Shànt Wellness
chiropractic • yoga • acupuncture

3840 E. Semoran Blvd. Suite 1054, Apopka, FL 32703
Ph: (407) 880-1218 Fax: (407) 749-0328

INTERNET SECURITY POLICY

Purpose

This office has adopted this Internet Security Policy to comply with HIPAA as well as our duty to protect the confidentiality and integrity of protected health information as required by law, professional ethics, and accreditation requirements. All employees of this practice must comply with this policy

Assumptions

This Internet Security Policy is based on the following assumptions:

- Our office benefits from access to and use of the Internet and its resources.
- The resources, services, and interconnectivity available via the internet provide significant resources to improve the efficiency of this practice.
- Use of the internet also involves more risks than an intranet.
- Improper use of the internet puts this practice and its employees at risk.
- The content of all web pages under this practice's jurisdiction must comply with local, state, and federal laws and its own policies and procedures.
- A policy is necessary to clarify the proper use of the internet to maintain the accuracy, security, and confidentiality of individually identifiable health information and other sensitive data.
- This office's system used to access the internet is the property of the practice and is subject to the office's control of such use.
- Data users have no expectation of privacy when using the office's system to access the internet.

Policy

This policy applies to all officers, employees, and independent contractors of this office who use its system for internet access and governs all internet access, communications, and storage using this practice's system.

All data users must strictly observe the following rules when using the internet:

- Users may not access or use the internet for personal business or personal commercial gain.
- Users must have a proper medical or business purpose for any access and use of the internet.
- Users may not access pornographic or other offensive websites (including, but not limited to, sexist, racist, discriminatory, hate, or other sites that would offend a reasonable person in the same or similar circumstances). If the user has any doubt whether access to a specific site is proper, he or she should seek approval from the Security Officer.

Form Copyright © 2013 by InstaCode Institute.
Form may only be copied and/or customized by the owner of this book for use in his/her own office.

- Access control:
    - Users may not use any other user’s ID, password or other identification to access the internet.
    - Users attempting to establish a connection with this office’s computer system via the internet must authenticate themselves at a firewall before gaining access to its internal network.
    - Users may not establish modems, internet, or other external network connections that could allow unauthorized users to access this practice’s system or information without the prior approval of the Security Officer.
    - Users may not establish or use new or existing internet connections to establish new communications channels without the prior approval of the Security Officer.
- Users may not transfer individually identifiable health information or the practice’s business information via the internet without prior approval of the Security Officer. Before transmitting individually identifiable health information, the user will comply with our Privacy Policy to ensure legal authority for the disclosure exists. The Privacy Officer is responsible for ensuring Business Associate Agreements are in place to protect the security and confidentiality of information transmitted via the internet when necessary.
- This practice supports strict adherence to software vendors’ license agreements. Data users may not copy software in any manner that is inconsistent with the vendor’s license.
- Users may not download and/or install software without prior permission from the Security Officer.
- Users must **not** open any email attachments they are not expecting to receive. Questionable emails should be referred to the appropriate compliance officer.
- At any time and without prior notice, this office reserves the right to audit internet access in accordance with our HIPAA policies.
- No data user may attempt to probe computer security mechanisms at our office or other internet sites unless part of an audit approved by the Security Officer.
- Data users will report security problems with internet use, breach of confidentiality, and any violations of this or other policies and procedures occurring during internet use in accordance with this office’s HIPAA incident reporting procedures.

Compliance and Enforcement

- All employees are responsible for adhering to and enforcing this policy. Employees who violate this policy are subject to disciplinary action up to and including termination.

Form Copyright © 2013 by InstaCode Institute.
Form may only be copied and/or customized by the owner of this book for use in his/her own office.