Policy Number:
7
Effective Date: May 1, 2008
Revised: August 15, 2016,
October 16, 2017

Subject: Security of Electronic Information

PURPOSE:

Camden County Developmental Disability Resources (CCDDR) shall have a policy to properly secure electronically stored client records, computerized client information and client information transmitted/received via facsimile (fax) machines. All CCDDR staff shall be trained with regard to data security procedures.

POLICY:

I. Security of Electronic Data

1. The following measures shall be enacted by CCDDR to protect the security of agency electronic data:

   A. User's workstations shall be automatically configured to go to screen-saver mode after a maximum period of 15 minutes of inactivity.

   B. Password authentication shall be required to log back on by users after screen saver mode has been enacted.

   C. All workstation users shall have individual usernames and passwords that comply with industry standards and eliminate unauthorized access.

   D. All passwords must meet the following requirements:

      - Not a word in the dictionary
      - Are 9 or more characters in length
      - Include a number or character
      - Are randomly generated by network administrator or Director

   E. All passwords shall be assigned to CCDDR staff by Director or contract IT personnel.

   F. Separate passwords shall be used to access service monitoring database.

   G. Employees are not to share passwords and should commit to memory rather than having these written on paper indefinitely.

H. All client information, files, documents, etc. shall be saved to the network drive by agency staff.

I. Client information can be temporarily saved to a working file on individual CCDDR workstation PCs and CCDDR portable computers; however, once the working file is completed, the file must be saved to the network drive and immediately deleted afterwards.

J. Client information cannot be saved on employee home, portable computers, or other devices.

K. All crucial agency information, such as bank information, bylaws, payroll data, etc., shall be saved to the network drive by designated agency staff.

L. Only contracted IT personnel and the Director shall have security rights to the network.

M. In addition to a network firewall, all individual workstations and portable computers shall also employ separate firewalls.

N. All data drives are maintained by the contracted database entity.

O. Designated staff shall ensure all media has been thoroughly cleansed of any client data before the media is released or disposed.

P. Access to data drives containing client data shall be controlled, by designated staff through:

- Access control lists to network media
- Physical access control to hardware

Q. CCDDR employees shall not load software from any source onto their assigned workstation or any other CCDDR equipment, without prior approval of the Director.

R. Software shall be loaded on workstations only by designated CCDDR employees.

S. CCDDR workstations shall be situated within work areas to prevent incidental observation of screens that may contain Private Health Information (PHI). Failure of employees to comply or assure compliance with this policy may result in disciplinary action.

II. Staff Access to Logging/Billing System Away from CCDDR Facility

1. The service monitoring database system is a web-based system designed for user convenience and can be accessed from other computers via the Internet. Nevertheless, security and confidentiality of client information remains paramount, and state/federal

confidentiality laws apply. The following guidelines apply to all CCDDR employees when accessing the service monitoring system away from the CCDDR facility:

A. As a general rule, the database system should only be accessed from a CCDDR portable computer; however, employee-owned home or portable computers can be used only when absolutely necessary.

B. Access from a computer located in public place is prohibited.

C. No other members of employee's family are authorized to view confidential information regarding CCDDR; therefore, steps must be taken to place monitors in secure locations or perform work when employee's family members are not present and do not have access.

D. Due to security concerns, use of unsecured wireless connections to access the database is prohibited.

E. Passwords for accessing the database are not to be written on paper in employee's home, but rather committed to memory.

F. Employees' home or portable computers must have the following:

- Firewall protection
- Anti-virus protection
- Controls set to time-out after a maximum of 15 minutes of inactivity, with password authentication required to log back on

III. Virus Protection

1. Virus protection for the network shall be maintained by CCDDR's contracted IT agent.

2. All workstations, portable computers, PDA's or any other device that connects to the network shall be protected using the anti-virus software for that device installed by designated CCDDR staff. Equipment that has not been purchased or leased by CCDDR shall not be allowed to connect to the CCDDR network.

3. Anti-virus server software shall be configured by CCDDR's contracted IT agent to check for virus signature updates daily. Special virus signature updates created in the event of a known virus, will be manually pushed by CCDDR's contracted IT agent to the network server, PCs, and portable computers within 24 hours of the time the receipt of the update has been received.

4. Anti-virus software shall be kept by CCDDR's contracted IT agent at the current release or no more than one release below the most current release version.

IV. Use of Facsimile (Fax) Machines

1. Fax machines are to be located in secure areas.

2. The designated person shall periodically check for and distribute incoming documents.

3. When faxing PHI the CCDDR staff person must:

    - Insure that documents are handled securely/confidentially
    - Insure that the document is delivered to the addressee
    - Verify the destination when sending number for the first time
    - Include a confidentiality notice within the fax cover sheet – no client PHI will be contained on the fax coversheet

V. Use of Internet

1. Employee use of the Internet for personal reasons while on duty is prohibited.

VI. Annual Review of Technology Needs

1. On an annual basis, the Director in consultation with the CCDDR contracted IT agent, shall evaluate the agency's current hardware and software systems, and how well current systems meet the agency's needs.

REFERENCES:

- HIPAA Privacy & Security Rule 68 FR 8334 & 65 FR 82462
- CARF Standards Manual
- CCDDR Technology Plan