HILTZ & ASSOCIATES
Insight • Diligence • Assurance.

Tel: (201) 503-3742
Fax: (855) 440-8624

Email: hello@hiltzandassociates.com
Web: www.hiltzandassociates.com
Facebook/Twitter @BetterCallBill

This a sample "code business conduct" for dental practices is provided on an "as-is" basis.

COMPUTER SYSTEMS AND BUSINESS COMMUNICATIONS

Employees have the responsibility to operate all Practice computer and communication resources in a professional, lawful, and ethical manner.

Technical advances are making it easier, via mobile phones, networks, E-mail, and the Internet, to share information with others. These are useful tools, but it means that valuable information needs to be protected from unwanted access, use or disclosure.

Every Practice employee is responsible for protection of information. This always applies, whether an employee is using a Practice computer or accessing the Practice's systems in a Practice office or an outside location.

NOTIFICATION OF AUDIT LOGGING

To ensure compliance with HIPAA[1] and to ensure the security and confidentiality of electronic records, the Practice's computer systems maintain comprehensive audit and event logs that automatically record staff actions.

An audit log (also called audit trail) is a security-relevant chronological record, set of records, that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Audit records typically result from activities such as financial transactions, and health care data transactions, or communications by individual people, accounts, or other entities.

Our dental software automatically logs when users edit, modify or delete transactions and accounts. The audit log records each entry and shows the action that was performed, the associated user account, and the date and time of the action.

GENERAL USE

All Practice telephones, electronic communication devices and computer systems, including, but not limited to, computers, laptops, servers, networks, cell phones, and tablets are Practice property. The purpose of these systems is to conduct Practice business.

Practice systems are not to be used to solicit others for commercial ventures, religious or political causes. Users are prohibited from distributing chain letters. Further, the systems must not be used in any way that would violate any the Practice's Computer Use Policy, including the Practice's policies against

[1] Change to PIPEDA for Canadian Dental Office

discrimination, slander and harassment, for example, by the transmittal or accessing of offensive material of any kind (obscene jokes, stories, or pornography).

Use of electronic communications must conform to our Practice's business standards and policies, including the electronic security standards and privacy policies.

Occasional and limited use of the Practice systems for personal reasons such as telephone calls, email and limited Internet usage is permissible provided such personal use does not violate Practice policies or law, interfere with an employee's job responsibilities or minimum hours of work or overburden Practice resources on an individual or aggregate basis.

The Practice reserves the right to terminate an employee's right to use Practice systems for personal communications and to take further appropriate employment action if in the judgment and sole discretion of the Practice, such personal use of Practice systems is inappropriate.

All documents, data, and information, and any E-mail, voice mail or other forms of electronic messages, composed, sent, stored and received on or over the Practice's systems are the property of the Practice.

This includes, but is not limited to, telephone and computer systems, voice mail, websites (Internet and intranet), and E-mail systems to prevent abuses or misuses, or for any other legitimate business reason. Since information technology resources are the property of the Practice, users of these systems are advised that there is no expectation of privacy while using these systems.

Employees should assume that all email and voice messages might be accessed by someone other than the designated recipient.

The authenticity, confidentiality, and integrity of electronic communications cannot be guaranteed, whether transmitted over the Internet or through the E-mail or voice mail systems.

It should be noted that even when a message is erased, it might still be possible to recreate the message. Therefore, ultimate privacy of messages cannot be ensured.

E-MAIL AND VOICE MAIL

The Practice maintains electronic messaging systems, including voice mail and E-mail. These systems are provided to assist in conducting Practice business.

It should be noted that the E-mail systems are backed up daily and these records can be used to respond to legal document requests or can be audited in the normal course of business. Subpoenas and other legal document requests usually require production of electronically stored documents and records.

E-mail, like other forms of electronic communication, is susceptible to misdirection and may be misaddressed. Information of a highly sensitive nature should be sent by electronic means with great care. Addresses of messages should be checked, and sensitive documents should be password protected or encrypted prior to sending.

PASSWORD USAGE

One of the Practice's most valuable assets is the information stored on the Practice network and computer systems. The confidentiality and integrity of data stored on Practice systems must be protected. The use of passwords and the implementation of password controls ensure that access is limited only to authorized personnel. Passwords provide the entry checkpoint to all computer resources. Every Practice employee must keep passwords private to prevent unauthorized access.

INTERNET USAGE

Keep in mind that all information posted on the Internet is "off the record". The proliferation of negative or careless E-mail, employee blogs, websites, news, or bulletin board messages can be damaging to the Practice.

Only the Practice's owner(s) or a designated employee(s) may author or approve material on the Internet that contains information about the Practice or any of its products or services; respond to E-mail or reply to a social media post on behalf of the Practice.

Any employee who finds or receives negative information about the Practice or any of its products on any news group bulletin board or a mail list should not reply but immediately contact the Practice's owner(s).

SECURITY AND APPROPRIATE USE

A. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the dentists, employees are prohibited from engaging in, or attempting to engage in:
    i. Monitoring or intercepting the files or electronic communications of other employees or third parties;
    ii. Hacking or obtaining access to systems or accounts they are not authorized to use;
    iii. Using other people's log-ins or passwords; and
    iv. Breaching, testing, or monitoring computer or network security measures.
B. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.
C. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system. (e.g.: downloading from YouTube, Pirate Bay, Torrents)
D. Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

ACTIVITIES EXPRESSLY PROHIBITED

Employees are expressly prohibited from:

a) Accessing computers, data and programs for which the employee is not authorized.

b) Sharing passwords and account with another employee. Each employee Each individual is given a unique username and password used to access our computer systems.
c) Violating copyright laws or software license agreements.
d) Installing software including freeware, shareware, public-domain or commercial software on any office-owned computer equipment without appropriate permission.
e) Using computers for unauthorized non-office-related commercial or for-profit activity.
f) Sending or forwarding electronic mail for unauthorized purposes
g) Using the Internet for non-office related activities.
h) Any activity which violates local or federal laws.

Employee Acknowledgement

I have been given a copy of the Practice Code of Business Conduct.

I agree to abide by these provisions and further understand that this Professional Code of Business Conduct may be revised from time to time and that I will be made aware of the changes.

I understand that the Practice computer systems maintain audit and event logs, and that there is no expectation of privacy when using any of the Practice's computer systems, Internet, email, or services.

Date: _____

Signature: _____

Name: _____
(Please print)