PROFESSIONAL PROTECTOR PLAN® FOR DENTISTS | PPP

Computer Use Policy

John Doe, DDS

Policy Statement

We are required by law to protect the privacy and security of our patients' protected health information. Since much of this information is now stored digitally on the computer network, we are required by HIPAA security standards to take certain precautions to ensure the integrity of this data.

Part of this security is through hardware and software such as firewalls, routers, antivirus programs, password systems, and monitoring systems.

Another part of the security program involves written office policy concerning computer use.

In general, the use of Clinic computers (including any type of internet access) is for Clinic business purposes only. This will minimize the risk of inadvertently introducing a computer virus, Trojan horse, spyware, or other malware.

Misuse of Clinic computers, networks, and Internet access may result in disciplinary action, up to and including termination of employment.

Examples of Misuse

The following list contains examples of misuse. This list is not exhaustive.

- Logging onto computer by using someone else's password.
- Revealing your password to others, or allowing use of your password by others, including other employees, family members, or other household members.
- Attempting to circumvent data protection, security restrictions, or usage/history logs.
- Engaging in private or personal business activities.
- Attempting to change computer date or time.
- Sending, receiving, or otherwise accessing personal email.
- Accessing social network sites.
- Participating in chat rooms, instant messaging, blogs, or forums for non-business use.
- Use of social media to post, discuss, or otherwise reveal any information related to patients in any manner.
- Making unauthorized copies of Clinic files or other Clinic data.
- Installing, storing, or using software programs that are not authorized by Clinic technicians.
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access.
- Destroying, deleting, erasing, or concealing files or other data, or making files or data unavailable or inaccessible to others or to other authorized users of Clinic systems.

- Deliberately introducing any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the network or systems.
- Sending, receiving, or accessing pornographic materials.
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private communications.
- Failing to log off if leaving a computer unattended.
- Using computer system for any illegal or unauthorized purpose, or any other use that is deemed excessive by administration.

Email, Internet Access, and Computer Files--No Expectation of Privacy

The Clinic owns the rights to all data and files in any computer or network used in the Clinic. This includes all data and files sent or received using any Clinic system, or data transmitted by using the Clinic's access to any other network, such as the Internet. The Clinic reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.

Employees must be aware that the electronic mail messages sent and received using Clinic equipment or Clinic- provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by Clinic officials at all times. The Clinic has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with Clinic policies and state and federal laws

The Clinic uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on Clinic electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Clinic use at any time.

Employees who wish to maintain their right to confidentiality must send or receive such information using some means other than Clinic systems or the Clinic-provided Internet access.

Use of Social Media

While the Clinic encourages its employees to enjoy and make good use of their off-duty time, certain activities on the part of employees may become a concern if they have the effect of impairing the work of any employee; harassing, demeaning, or creating a hostile working environment for any coworker; disrupting the smooth and orderly flow of work within the office; or harming the goodwill and reputation of the Clinic among its patients or in the community at large.

In the area of social media (print, broadcast, digital, and online services such as Facebook, LinkedIn, MySpace, Plaxo, and Twitter, among others), employees may use such media in any way they choose as long as such use does not produce the adverse consequences noted above, and as long as it is during their off-duty time. For this reason, the Clinic reminds its employees that the following guidelines apply in their use of social media, both on and off duty:

1. If an employee publishes any personal information about the employee, a coworker, the doctor, the Clinic, a patient, or a customer in any public medium (print, broadcast, digital, or online) that:

a. has the potential or effect of involving the employee, their coworkers, or the Clinic in any kind of dispute or conflict with other employees or third parties.
b. interferes with the work of any coworker.
c. creates a harassing, demeaning, or hostile working environment for any coworker.
d. disrupts the smooth and orderly flow of work within the office, or the delivery of services to the Clinic's patients or customers.
e. harms the goodwill and reputation of the Clinic among its patients or in the community at large; or
f. tends to place in doubt the reliability, trustworthiness, or sound judgment of the person who is the subject of the information,

the employee(s) responsible for such problems will be subject to counseling and/or disciplinary action, up to and potentially including termination of employment, depending upon the severity and repeat nature of the offense.

2. Employees who conduct themselves in such a way that their actions toward and relationships with each other interfere with or damage work relationships, disrupt the flow of work or patient relations, or cause unfavorable publicity in the community, should be concerned that their conduct may be inconsistent with one or more of the above guidelines. In such a situation, the employees involved should request guidance from Clinic management to discuss the possibility of a resolution that would avoid such problems. Depending upon the circumstances, failure to seek such guidance may be considered evidence of intent to conceal a violation of the policy and to hinder an investigation into the matter.

Criminal Activity

Use of Clinic computer systems that involve any kind of criminal activity or harms the rights of others may result in criminal prosecution or civil liability to those harmed, or both.

Acknowledgement of Understanding of Policy

“I have read this Computer Use Policy, and have had any questions answered that I might have”.

_____ _____

Employee Date