of Children & Families (DCF) Database Access Request Form & Security Agreement Form
3. DCF Florida Individual Security Information Form
4. Summary of The HIPPA Privacy Rule

DEFINITIONS:

REVISION LOG

REVISION	DATE

The BBHC CQI Manager and Chief Executive Officer are responsible for all content in this policy.