Communities Connected *for* Kids

Series: 1100 Technology, Data, Records, and Reporting

Policy Name: **Security of Information Systems, HIPAA and Technology Resources**

Policy Number: 1108

Regulation/Reference: 45 C.F.R 164.312 (c); 45 C.F.R. 164.312 (C) (2); 45 C.F.R. 164.530 (f); 45 C.F.R 164.312 (b) DCF CFOP 50-2**;** CCKids 803**,** 1114, 1115, 1116, 1117, 1118**,** DCF CFOP 60-17

Origination Date 11/1/2013 **Revision Date:** June 8, 2022

Attachments:

Policy: Communities Connected for Kids (CCKids) locally stores electronic sensitive data necessary for daily business operations. It is the policy of CCKids to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our clients and the mission of CCKids. CCKids implements and enforces a level of security that provides for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside of CCKids in an unauthorized manner.

Procedure:

CCKids establishes and maintains an environment in which electronic, sensitive data is protected against unauthorized access. This policy addresses minimum security responsibilities regarding CCKids and contract provider employee access to data. Adherence to this policy ensures the ability to provide personal accountability pertaining to the security of department and contract provider employee access to data through the use of computer-related media.

I. Physical / Site Security.

CCKids Headquarters

An annual analysis/review audit shall be conducted to determine the adequacy of physical/site security. It will take into account controlled physical access to the area, the need for disaster contingency planning, and other appropriate security requirements. Additional security measures include confidential secure system logons, secure system backups, necessary security agreement, encrypted removable media, proper usage agreement and the email encryption policy. These safety measure insure the integrity in protecting electronic protected health information from improper alteration or destruction. In the event that mitigation becomes needed, and to the extent possible, any harmful effects that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedure or the requirements of this subpart by the covered entity or its business associate will follow

Communities Connected for Kids Incident Reporting policy 803, Department of Children's and Families Security of Data and Information Technology Resources policy 50-2.

ll. Integrity and Audit Controls processes in place:

- Audit Controls; CCKids 1114
- Backups: ePHI is routinely backed up to preserve integrity in case of altercation or destruction; CCKids 1115
- Security agreement: Users are required to sign security agreement, complete DCF Security Awareness Training; CCKids 1116
- Encrypted removable media: All removable media must be encrypted prior to write access being granted – set by Windows Group Policy; CCKids 1117
- Email encryption policy: email containing ePHI is automatically encrypted by the email system; CCKids 1118
- Access Control/Logons; CCKids 1121

lll. Orientation.

CCKids's Security Coordinator will be responsible for providing rules, policies, procedures and guidelines on departmental information security that will be made available to and reviewed by all employees during new employee orientation sessions.

lV. Training.

All new CCKids employees are required by this operating procedure to review applicable state and federal rules and regulations that pertain to data confidentiality and information security as a part of their pre-service training. Employees will be advised of the specific security requirements of their positions. Employees will be notified of any changes to confidentiality laws or changes to Departmental security rules, policies, procedures and/or guidelines, or any specific security requirements of their positions by their supervisor and/or Director of Information Technology.

V. Security Awareness, HIPAA.

New CCKids staff will complete the Security Awareness Training program that ensures employees are aware of the importance of information security through the Department of Children and Families annual on-line training. All employees must complete the Security Awareness Training within 5 days after being hired and/or gaining access to agency systems, or face revocation of their access. Each Employee shall attend annual HIPAA training that is provided by The Department of Children and Families. In the event that a HIPAA or Privacy Practice Breach may have occurred, CCKids will follow CCKids Incident Reporting and HIPPA Breach Notifications, Policy 803 and CFOP NO. 60-17, Chapter 7 HIPAA Breach Notification Procedures.

DocuSigned by:

Approved: Carol Deloach
96C0E7A7E02E4BA...
Carol A. Deloach, CEO

Date: 7/27/2022