



Children's IQ Network[®]

Ensuring best security and privacy practices for your office

Protecting passwords and workstation

- *Computers should have screen savers so that unauthorized people cannot read the information if they happen to wander into a restricted area.*
- *Computers should be password protected.*
- *Computers should be configured to time-out when there is inactivity or idle time. On resume, the staff member should be required to enter his/her password.*
- *It is important to ensure that each person in your office has access only to the computer(s) and information to which they are entitled. Toward that end, each user needs to have his/her own password.*
- *Passwords need to be kept confidential (i.e., not shared with anyone else)*
- *Passwords must never be left on "Post-it" notes next to the computer.*
- *Educate employees on how to choose strong passwords that include a mix of uppercase and lowercase letters and numbers; avoid easy-to-guess words such as your child's name, your pet's name or your birthday.*
- *Change your passwords on a regular basis (90-120 days) to ensure security*

Physical Security & Faxing PHI

- *It is important that only staff members gain access to the fax machines, copiers, computers and tablets. This access includes restricted physical access as well as restricted viewing access.*
- *Whenever you fax personal information about a patient you should use a fax cover sheet with a confidentiality statement. The statement should explain that the following fax contains personal medical information and that if the fax is received by anyone other than the intended party, then the fax should be destroyed and they should notify you that it was received in error.*
- *Ensure that you send the information to the correct fax number by using pre-programmed fax numbers whenever possible.*
- *Lock offices containing computing equipment that store personal health information*
- *Immediately report loss or theft of these devices*

Technical Safeguards

- *Securely configure computing equipment with up-to-date anti-virus software and firewalls*
- *PHI (Protected Health Information), Confidential and Personal Identifying information must be encrypted when sending outside the internal network.*
- *Regularly backup electronic health information to another computer file server*
- *PHI (Protected Health Information) and Confidential and Personal Identifying information must be encrypted on mobile computing equipment such as laptops, tablets and smart phones.*
- *Continuously audit health IT operations*

Opt-In and Opt-Out

Provide patients the right to “opt out” of disclosures of their non-public personal information. In order to maximize trust we must protect a patient's right to control what happens to their highly personal medical information.

- *If a patient opts-out of having his/her information shared or provided to family or friends, staff should not release information.*
- *Staff members responsible for release of patient information have received HIPAA (Health Insurance Portability and Accountability Act) specific training. If its not apart of your job, do not release the information.*
- *Any uncertainties should be forwarded to the appropriate staff member.*

Storage Media

Removable storage media can introduce malicious code to the network via USB ports; consequently their use must be better controlled. USB thumb drives and other storage media, pose one of the highest data security risks. Permission should be obtained by a designated practice manager before they can be utilized. The following are best practices for storage media use:

- Patient information should never be stored on unprotected USB thumb drives or other portable media.
- Employees should not access or store any patient information using a thumb drive that has not been authorized and protected by the medical practice.
- Protected information on external storage devices must be encrypted.
- Never leave mobile computing or external storage devices unattended in unsecured areas.
- Immediately report loss or theft of these devices.

Disposal of Information

- For Protected Health Information (PHI) in paper records, shredding, burning, pulping, or pulverizing the records so that Protected Health Information is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- For Protected Health Information (PHI) on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).
- The hard drives of your PC must be physically destroyed or “electronically shredded” using approved software

Name: _____
(Please Print)

Employee ID # _____

Signature: _____

Date: _____