Children’s Friend and Service

Policy and Procedures

Policy Title: Remote Access Policy

Program or Department: IS Department

Author’s Name and Title: Aimee Mitchell, Viken Jawharjian (CIO)

Title of Staff Member(s) Responsible for Implementation: All

Policy Statement Date Written: April 15, 2015
Policy Statement Date Revised: 
Policy Statement Approved by Board: April 22, 2015
Procedures Written/Revised by: 
Procedures Date Revised: 
Procedures Date Approved by Senior Administration: May 14, 2015

Policy:

The purpose of this policy is to establish uniform security requirements for all authorized users who require remote electronic access to Children’s Friend’s network and information assets. The guidelines set forth in this policy are to limit unauthorized access to Children’s Friend’s information system resources and limit the possible damages that may result from such events.

This policy also establishes guidelines and defines standards for remote access to Children’s Friend’s information resources (networks, systems, applications, and data including but not limited to, electronic protected health information (ePHI) received, created, maintained or transmitted by the organization). Remote access is a privilege, and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Children’s Friend’s established safeguards which protect the security, confidentiality, integrity, and availability of information resources.

Children’s Friend will adhere to HIPAA/HITECH best practices and applicable regulations as noted within this document. These security guidelines will help ensure that the agency’s assets (clients, data, staff, and reputation) are protected from potential vulnerabilities and mitigate risks.
1. **Procedures:**

   a. These safeguards have been established to address HIPAA Security regulations including:

   - Workforce Clearance Procedures [45 CFR §164.308(a)(3)(ii)(B)]
   - Access Authorization [45 CFR §164.308(a)(4)(ii)(B-C)],
   - Automatic Logoff [45 CFR 164.312(a)(2)(iii)],
   - Supervision [45 CFR §164.308(a)(3)(ii)(A)],
   - Termination Procedures [45 CFR §164.308(a)(3)(ii)(C)].
   - Security Management Process (164.308a1i);
   - Security Incident Procedures (164.308a6ii-ii);
   - Sanction Policy (164.308a1iiC);
   - Health Information Technology for Economic and Clinical Health Act (HITECH), revisions to 45 C.F.R. Parts 160, 162, & 164

2. This policy applies to all authorized system users, including members of the workforce, business associates, interns, volunteers and vendors, requiring remote connectivity to Children’s Friend’s networks, systems, applications, and data. Users are frequently categorized in one of these user groups:

   a) **Workforce members with permanent remote access.** These users are often Information Services (IS), executive, or specific administrative staff, business staff, providers, professional staff who require 24-hour system availability and are often called upon to work remotely or who travel often. Their remote access offers the same level of file, folder and application access as their on-site access.

   b) **Contractors and Vendors offering product support with NO access to PHI.** These users have varied access depending upon the systems needed for application or system support, but do not have access to any PHI in the applications or systems. These users access the system on an as needed, or as called upon basis for system troubleshooting.

   c) **Contractors and Vendors offering product support and other Business Associates/Partners with access to PHI.** These users have varied access to PHI depending on the application or system supported and/or accessed. Appropriate Business Associate/Partner Agreements must be on file prior to allowing access, and all such access must be audited on a regular basis.

3. **Key Definitions:**

   a) **Defined Network Perimeter:** Refers to the boundaries of the Children’s Friend’s internal computer network.

   b) **Electronic Protected Health Information (ePHI):** Protected health information means individually identifiable health information that is: transmitted by electronic media,
maintained in electronic media, or transmitted or maintained in any other form or medium.\(^1\)

c) **Firewalls**: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.

d) **Information Resources**: Networks, systems, applications, and data including but not limited to, ePHI received, created, maintained or transmitted by the Children’s Friend.

e) **Protected Health Information (PHI)**: Individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
   a) Past, present or future physical or mental health or condition of an individual;
   b) The provision of health care to an individual;
   c) The past, present, or future payment for the provision of health care to an individual;
   d) Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.\(^2\)

f) **Privileged Access Controls**: Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.

g) **Remote Access**: Remote access is the ability to gain access to a Children’s Friend’s network from outside the network perimeter. Common methods of communication from the remote computer to Children’s Friend’s network includes, but is not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.

h) **Role-Based Access**: Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

i) **Teleworker**: An individual working at home (or other approved location away from the regular work site) on an established work schedule using a combination of computers and telecommunications.

j) **Virtual Private Network (VPN)**: A private network that connects computers over the Internet and encrypts their communications. Security is assured by means of a tunnel connection in which the entire information packet (content and header) is encrypted. VPN technology should use accepted standards of encryption, based, for example, on FIPS 140-2.

---

\(^1\) 45 CFR § 164.503.

\(^2\) § 164.502(f).
k) **Web-based Portal:** A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system. Web-based portals most often use 128-bit or higher SSL encryption.

l) **Workforce Member:** Workforce means employees, volunteers (board members, community representatives), trainees (students), interns, contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.³

m) **Authentication/Security Tokens:** Security tokens are used to prove one's identity electronically. The token is used in addition to or in place of a password to prove that the user is who they claim to be. The token acts like an electronic key to access something. (FortiTokens/RSA Tokens)

4. **Gaining Remote Access:**

   A) Workforce members shall apply for remote access connections by completing an “Employee Status Form” and submitting it to the IS department by their manager. Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion and approval of the workforce member’s manager and IS department.

   B) The workforce member is responsible for adhering to all of Children’s Friend's policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Children’s Friend.⁴

   C) Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with Children’s Friend which clearly defines the type of remote access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors with a defined business need, at the discretion of and approval by the Security Officer or designee.

   D) It is the remote access user’s responsibility to ensure that the remote worksite meets security and configuration standards established by Children’s Friend. This includes configuration of personal routers and wireless networks

2) **Equipment, Software, and Hardware**

   A) The organization will provide any equipment or supplies necessary to ensure proper protection of information to which the user has access. The following assists in defining the equipment and environment required.

   i) **Organization Provided:**

      (1) Encrypted workstation

---

³ 45 CFR § 164.103.

⁴ All P&Ps need to consider remote access.
(2) If individual’s role requires remote connectivity, an organization issued cellular data plan. (Gobi Cards)
(3) Cable lock to secure the workstation to a fixed object
(4) If using a VPN, an organization installed VPN client or issued hardware firewall
   (a) Corresponding Authentication/Security Token to access VPN.
(5) If printing, an organization supplied printer
(6) If retrieving signatures, an agency issued USB signature pad
(7) If approved by management, an organization supplied phone
ii) User Provided (If working from home):
   (1) Broadband connection and fees (Separate from Cellular plan)
   (2) Paper shredder
   (3) Secure office environment isolated from visitors and family
   (4) A safe location to lock and secure documents when unattended.
B) Remote users will be allowed access through the use of Children’s Friend issued equipment, or through the use of the workforce member’s personal computer system provided it meets the minimum standards developed by Children’s Friend, as indicated above.
C) Remote users utilizing personal equipment, software, and hardware are:
   i) Responsible for remote access. Children’s Friend will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
   ii) Responsible for remote access used to connect to the network and meeting Children’s Friend requirements for remote access.
      (1) Up to date Antivirus software
      (2) Installed firewall software/hardware
      (3) Latest operating system patches.
      (4) Approved FortiClient VPN software
      (5) Two factor authentication token
   iii) Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to Children’s Friend.
D) Continued service and support of Children’s Friend owned equipment is completed by IS workforce members. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Children’s Friend to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Children’s Friend.
E) The ability to print a document to a remote printer is not supported without the organization’s approval. Documents that contain confidential business or ePHI shall be managed in accordance with the Children’s Friend’s confidentiality and information security practices.

3) Security and Privacy
A) Only authorized remote access users are permitted remote access to any of Children’s Friend’s computer systems, computer networks, and/or information, and must adhere to all of Children’s Friend’s policies.
B) It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Children’s Friend’s network when access is no longer needed to perform job responsibilities.

C) Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or organizationally sensitive information.

D) Remote access users are automatically disconnected from the Children’s Friend’s network when there is no recognized activity for 15 minutes.

E) It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

F) All remote users will be required to utilize a two factor authentication token in order to login into their agency issued laptop.

G) Remote access users must take necessary precautions to secure all of Children’s Friend’s equipment and proprietary information in their possession.

H) Virus Protection software is installed on all Children’s Friend’s computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may not stop the update process for Virus Protection, on organization’s or the remote user’s workstation.

I) A firewall shall be used and may not be disabled for any reason.

J) Copying of confidential information, including ePHI, to personal media (hard drive, USB, cd, etc.) is strictly prohibited, unless the CIO has granted prior approval in writing.

K) Children’s Friend maintains logs of all activities performed by remote access users while connected to Children’s Friend’s network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 30 days will be disabled.

L) Electronic Data Security
   i) Backup procedures have been established that encrypt data moved to an external media. If there is no backup procedure established or if Children’s Friend has external media that is not encrypted, contact the IS Department for assistance.
   ii) Transferring data to Children’s Friend requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the Children’s Friend.
   iii) Users may not send any ePHI via e-mail unless it is encrypted. If PHI or ePHI needs to be transmitted through email, IS must be contacted to ensure an approved encryption mechanism is used.

4) Enforcement
   A) Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with Children’s Friend’s termination policy.
   B) Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Children’s Friend’s network, and liability for any damage to property and equipment.
Applicable Standards and Regulations:

- 45 CFR §164.312(a)(2)(iii) – HIPAA Security Rule Automatic Logoff

References

Federal Information Processing Standard (FIPS) Publication 140-2
Department of Health and Human Services, Centers for Medicare & Medicaid Services (CMS),"HIPAA Security Guidance” (12/28/2006)

SANS (SysAdmin, Audit, Network, Security) Institute

The Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009 (ARRA)