

CDHO Advisory: Clinical Information Practice Standard

COLLEGE OF DENTAL HYGIENISTS OF ONTARIO ADVISORY

ADVISORY TITLE

Clinical Information Practice Standard for Dental Hygiene

ADVISORY STATUS

Cite as

College of Dental Hygienists of Ontario, Clinical Information Practice Standard for Dental Hygiene, October 2010

SCOPE

RESPONSIBILITIES FOR PROTECTION OF PERSONAL HEALTH INFORMATION AND PRIVACY OF PATIENTS/CLIENTS

Registrants have responsibilities

1. that arise in contexts such as dental hygiene practice in
 - a. a dental office
 - b. a healthcare facility or medical clinic
 - c. a mobile dental hygiene service
 - d. a residential or long-term care facility
 - e. an independent dental hygiene office.
2. for prevention of the risk to their patients/clients of harm associated with personal health information that is
 - a. insufficiently protected
 - b. unavailable when needed for the purposes of safely providing oral healthcare
 - c. inaccurate
3. for compliance with legal and ethical requirements for the protection of personal health information
4. for respect for the privacy-related concerns and sensitivities of individual patients/clients

THE IMPORTANCE OF GOOD INFORMATION MANAGEMENT PRACTICES FOR DENTAL HYGIENISTS

Dental hygienists are required to have good information practices to

1. protect the personal health information of all their patients/clients within the relevant frameworks of
 - a. applicable legislation
 - b. common law duties, including negligence
 - c. professional standards of the College of Dental Hygienists of Ontario
2. respect the privacy-related concerns and sensitivities of
 - a. every individual patient/client

- b. patients/clients with medical conditions that
 - i. may affect their
 - 1. attitudes to the collection and sharing of personal health information
 - 2. perceptions about the use, misuse and abuse of personal health information
 - ii. may require the dental hygienist to obtain advice from
 - 1. an appropriate physician or other healthcare provider
 - 2. the College of Dental Hygienists of Ontario
 - 3. Legal Counsel
 - 4. Office of the Information and Privacy Commissioner of Ontario

INTENDED USERS

Advanced practice nurses	Nurses
Dental assistants	Patients/clients
Dental hygienists	Pharmacists
Dentists	Physicians
Denturists	Public health departments
Dieticians	Regulatory bodies
Health professional students	

TARGET POPULATION

The target population comprises

1. The full demographic range of patients/clients of dental hygienists.
2. Subgroups of the full range characterised by particular sensitivities, special needs or specific medical conditions.
3. Caregivers for persons with special needs or medical conditions.
4. Parents or guardians of children and young persons.

ADVISORY OBJECTIVES

1. For persons receiving oral healthcare, by promoting fulfillment by dental hygienists of their responsibilities, to achieve
 - a. maximization of health benefits associated with appropriate use of personal health information
 - b. minimization of harm arising from
 - i. inadequate protection of personal health information of the [target population](#) served by dental hygienists
 - ii. insufficient respect for the privacy-related concerns and sensitivities of individual patients/clients.
2. For dental hygienists, to provide guidance in
 - a. understanding the harm that may result from
 - i. inadequate management and protection of personal health information
 - ii. insufficient respect for the privacy-related concerns and sensitivities of individual patients/clients
 - b. sourcing information about protection of personal health information in the various types of dental hygiene practice

- c. using information about protection of personal health information in the various types of dental hygiene practice
- d. taking the history of the experience, concerns and preferences of the patient/client relative to the handling of his/her sensitive personal health information from
 - i. a medical perspective
 - ii. an information management perspective
- e. deciding when to seek advice about
 - i. responsibilities and requirements
 - ii. dealing with adverse events, such as failure in the application of management and protection for personal health information
 - iii. legal or ethical issues
- f. identifying and contacting the most appropriate source(s) of expertise for advice about problems pertaining to
 - i. medical concerns
 - ii. information management issues in various types of dental hygiene practice
- g. communicating to the patient/client the methods for management and protection of personal health information and for respecting privacy in the dental hygienist's practice.

RECOMMENDATIONS

TERMINOLOGY

Terminology varies: that which is used in the present Advisory reflects common but not necessarily universal usage.

1. **Availability.** The state in which information is accessible and useable upon demand by an authorized person.
2. **Breach.** The unauthorized acquisition, access, use, or disclosure of personal information where there is the actual or potential risk of harm to the individuals whose personal information has been the subject of such unauthorized acquisition, access, use, or disclosure. A breach is a form of [incident](#).
3. **Caregivers.** A person who provides care to individuals who, because of disability, debility or other health-related reasons, depend on others for care of various types; caregivers are
 - a. individuals with a relationship to the person receiving care, including but not limited to spouses, partners, parents, children, siblings, friends, neighbours and co-workers of the person receiving care
 - b. personal service workers.
4. **Circle of Care.** A term that describes [health information custodians](#) and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct healthcare. Circle of care is implied but not defined by Ontario's *Personal Health Information Protection Act, 2004*.
5. **Confidentiality.** The state in which information is not made available or disclosed to unauthorized individuals or organizations.
6. **Consent.** The acceptance, agreement or approval of a proposed action or outcome. Under Ontario's *Personal Health Information Protection Act, 2004*, consent must be knowledgeable. The form of consent may be implied or expressed.

7. **Disclosure.** The release, transfer, provision of access to, or divulgence in any other manner, of information to another individual or organization that is not an agent of nor service provider of the [health information custodian](#).
8. **Electronic Dental Record.** The record of an individual's personal dental health information including health status and care, in an electronic format that is created, managed, and accessed by authorized healthcare providers within a practice, clinic or multidisciplinary team.
9. **Electronic Health Record.** The record of an individual's personal health information including health status and care, in an electronic format that is created, managed, and accessed by authorized healthcare providers and which is shared or easily accessible within one or among several healthcare organizations.
10. **Electronic Medical Record.** The record of an individual's personal health information including health status and care, in an electronic format that is created, managed, and accessed by authorized healthcare providers within a practice, clinic or multidisciplinary team.
11. **Express Consent.** [Consent](#) that is expressly communicated by an oral or written statement.
12. **Hacker.** An individual who "hacks" or circumvents security mechanisms in technology systems (such as networks and applications) to interfere with the [information security](#) of computer systems.
13. **Health Information Custodian.** The 'health information custodian' as that term is defined in Ontario's *Personal Health Information Protection Act, 2004*, is a person who has custody or control of personal health information and who is listed within the definition of a 'health information custodian' in that legislation. A 'healthcare practitioner', defined in the legislation to include 'a person who is a member within the meaning of the *Regulated Health Professions Act, 1997* and who provides health care', is a 'health information custodian'. A dental hygienist is a healthcare practitioner and accordingly is a health information custodian under Ontario's *Personal Health Information Protection Act, 2004*.
14. **Identity Theft.** Theft of identity data such as provincial health insurance numbers or credit card data for criminal purposes.
15. **Implied Consent.** Consent that is inferred from signs, actions, circumstances or facts. Implied consent may also be inferred by inaction or silence.
16. **Incident.** The violation of policy or procedure which constitutes a potential [breach](#) or results in an actual breach.
17. **Information Security.** The preservation of [confidentiality](#), [integrity](#) and [availability](#) of information.
18. **Integrity.** The state in which information has not been altered or destroyed in an unauthorized manner.
19. **Knowledgeable Consent.** [Consent](#) where it is reasonable in the circumstances to believe that the individual knows the purposes of the proposed action or outcome, and that the individual may give or withhold consent.
20. **Opportunistic.** A type of threat which takes advantage of situations in which protections are temporarily or permanently weak.
21. **Personal Health Information.**
 - a. 'Personal health information' as that term is defined in Ontario's *Personal Health Information Protection Act, 2004*.
 - b. Generally, personal health information may be considered as information about an individual, whether in oral or recorded form, that identifies or permits the identification of an individual and which relates to the physical or mental health of the individual or the provision of healthcare to that individual.
22. **Personal Information.** Information about an identifiable individual including name, address, health card number, social insurance number, and credit card number.

23. **Phishing.** A form of Internet fraud with the objective of stealing valuable personal information. Usually, an e-mail is sent requesting the recipient to access a replica of a trusted web site and to enter [personal information](#), including credit card numbers, social insurance numbers, user IDs and passwords. The term is derived from "fishing," where bait is used to catch a fish. In phishing, e-mail serves as the bait.

HARM ASSOCIATED WITH INADEQUATE PROTECTION OF PERSONAL HEALTH INFORMATION

*[Please see source list on page #9](#)

1. The practice of dental hygiene, like all other professional healthcare practice, relies on the open disclosure of [personal health information](#), which
 - a. is a particularly sensitive type of information
 - b. requires the use of processes, which are not free from risk, by which the information is collected, used, disclosed, processed, retained and ultimately destroyed
 - c. if the information is inadequately protected or is inaccurate, may
 - i. place patients/clients of dental hygienists at risk of [harm](#)
 - ii. diminish or lose the trust of individual patients/clients in
 1. individual dental hygienists
 2. the profession of dental hygiene.
2. The practice of dental hygiene, in relation to information management, requires awareness of the
 - a. [harm](#) that may result where the Registrant, employee or service provider failed to minimize the risk
 - b. actions by which there is minimization of harm, to the extent possible, through prudent information management and protection in
 - i. self-initiated dental hygiene practice
 - ii. non-self-initiated dental hygiene practice
 - c. causes of information-related [harm](#) to patients/clients, focused chiefly on their nature, which is [opportunistic](#), resulting in inappropriate access, which may be
 - i. unintended
 - ii. unethical
 - iii. uncompliant to legislative requirements
 - iv. unlawful in the sense of criminal law, chiefly comprising
 1. identity theft
 2. fraud
 - d. potential for occurrence on a large scale of harm to persons
 - e. nature and severity of information-related harm to patients/clients, as classified in [Health informatics – Classification of safety risks from health software ISO/TS 25238:2007](#) as
 - i. catastrophic; involving multiple
 1. deaths
 2. permanent, life-changing incapacity
 3. instances of
 - a. any condition for which the prognosis is death or permanent life-changing incapacity
 - b. severe injury or severe incapacity from which recovery is not expected in the short term
 - ii. major, involving
 1. single instance of

- a. death
 - b. permanent life-changing incapacity
 - c. any condition for which the prognosis is death or permanent life-changing incapacity
 - 2. multiple instances of
 - a. severe injury or severe incapacity from which recovery is expected in the short term
 - b. severe psychological trauma
- iii. considerable, involving
 - 1. single instance of
 - a. severe injury or severe incapacity from which recovery is expected in the short term
 - b. severe psychological trauma
 - 2. multiple instances of
 - a. minor injury or injuries from which recovery is not expected in the short term
 - b. significant psychological trauma
- iv. significant, involving
 - 1. single instance of
 - a. minor injury or injuries from which recovery is not expected in the short term
 - b. significant psychological trauma
 - 2. multiple instances of
 - a. minor injury from which recovery is expected in the short term
 - b. minor psychological upset; inconvenience
- v. minor, involving single instance of
 - 1. minor injury from which recovery is expected in the short term
 - 2. minor psychological upset
 - 3. inconvenience
 - 4. any negligible consequence
- f. classification of breaches and related matters that lead to harm
 - i. types of systems in which breaches occur
 - 1. paper record systems
 - 2. computers and accessories, including
 - a. laptops
 - b. desktops
 - c. mobile devices
 - d. network servers
 - e. drives, media and storage
 - i. CDs
 - ii. hard and portable drives
 - iii. backup tapes
 - iv. flash drives
 - 3. communications systems
 - a. voice mail
 - b. e-mail
 - c. fax machines
 - ii. types of breaches that lead to harm, include

1. inappropriate usage including unauthorized access, leading to loss of data
2. unauthorized access for the purposes of
 - a. curiosity
 - b. malice
3. poor management of passwords
4. failure to protect information in circumstances where it transported or stored on mobile devices by
 - a. anonymization
 - b. encryption
5. use of a computer for both personal and professional uses, which carries the risk of inadvertent distribution of personal health information if file-sharing programs are used
- iii. fraudulent use of information, which may occur through
 1. [hacking](#)
 2. social engineering including [phishing](#)
 3. inadequate tracking and auditing of usage
 4. misdirected or misaddressed e-mail, fax, or voice messages with or without attachments
 5. theft of paper documents
 6. unauthorized access to paper documents
 7. incorrect mailing of paper documents
- iv. particularly sensitive information pertaining to
 1. the identification data of patients/clients, healthcare providers, next of kin, guardians, and [caregivers](#), such as
 - a. health card numbers
 - b. social insurance numbers
 - c. insurance policy numbers and related data
 - d. credit card numbers
 2. the patient/client's medications
- g. types of risks that may arise when a desktop or laptop computer is connected to a network.

PERSONS AT PARTICULAR RISK OF HARM AND ITS CONSEQUENCES

Persons at particular risk of [harm](#) if their personal health information is not protected or their privacy is not assured include those with

1. mental disorders, which
 - a. include
 - anxiety disorders ([CDHO Advisory](#))
 - autism spectrum disorders ([CDHO Advisory](#))
 - bipolar disorder ([CDHO Advisory](#))
 - dementia ([CDHO Advisory](#))
 - depression ([CDHO Advisory](#))
 - fetal alcohol spectrum disorder ([CDHO Advisory](#))
 - psychosis and schizophrenia ([CDHO Advisory](#))
 - b. may lead to
 - i. stigmatization

- ii. reluctance to disclose relevant medical or social history, which may put at risk the health and safety of
 - 1. themselves
 - 2. their family members
 - 3. the wider public
 - iii. accentuation of paranoid beliefs and behaviours, such as feelings of being spied on
 - iv. conflicting interpretations of the medical history associated with symptoms of mental disorder, such as
 - 1. confusion
 - 2. memory problems
 - v. irritation, anger or aggression in response to history taking
- 2. drug or alcohol dependency ([CDHO Advisory](#)), which may lead to reluctance to disclose relevant medical or social history, which puts at risk the health and safety of
 - a. themselves
 - b. their family members
 - c. the wider public
- 3. particular categories of infectious disease, including
 - a. sexually transmitted disease
 - b. HIV/AIDS ([CDHO Advisory](#))
 - c. tuberculosis, latent or active ([CDHO Advisory](#))
- 4. medical conditions complicated by a history of
 - a. incorrect diagnosis because of medical errors
 - b. incorrect reporting because of errors in laboratory or other test results
 - c. erroneous attribution of important information because of confusions of identity arising from non-medical causes as well as medical factors.

PRIVACY NEEDS, CONCERNS AND SENSITIVITIES OF INDIVIDUAL PATIENTS/CLIENTS

In general, the dental hygienist should enquire about privacy-related concerns and sensitivities of individual patients/clients and, where appropriate, include these in the dental hygiene record to

- 1. report that an opportunity was taken to apprise the patient/client of the privacy policy of
 - a. the dental hygienist
 - b. the office or facility in which the dental hygienist practices
- 2. alert other dental hygienists or professional colleagues in the [circle of care](#) to an individual whose history is suggestive of [particular sensitivity to information-related harm](#)
- 3. highlight needs for medical advice if the fears and sensitivities seem excessive or inappropriate.

REQUIREMENTS FOR PROTECTING PERSONAL HEALTH INFORMATION IN RECORDS

- 1. General requirements
 - a. For all patients/clients for whom the dental hygienist provides oral healthcare, the dental hygienist is required to
 - i. protect the [personal health information](#) in all records compiled for individually identifiable patients/clients, as specified
 - 1. in [Ontario Regulation 9/08](#) Part III.1, Records
 - 2. in [Ontario's Personal Health Information Protection Act, 2004](#)
 - 3. elsewhere in law

- ii. comply with the requirements for additional clinical information pertaining to particular medical conditions as stipulated in the relevant CDHO Advisories
 - iii. protect the privacy of identifiable individuals in accordance with the College of Dental Hygienists of Ontario's [Standards of Practice](#)
 - iv. ensure the security of their personal health by
 1. assuring the confidentiality of their personal health information
 2. assuring the integrity of their personal health information by keeping their records up to date
 3. assuring the availability of their personal health information by
 - a. avoiding loss of personal health information
 - b. ensuring that any electronic dental record keeping system in dental hygiene use
 - i. complies with relevant standards
 - ii. is maintained with authorized updates
 - v. with the patient/client, be
 1. transparent about the handling of personal health information
 2. ready to engage in discussion about
 - a. privacy-related concerns and sensitivities
 - b. policy or polices relevant to particular privacy-related concerns and sensitivities
 - vi. obtain knowledgeable consent for collection, use and disclosure of personal health information
 - vii. upon discovery or suspicion of an incident or a [breach](#), promptly take steps appropriate for
 1. self-initiated practice
 2. non-self-initiated practice.
2. Specific requirements
- For all patents/clients for whom the dental hygienist provides oral healthcare, the dental hygienist is required to adhere to specific information management and information protection requirements as published from time to time by the College, as follows.

SOURCES OF INFORMATION PERTAINING TO RESPONSIBILITIES AND REQUIREMENTS

Sourcing information

Sources of general information

- [American Medical Association, New Health Privacy and Security Requirements](#)
- [BC Physician Privacy Toolkit](#)
- [Canadian Medical Protective Association, Electronic Records Handbook](#)
- [eHealth Ontario Guide to Information Security for the Health Care Sector](#)
- [Electronic Health Information Laboratory](#)
- [Health informatics — Classification of safety risks from health software ISO/TS 25238:2007](#) (Payment required)
- [Information technology — Security techniques — Code of practice for information security management ISO/IEC 27002 2005](#) (Payment required)
- [Office of Information and Privacy Commission, Ontario](#)
- [U.S. Department of Health & Human Services, Breaches Affecting 500 or More Individuals](#)

IDENTIFYING AND CONTACTING THE MOST APPROPRIATE SOURCE OF ADVICE

1. Given the increasing role of dental hygiene in health protection the likelihood is increasing that dental hygienists will encounter complex questions arising in connection with care
 - a. of the elderly at home or in facilities
 - b. of persons of all ages with diseases that may be
 - i. long-term
 - ii. incurable
 - iii. socially sensitive.
2. In particular situations, the dental hygienist may not feel comfortable recording or disclosing PHI and therefore, in such instances, should seek
 - a. competent legal counsel on questions of law
 - b. advice from the College of Dental Hygienists of Ontario on
 - i. matters of ethics
 - ii. uncertainties of a professional nature.

BENEFITS/HARMS OF IMPLEMENTING THE GENERAL AND SPECIFIC REQUIREMENTS**POTENTIAL BENEFITS**

1. Promotion of health through oral healthcare for individual patients/clients by
 - a. protecting personal health information by fulfilling the appropriate requirements
 - b. maintaining trust in the dental hygienist and the dental hygiene profession
2. Reduction of harm by the dental hygienist's
 - a. generally increasing the comfort of patients/clients receiving dental hygiene using appropriate techniques of communication
 - b. applying ethical principles and appropriate protection of personal health information
 - c. effective approach to information management as part of practice management.
3. Reduction of risk of oral health needs being unmet.

POTENTIAL HARMS

The dental hygienist undermines the health, safety and well-being of individual patients/clients and their families by failing to

1. provide adequate protection of their personal health information
2. sufficiently respect their privacy-related concerns and sensitivities
3. recognize in the particular circumstances of an individual patient/client a need for medical advice.

DATE OF LAST REVIEW

October 2010

ADVISORY DEVELOPER

College of Dental Hygienists of Ontario, regulatory body

SOURCE(S) OF FUNDING

College of Dental Hygienists of Ontario

ADVISORY COMMITTEE

College of Dental Hygienists of Ontario, Practice Advisors, Executive Committee

COMPOSITION OF GROUP THAT AUTHORED THE ADVISORY

Dr. Gordon Atherley

Mr. Michael Power

ACKNOWLEDGEMENTS

The College of Dental Hygienists of Ontario gratefully acknowledges the Template of Guideline Attributes, on which this advisory is modelled, of The National Guideline Clearinghouse™ (NGC), sponsored by the Agency for Healthcare Research and Quality (AHRQ), U.S. Department of Health and Human Services.

COPYRIGHT STATEMENT

© 2010 College of Dental Hygienists of Ontario