Policy Number:
7
Effective Date: May 1, 2008
Revised: August 15, 2016, October 16, 2017, April 9, 2020

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:

Security of Electronic Data

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

A. Employees' workstations/computers 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 employees after the screen saver mode has been initiated.
C. All employees shall have individual usernames and passwords that comply with industry standards and eliminate unauthorized access.
D. All passwords must meet the following requirements:

- Are 9 or more characters in length
- Include a number and/or character (preferably both)
- Are randomly generated by the network administrator, Executive Director, or authorized designee(s)

E. All passwords shall be assigned to CCDDR staff by the Executive Director, contracted IT Personnel, or authorized designee(s).
F. Separate passwords shall be used to access the service monitoring database.
G. Employees are not to share passwords and should commit to memory rather than having them written on paper indefinitely.
H. All client information, files, documents, etc. shall be saved to the appropriate secured online network databases by agency staff.
I. Client information can be temporarily saved to a working file on CCDDR-owned computers; however, once the working file is completed, the file must be saved to the appropriate online secured network database(s) and immediately deleted from the computer afterwards.
J. Client information cannot be saved on employee personal computers, employee personal

portable computers, or other computers or devices not owned by CCDDR. Files temporarily stored on approved cell phones, digital cameras, or other similar storage devices used in the course of CCDDR business/services must be transferred as soon as possible to the appropriate CCDDR secured online database and then immediately deleted from the device afterwards.

K. All crucial agency information, such as bank account numbers, vendor account numbers, etc., shall be saved to the online secured network database(s) by designated agency staff.
L. Only contracted IT personnel, the Executive Director, and authorized designee(s) shall have security rights to the network.
M. In addition to a network firewall, all individual workstations and portable computers shall also utilize firewalls.
N. All databases are maintained by the contracted database entity/entities.
O. Designated staff or contracted IT personnel shall ensure all media has been thoroughly cleansed of any client data before the media is released or disposed.
P. Access to databases 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 Executive Director.
R. Software shall be loaded on workstations only by authorized CCDDR employees or contracted IT personnel.
S. CCDDR workstations shall be situated within work areas to prevent incidental observation of screens that may contain Protected Health Information (PHI). Failure of employees to comply or assure compliance with this policy may result in disciplinary action, including termination.

<u>Staff Access to the Secure Online Databases Away from CCDDR Facilities</u>

CCDDR's secure online database systems are web-based systems designed for authorized employee-user convenience and can be accessed from other computers via the Internet. Nevertheless, security and confidentiality of client information remains paramount, and state and/or federal confidentiality laws apply. The following guidelines apply to all CCDDR employees when accessing CCDDR's secure online databases away from the CCDDR facility:

A. As a general rule, the database systems should only be accessed from a CCDDR-owned computer; however, the Executive Director may approve the use of devices not owned by CCDDR in emergency situations. If approved to use by the Executive Director, computers not owned by CCDDR must have the following:

- Firewall protection
- Anti-virus protection
- Controls set to time-out after a maximum of 5 minutes of inactivity, with password authentication (known only to the employee) required to log back on

B. Steps must be taken to place computers in secure locations while performing work remotely to ensure unauthorized individuals do not have access.
C. Due to security concerns, use of unsecured wireless connections to access CCDDR databases is prohibited.
D. Passwords for accessing the database are not to be written on paper in the employee's home or any other location accessible to others and should be committed to memory.

Virus Protection

Virus protection for the office network shall be maintained by CCDDR's contracted IT agent. All computers or other devices connected to the network shall be protected using the anti-virus software for that device installed by designated CCDDR staff or contracted IT personnel. Equipment that has not been purchased or leased by CCDDR shall not be allowed to connect to the CCDDR office network.

Anti-virus software shall be configured by CCDDR's contracted IT agent to check for virus signature updates as recommended. 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 components, including all computers and connected hardware, within 24 hours of receipt.

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.

Use of Facsimile (Fax) Machines

Fax machines are to be located in secure areas, and the designated employee(s) shall periodically check for and distribute incoming documents.

When faxing PHI, the CCDDR staff person must:

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

Use of Office Internet

Employee use of the office Internet for personal reasons is prohibited.

Annual Review of Technology Needs

On an annual basis, the Executive Director, in consultation with the CCDDR contracted IT agent and CCDDR's Administrative Team, shall evaluate the agency's current hardware and software systems. The systems will be evaluated to determine how well the current systems meet the agency's needs and if substantial upgrades are necessary.

REFERENCES:

- HIPAA Privacy & Security Rules & Regulations
- CARF Standards Manual
- CCDDR Technology Plan