Great Rivers Behavioral Health
Administrative Services Organization

Policy Title:	**Computer and Information Security**	Policy No. **5027.00**
Category:	Privacy & Security	Date Adopted: 1/10/2020 Date Revised: Date Reviewed:
Reference:	Washington Department of Social and Health Services Contract with Great Rivers Behavioral Health Organization	

POLICY

1.1. Great Rivers Behavioral Health Administrative Services Organization (Great Rivers BH-ASO), in an effort to be compliant with the Security Rules of HIPAA's Administrative Simplification provisions, 42 CFR Part 2, and Health Information Technology for Economic and Clinical Health 04/27/09 (HITECH) and to define the responsibility of Great Rivers BH-ASO to safeguard the confidentiality and integrity of protected health information (PHI) as required by law, and professional ethics and the importance of employee familiarity with these responsibilities.

1.2. Much of Great Rivers BH-ASO confidential information is stored in electronic computer networks and devices. Great Rivers BH-ASO takes great care to ensure that access to those computers, networks, and devices is strictly limited to staff with a need to know and/or view that information. The key elements of Great Rivers BH-ASO's computer and information use are included in the following procedures:

1.2.1. Desktop and Laptop Computers

1.2.2. Password Protection

1.2.3. Remote Access

1.3. Great Rivers BH-ASO makes use of access codes and passwords. The Password Protection Procedure outlines the specific policies and procedures for management of those codes and passwords. All users are familiar with and comply with this procedure.

1.4. Great Rivers BH-ASO staff using desktop computers, laptops, or other electronic appliance either standalone or networked are familiar with and follow the contents of the Desktop and Laptop Computer Procedure.

PROCEDURE:

2.1. Desktop Computer Use Assumptions:

2.1.1. Every desktop computer in Great Rivers BH-ASO is vulnerable to environmental threats, such as fire, water damage, power surges, and the like.

2.1.2. Any desktop computer in Great Rivers BH-ASO can access confidential information if the user has the proper authorization.

2.1.3. All computer screens can be visible to individuals who do not have access to confidential information that may appear on the screen.

3.1. Laptop Computer Assumptions:

3.1.1. Laptop computers pose a significant security risk because they may contain confidential information and, being mobile, are more at risk for loss, theft, or other unauthorized access than Great Rivers BH-ASO's stationary desktop computers.

3.1.2. Laptop computers may be more vulnerable to viruses and security threats since they are used as a mobile device. Public or private networks other than Great Rivers BH-ASO's network may not regularly provide a virus or security protected environment like Great Rivers BH-ASO's network.

3.1.3. Laptop computer use is more difficult for Great Rivers BH-ASO to audit; thus security breaches may be more difficult to identify and correct.

4.1. Preventative Measures for Desktops and/or Laptop Computers:

4.1.1. Great Rivers BH-ASO staff will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, slow response times of accessing data, unexpected reboots of the computer/laptop, computer/laptop system halts, virus messaging, or other such attacks.

4.1.2. All computers plugged into an electrical power outlet will use a desktop ups unit with surge suppressing approved by the Information Services Manager.

4.1.3. Great Rivers BH-ASO staff shall take appropriate measures to protect computers and data from loss or destruction.

5.1. Remote Access:

5.1.1. Remote access is meant to be an alternative method of support for Great Rivers BH-ASO's office functions. By using Great Rivers BH-ASO's hardware, software, and/or network systems, staff assumes personal responsibility for their appropriate use. Staff reads and complies with the Remote Access Procedure, and understands the following:

5.1.1.1. That any software and hardware devices provided to staff by Great Rivers BH-ASO remain the property of Great Rivers BH-ASO.

5.1.1.2. There is no modifying, altering or upgrading any software programs or hardware devices provided to staff by Great Rivers BH-ASO without the permission of the Information Services Department.

5.1.1.3. The need to take maximum precautions to prevent unauthorized access and/or viewing of client's protected health information.

5.1.1.4. All staff is strictly prohibited from downloading, copying, or keeping in any form protected health information (PHI) on personal computer(s).

5.1.1.5. There is no copying, or duplicating (except for backup purposes as part of your job), or allowing anyone else to copy or duplicate any software.

5.1.1.6. If staff leave Great Rivers BH-ASO for any reason, they immediately return the original and/or copies of any and all software, computer materials, or computer equipment received from Great Rivers BH-ASO that is either in immediate possession or otherwise directly or indirectly under their control.

5.1.1.7. All staff is in agreement that reasonable efforts to protect all Great Rivers BH-ASO provided software and hardware devices from theft and physical damage must be taken.

6.1. Confidentiality and Security Agreement:

6.1.1. The Confidentiality and Security Agreement is used to acknowledge receipt of, and compliance with, this policy. A signed and dated Confidentiality and Security Agreement is placed in each employee's personnel file.

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