Talking Ethics

Responsibility Without Power: The Dilemma of Privacy Compliance for Canadian Dental Hygienists
by Anne Genge, CIPP/C, CHSP, CCSP • agenge@healthcarecompliance.ca

The Dental Hygienists’ Code of Ethics states that a dental hygienist’s primary responsibility is “to the client.” Furthermore, dental hygienists are bound to conduct themselves in accordance with applicable laws and guidelines, and are mandated to report non-compliance that they may witness.¹

PRIVACY COMPLIANCE FOR DENTAL HYGIENISTS PRESENTS A CHALLENGE
If you work in or operate a dental/hygiene practice in Canada, you are subject to the same health care privacy laws as hospitals and other large organizations. Unless you own your practice, you are at a disadvantage, since you are not likely the decision maker in your workplace. It is also unlikely that you would have access to teams of privacy personnel, large security budgets or robust training and policy development. Still, the government and your clients demand and expect safeguards for personal health information.

WHAT’S HAPPENING?
The loss and misuse of client information is increasing exponentially. Breaches of client confidentiality are becoming epidemic. According to the Ponemon Institute, a world leader in information technology research, health care organizations of all sizes experience data breaches, putting the personal security of clients at risk and costing the health care system millions of dollars.²

In Canada, health care privacy legislation is largely a provincial responsibility. Although the Personal Information Protection and Electronic Documents Act (PIPEDA) exists at the federal level, there are specific health privacy acts in most provinces (see, for example, www.ipc.on.ca). Additionally, dental and dental hygiene colleges have their own professional guidelines, which essentially reinforce the jurisdictional acts.

YOU ARE RESPONSIBLE
The bottom line is that, anywhere you practise in Canada, you are responsible for client information, regardless of whether you're a practice owner, administrative staff or a clinical dental hygienist. It's a group effort, but you can be held responsible individually. You are responsible for the security of data not only from criminal attacks, but also from things that are seemingly innocuous, such as “snooping” (looking at a client record for purposes other than providing health care).

HOW DO YOU PRACTISE?
The challenges for dental hygienists depend on the nature of their workplace. For example, if you own your own clinic then you are the health information custodian and, by default, you become the privacy officer/information officer. In other words, you are in charge of setting the policies and procedures under which your practice must operate to secure and safeguard client data. You are the enforcer of the rules, and you control most aspects of the client record.

Continued...
A more difficult situation (and the most common) arises when dental hygienists work in someone else’s practice. In this scenario, you are still responsible for client information, but are likely not the decision maker on policy, procedures, and data security. No matter how much you may want to comply, you may not be able to do so.

HERE’S WHERE IT GETS STICKY...AND SOMEWHAT SCARY

1. **Tracking**
   Governments and colleges want practices to have individual computer logins (user name/password) for each user, so they can audit “who did what.” This is a network configuration issue and a decision made by others, which impacts your ability to be compliant on many levels. There are still many practices in which computers and client management system access are shared through a single common password.

2. **Understanding laws**
   In most parts of Canada, health care practitioners must have annual privacy and security training. Yet many dental practices still lag behind in embracing good training and review practices for information privacy. In such cases, dental hygienists must then seek this training externally for themselves.

3. **Availability of data**
   If you’re not in control of the database, its configuration, security or backup, you may one day lose access to your clients’ charts. What happens if all your notes “disappear” because of hacking, viruses or a system failure?

**WHAT CAN YOU DO?**
As always, “challenging for change” can be a precarious venture. We want to be part of the betterment of the practice without rocking the boat, and trying to be compliant with other regulations already overwhelms many practice owners. Privacy, however, requires daily vigilance. It must be pushed to the top of the priorities list.

My experience is that dental practices in this country are still severely exposed and, by extension, so are dental hygienists. I encourage dental hygienists to engage their practice owners to establish rock-solid privacy and security measures. A breach will not only tarnish reputations, but it can have heavy collegial and financial consequences for practice owners and staff members.

Prevention is critical in training, policy, and network security. Surprisingly, preventive measures are not expensive, especially when hundreds and often thousands of dollars are wasted fixing “silly” mistakes. Many practice owners don’t realize that there are newer and better ways to be protected. Most are pleasantly surprised by reduction of downtime and system failures once proper solutions are deployed in their network. Healthcare Compliance Network Inc. (HCN) specializes in affordable turn-key privacy compliance and IT security for dental offices, and welcomes questions and comments from CDHA members via email at info@HealthcareCompliance.ca

**References**