Series: 1100 Information Technology

Policy Name: Access Control

Policy Number: 1121

Regulations: 45 C.F.R 164.308

Origination Date: 7/20/2022 **Revision Date:**

Policy:

1. Only authorized personnel will access electronic data, including the hardware and/or software on which the electronic PHI, PII or other sensitive data is stored. Data access will be granted based on user roles and departments operational requirements for those roles. Communities Connected for Kids will utilize authentication mechanisms to corroborate user identity as outlined in the related procedure. Emergency access may be granted, as defined in the related procedure.

2. All employees will be granted access to the following systems: Communities Connected for Kids email, Intranet, Employee Self Service, Learning Management, Applicant Tracking, timekeeping, collaboration utilities and personal file storage. Managing access to any other business applications requires approval via the System Access Request (SAR) process.

3. CCKids IT Department and approved Corporate Information Resources staff are permitted to create or change local file server data access control settings. User access changes require an approved SAR with supporting documentation for the change request, as well as the supervisor's approval.

4. Users with administrative access to servers, databases, and other critical IT infrastructure are granted access to those systems via a procedure maintained by the IR Director of Infrastructure Management.

5. Electronic sessions will be automatically locked/terminated after a preset period of inactivity established by the Communities Connected for Kids IT department and applied to all Communities Connected for Kids facilities.

6. When an employee, contractor, or any other Communities Connected for Kids representative leaves, or a role change occurs, the user's system access will be removed or modified in a timely manner.

7. Physical access to equipment with the ability to store or transmit PHI, PII and other sensitive data will be restricted to authorized personnel.

Procedure:

Access Control Mechanisms

1. Only appropriately authorized data access will be granted.
2. The rights to modify access control settings must be requested through the System Access Request (SAR) process.
3. Quarterly user access audits and other routine access monitoring are conducted to ensure access permissions are assigned correctly.
4. Upon notice of a user's termination, all network, application and physical access is revoked.

Procedures for Unique User Identification

1. Prior to giving an individual his/her account information (i.e., user id and temporary password), validate the identity claimed either in person, or send the person's supervisor the account information.
2. Assign each individual a unique user ID.
3. The Corporate HelpDesk maintains procedures on the standard convention for assigning unique user identifiers.
4. Access control modifications must be requested via an approved SAR.
5. Advance set up of non-user specific accounts is permitted based on business need to facilitate timeliness of access to the system (see *Auditor Access Procedure*, below, as an example). The account is only enabled when a specific user and need are identified and is disabled when the business need expires. Such accounts are approved on a case by case basis and require submission of a SAR.

Password Standard

Each Communities Connected for Kids' application which contains PHI, PII and other sensitive data will require a password to access the system. Standard password parameters include:

1. *Network Access Password Settings:*

    a. User password lengths must be at least 8 characters.
    b. User passwords must be reset at least every 90 days.
    c. User passwords cannot be reused within the last 24 resets.
    d. Passwords must include characters from three of the following four categories: lowercase, uppercase, numbers or symbols.

2. *Oracle Password Settings:*

    a. The password must be alphanumeric (i.e., include both letters and numbers).
    b. The password must be at least 8 characters in length.
    c. The password may not include the user's ID.

Multi-Factor Authentication (MFA)

All users have MFA enabled on their network accounts (Office 365 applications and Citrix access). Users working on Communities Connected for Kids-owned equipment on the network will not be prompted with MFA for authentication. Users can review and update their MFA preferences at verifyme.devereux.org.

Self-Service Password Reset

Users have the ability to reset their network account passwords at passwordreset.devereux.org.

Emergency Access Procedures

1. Identify the necessary electronic PHI, PII or sensitive data that needs to be obtained during the emergency.
2. Configure and update the access controls to be consistent with approved authorizations.
3. Remove the emergency access rights after the emergency has been declared over.

Automatic Logoff Procedure

Communities Connected for Kids' standard PC workstation images contain a screen-saver timeout after 15 minutes of inactivity, requiring a valid ID and password to gain re-entry into the system.

Physical Access Controls Procedures

1. An inventory of keys and key card assignment will be maintained so that they can be recovered or revoked.
2. All combination locks will be changed periodically.

Auditor Access Procedure

HIPAA permits disclosure of protected health information to a health oversight agency for oversight activities authorized by law, including audits. Centers are required to have non-user specific auditor accounts for this purpose. It is never appropriate to allow an auditor to log in to Citrix or Pro-Filer with a staff person's credentials. The procedure is as follows:

1. If a Center-specific auditor account does not already exist, or if additional accounts are required for simultaneous audits, a SAR is required to request creation of auditor accounts (AZAudit1, AZAudit2, etc.). The Quality Professional will be named as the supervisor to approve the SAR. This should be done in advance of the onsite audit, when possible.
2. While logged in to an auditor account, a Communities Connected for Kids employee would apply a simple filter query to limit the client list to what is required for the audit. A read-only version of the complete record is presented by client (i.e., auditors can access all content for queried clients).
3. Center staff should be prepared to supply the auditors with documentation to login to Citrix and Pro-Filer, navigate Pro-Filer, and query for additional client records.
4. When the audit is completed, the IT Department will be responsible for the management of the audit and must notify the HelpDesk to disable the account.

Communities Connected *for* Kids

5. Subsequent requests for account reactivation must be documented in writing. Given the potential need for quick turnaround, this request may be initiated by phone call to the HelpDesk followed by email to the HelpDesk (SAR not required), with a copy to the Pro-Filer account manager. Passwords are changed at each account reactivation.

Approved: DocuSigned by: Carol Deloach 90C0E7A7E02E4BA... Date: 7/27/2022

Carol Deloach, CEO