Great Rivers Behavioral Health
Administrative Services Organization

Policy Title:	**Password Protection Procedure**	Policy No. **5029.00**
Category:	Privacy & Security	Date Adopted: 1/10/2020 Date Revised: Date Reviewed:
Reference:	Washington Health Care Authority Contract with Great Rivers Behavioral Health Administrative Services Organization	

POLICY

1.1 Great Rivers Behavioral Health Administrative Services Organization (Great Rivers), in an effort to be compliant with the Privacy Rules of HIPAA's Administrative Simplification provisions, sets out, in this policy to define standards and procedures to safeguard confidential information.

1.2. Great Rivers places great value on the privacy and confidentiality of information. Beyond these principles, privacy and security is mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 CFR Part 2, and Health Information Technology for Economic and Clinical Health 04/27/09 (HITECH). These regulations require that Great Rivers deploy and maintain a set of policies, practices, and technologies to safeguard confidential information and ensure that such information is not disclosed to anyone without the proper authorization to view or possess such information.

PROCEDURE

2.1. Access Codes and Passwords

2.1.1. The confidentiality and integrity of data stored on company computer systems is protected by access controls to ensure that only authorized employees have access. This access is restricted to only those capabilities that are appropriate to each employee's job duties.

2.1.2. The Information Services department institutes a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use Great Rivers computer systems and networks. The characteristics of the password requirement consist of the following:

2.1.2.1. The password consists of at least 8 alphanumeric characters from at least three of the following:

2.1.2.1.1. Upper case.

2.1.2.1.2. Lower case.

2.1.2.1.3. Numbers.

2.1.2.1.4. Special Characters.

2.1.2.2. The password is changed by each user at least every 60 days.

2.2 Information Services Responsibilities

2.2.1. The Information Services department is responsible for the administration of access controls to all company computer systems.

2.2.2. The Information Services department deploys and maintains a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.

2.2.3. The Information Services department maintains a list of administrative access codes and passwords and keeps this list in a secure area.

2.2.4. The Information Services department assigns responsibility for maintenance of the access code and password assignment to a qualified individual in the Information Services department. Additionally, a back-up staff person of the department is also assigned these duties as a backup to the primary staff person.

2.2.5. Set the default to change passwords at least every 60 days.

2.2.6. Set the default so that passwords consist of at least 8 alphanumeric characters from at least three of the following: Upper case; Lower case; Numbers; Special Characters.

2.2.7. Set the default to activate a password protected screensaver set for 20 minutes of inactivity, requiring the end user to log back in.

2.2.8. Set the default that after three failed attempts to log on, the system will refuse to permit access for 30 minutes.

2.2.9. Set the default for a password history of 5 remembered passwords.

2.3. Employee Responsibilities

2.3.1. Employees are responsible for all computer transactions that are made with his/her User ID and password.

2.3.2. Employees do not disclose passwords to others. This is strictly interpreted and applicable to all staff.

2.3.3. Passwords are changed immediately if it is suspected that they may have become known to others. In the event that an employee suspects or knows that his/her password has become known to an unauthorized person, the employee immediately reports this event to the IS Manager or Systems Administrator. Passwords are not recorded where they may be easily obtained. Employees do not display passwords in any area that can be viewed by others. Passwords are changed at least every 60 days.

2.3.4. Employees will use passwords that will not be easily guessed by others.

2.3.5. Employees will log out when leaving a workstation for more than 30 minutes or when leaving the premises for any length of time.

2.3.6. Employees have a password protected screensaver set for 20 minutes, of inactivity, requiring employees to log back in.

2.4. Emergency Access to Applications

2.4.1. An emergency may arise in which a user needs access to a system resource that is password-protected under another user ID and where that particular user is unavailable. In no circumstance will the original user ID-account owner's password be shared to access the application. In order to have a clear chain of responsibility, the IS Manager will reset the resource owner's password and reassign the account to another individual (thereby transferring responsibility for actions performed by that particular user).

2.5. Managers' Responsibility:

2.5.1. Managers will notify the Information Services department (IT/IS Manager) promptly whenever an employee leaves the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

2.6. Enforcement:

2.6.1. All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with Great Rivers Sanction Policy.

2.7. Visitor Passwords:

2.7.1. Great Rivers will provide visitor passwords that will be unique to each user and will be stored within Great Rivers system to allow tracking of where the individual viewed within the access points the individual was authorized to access. Access to service areas will be determined based upon need, with minimal access provided to ensure the work being addressed can be accomplished. Passwords will be terminated at the end of the visitors stay.

POLICY SIGNATURE

Edna J. Fund DIGITALLY SIGNED

Edna J. Fund, Chair
Great Rivers BH ASO Governing Board

01/30/2020
07:57 PM EST

Date