dentalcorp

dentalcorp privacy and protection guide

2021

CANADA'S BEST MANAGED COMPANIES

dentalcorp.ca/resources

Table of Contents

Privacy and data protection – Best practices

The purpose of this document is to provide leaders with strategies and resources to embed privacy and data protection best practices in the day to day operations of the practice.

Clearly and consistently communicate the key messages to the practice team

It is important that you share the Privacy and Data Protection messages and learnings with everyone on the team in a way that is relevant and meaningful. The key messages include:

- Why data protection and privacy are important
  - Legal and regulatory framework
  - Financial and reputational repercussions of breaches
- Key definitions
- Team members' roles in protecting privacy
- The types of privacy risks within dental practices
- Standard control measures for each type of risk
- Notification of and responding to breaches

Refer to **Appendix A: Privacy and data protection – Key messages for practice teams** for more details.

Schedule privacy and data protection huddles

A commitment to protecting privacy goes beyond a one-time training event and we recommend that you routinely incorporate privacy and data protection within team meetings and staff huddles throughout the year.

A recommended strategy is to dedicate ten minutes of a team huddle every quarter to discuss privacy and data protection matters. During the session, focus on a case study with group discussion for an interactive and effective learning experience. When planning the sessions, aim to have all team members present at the same time. If this is not feasible, you may need to use different strategies to share the messages with all staff.

Here is a suggested outline for the sessions:

1	**Our role in protecting privacy** • Case study: Dental practice (or related healthcare example) which failed to protect their patient's privacy • Discussion points: ◦ Repercussions of failing to protect privacy ◦ Roles and responsibilities in protecting privacy
2	**Identifying common privacy risks – Intentional and accidental misuse of data** • Case study: Example of either intentional or accidental misuse of data • Discussion points: ◦ What would you do in this situation? ◦ What could we do in our practice to stop this from happening here? ◦ Have you seen this or something similar happen in our practice? ◦ What other situations do you think could pose similar risk?
3	**Identifying and mitigating common privacy risks – Obtaining consent and using technology safely** • Case study: Example of either failure to obtain consent or failure to use technology safely • Discussion points: ◦ What would you do in this situation? ◦ What could we do in our practice to stop this from happening here? ◦ Have you seen this or something similar happen in our practice? ◦ What other situations do you think could pose similar risk?
4	**Responding to privacy breaches** • Case study: Example of a breach occurring • Discussion points: ◦ If this had happened in our practice, what would we need to do in response? ◦ What do you think the repercussions could be? ◦ How could we make sure that the incident didn't happen again?

Sample case studies are provided in **Appendix B: Examples and discussion points**.

Here are some suggestions for effective facilitation:

1. If the meeting is large, you can make group discussion more manageable by assigning each person one question and ask them to respond and share their thoughts with everyone
2. Use real world events or realistic examples to make the discussion relatable and relevant:
    - Leverage case studies provided in **Appendix B: Examples and discussion points**
    - Identify privacy-related stories in the news related to healthcare or other industries. Be sure to:
        - Create a short summary which sets the scene for the case study
        - Describe the three or four key learnings that the example provides
        - Identify how it relates to the operations in your practice
        - Share the article with everyone afterwards to help reiterate that the scenarios and discussions are not hypothetical
    - dentalcorp provides privacy updates with key learnings for emerging news stories which can be used when appropriate
    - Use examples of near misses from your own practice; be sure this done in a way that does not single out any individuals
3. Avoid tangents and side conversations – keep people on topic by refocusing any tangents and side discussions early

4. Keep out of the weeds – the purpose of the meeting is to share general ideas, not to discuss specific issues or processes in detail; set up offline discussions or working groups if an issue needs more detailed discussion
5. Try to get everyone involved – some people find it easier to contribute to group discussions than others so make sure everyone is encouraged to share their views

Make privacy and data protection a standing discussion item

You can keep privacy and data protection top of mind by embedding discussions as a standing agenda item in any other team meetings you have. Having it set out on the agenda will make discussing privacy and data protection a habit, and provides team members with the opportunity to:

- Discuss any privacy concerns
- Recognize someone who proactively took steps to protect privacy and confidentiality
- Share lessons learned from any recent breaches or near-misses

You can also remind team members about the online learning module and provide an update on how many people have completed it.

Build privacy and data protection into onboarding

Whenever a new team member starts, it is important to make sure that you incorporate privacy and data protection into your onboarding process. You should make sure new hires are aware of:

- Their roles and responsibilities in protecting privacy.
- Any processes or procedures relating to privacy (e.g. privacy consent forms, data access etc.).
- Who to contact in the event of a breach or near-miss.
- Training resources and requirements.

Complete leader checklist

Use the checklist below to ensure you are taking the necessary steps to embed privacy and data protection best practices within your practice:

□ Research relevant federal and provincial regulations.

□ Review and update policies, processes and privacy consent forms to ensure compliance with legislation and best practices.

□ Communicate Privacy & Data Protection training to all team members.

□ Schedule quarterly privacy sessions as part of team huddles.

□ Add privacy and data protection as a standing agenda item for team meetings.

□ Include a privacy and data protection briefing within onboarding programs.

Appendix A: Privacy and data protection – Key messages for practice teams

The importance of privacy and data protection

All Canadians are entitled to privacy, and the assurance that their confidential health information is secure. These rights are protected by law and by health regulators. Together they set out the standards, rules, and regulations that organizations must comply with when they collect, process and share data, including what to do in the event of a breach. If a practice or individual is found liable for not meeting these standards, there can be significant financial and reputational repercussions for the principals and employees of that practice.

Healthcare providers are held to the highest legal standards because of the sensitive nature of Personal Health Information (PHI) that we collect. Regulatory bodies within the healthcare sector set out additional standards for their registrants. Anyone found to not meet these can face financial penalties and a range of professional sanctions.

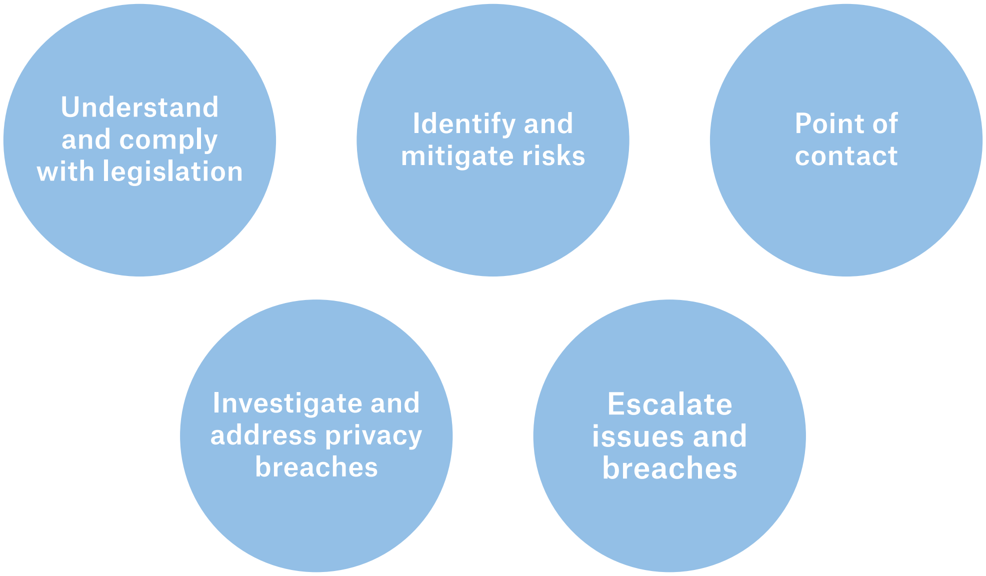
Key definitions

Within privacy and data protection there are five important concepts that apply within a dental practice. They are defined below:

Concept	Definition
Personal Information	Personal Information is data that, on its own or combined with other pieces of data, can identify an individual. This includes contact information, address, date of birth, as well as race, national or ethnic origin, religion, occupation, marital status, personal health numbers, insurance numbers/data, financial information etc.
Privacy	Privacy is an individual's right to control access to their Personal Information.
Confidentiality	Confidentiality is an ethical duty requiring healthcare professionals to "hold in confidence" all information they receive while providing care. Even the fact that someone is a patient is considered confidential information. Confidentiality is also enshrined in Federal and Provincial legislation in every jurisdiction in Canada.
Personal Health Information	Personal Health Information (PHI) is a subset of Personal Information and includes any information about an individual's health. This includes, medical history, diagnoses, treatment plan and any information that is contained with a health record. These are examples only – the complete list of things that qualify as PHI is broader than this.
Business Information	Business information is data that relates to the management and operations of an organization rather than an individual. Business information may include proprietary information, trade secrets, client lists and intellectual property.

Roles and responsibilities

All members of the practice team are responsible for protecting privacy and confidential information belonging to the practice and patients. Ways to protect privacy and confidential information are outlined below.



Understand and comply with legislation

Identify and mitigate risks

Point of contact

Investigate and address privacy breaches

Escalate issues and breaches

The practice should have a named individual who is accountable for ensuring that all team members are aware of and have the necessary resources to meet their responsibilities. This individual is referred to as the information custodian. The information custodian is responsible for responding to patient privacy complaints and, where indicated, escalating issues to the privacy officer. In most cases the information custodian is the Practice Manager.

dentalcorp provides practices with IT infrastructure and a federally-compliant Privacy Officer which provides support and guidance to help Practice Managers identify, manage and mitigate privacy risks.

Understanding and complying with legislation

The **Personal Information Protection and Electronic Documents Act** (PIPEDA) provides the federal framework for protecting privacy. Provinces and territories may have different legislation, or statutes directly related to healthcare, that apply instead of (or in addition to) PIPEDA.

It is important to research the specific requirements within your province or territory. Information relevant to your specific province or territory are provided in **Appendix C: Privacy legislation resources**.

In your research, it is important to identify the requirements for:

- A named contact for privacy inquiries
- Publication of policies
- Notification to be provided to patients about collection and permitted use of personal health information
- Breach notification
- Data collection, storage and destruction
- Complaint policies and processes
- Obtaining and confirming consent for data sharing
- Providing patients access to their records

Identifying and mitigating risks

There are four main categories of privacy risk in dental practices that all team members should be aware of:

- Intentional misuse/illegal access to data
- Inadvertent disclosure by employees
- Failure to obtain required authorization and consent
- IT related risks

Intentional misuse/illegal access to data

Privacy legislation outlines clear parameters for the legitimate collection and use of personal health information and other private data. Some of the more common risks of misuse and unauthorized access are described in the figure below along with mitigating strategies for that risk.

Common risks in this category	Standard control measures
Current employees using their access to “snoop” in patient files they are not directly involved in the provision of care for. Former employees using their previous access to steal or snoop in practice data. Team members removing data from the practice (as physical files or electronic records) increasing the risk of loss or theft. Teams storing patient and practice data on personal mobile devices, which are vulnerable to loss or theft.	Educate the team on the legitimate use and access of patient and practice data. Implement administrative controls so that people only have access to information required to fulfill their responsibilities. Secure areas and systems where data is stored and restrict access as far as possible. Conduct regular access audits to ensure compliance by team. Remove all system access, passes, keys and devices from departing staff. Inform all team members when a member of staff leaves. Never remove data from the practice. Secure mobile devices with screen locks and ensure they are stored safely.

Inadvertent disclosure by employees

Even with standard control measures in place, there is a risk that team members will accidentally cause a privacy breach.

Common risks in this category	Standard control measures
Team members talking about a patient's Personal Information in a public or semi-private place where they could be overheard. Sending patient information to the wrong email, address or fax. Attaching the wrong patient file to an email or transfer. Sending information that is not encrypted and password protected.	Educate the team on the importance of not referring to Personal Information in public settings. If this is not possible, they should lower their voice. If space allows, ensure there is distance between the waiting area and the front desk or a separate space to discuss issues discretely. Where available, use more secure platforms to transfer files to other providers and use encryption software to protect the information. Put in place a process to check the recipients and attachments before sending data.

Failure to obtain required authorization and consent

Legislation requires practices to obtain consent for collection, use and sharing of patient information. Although there is implied consent within the Circle of Care, there are some situations where it is not appropriate to rely on the Circle of Care to share information. Explicit consent is always preferred to implied consent.

Common risks in this category	Standard control measures
Responding to patient comments in a public setting e.g. responding to a negative review online. Sharing information not directly related to the provision of care with another practitioner within the circle of care. Obtaining consent from a parent or partner rather than the patient themselves. Disclosing patient information of a minor to a parent or guardian without explicit consent of the minor to do so. This most often occurs in situations where the parents/guardians live separately or apart and where the patient is not able to provide consent themselves.	Never refer to patient information in a public setting and ensure there is a formal process for responding to complaints. Establish procedures to review any information before it is shared (including with other health care professionals) to check that it does not include details which are not required by the recipient or relate to the Personal Information of another individual. Have clearly defined processes in place for capturing, storing and updating patient consent to share data.

IT-Related risks

Although technology is a key enabler for the delivery of care, the systems we use can introduce additional vulnerability for privacy.

Common risks in this category	Standard control measures
Phishing attempts through calls, emails and messages, especially targeted attempts appearing to be from trusted sources. Suspicious attachments and links. Fraudulent attempts to befriend or contact employees in order to persuade them to share private and confidential information about access to IT systems. Out-of-date virus protection or software which is not equipped to defend systems against evolving threats. Weak, repeated, shared or publicly displayed passwords. Accessing systems from shared or remote locations. Using third-party messaging platforms to discuss patient information.	Be vigilant and cautious about any interaction that relates to system access or unsolicited offers of help. Train frequently on this and provide reminders and resources on social engineering, phishing and malware trends. Validate any interactions relating to technology or access with IT using verified contact details. Regularly update virus protection. Use unique passwords that are at least 12 characters long and updated at least once a year. If accessing systems remotely or from shared locations (which should be avoided wherever possible), ensure that the Wi-Fi connection is secure, and that you have logged out and cleared browser history when you are finished. If you are working remotely from home, ensure your router admin password is not the "default" password, is complex and has been changed at least once every 6 months. Ensure your Wi-Fi password is likewise secure and do not share your device with anyone else in your household. If that is not possible, ensure that you have separate secure log-ons to your device which restricts file/folder access. Avoid referring to identifiable patient information on third-party messaging platforms.

Notification of and responding to breaches

Even with control measures in place, not all risks can be avoided; therefore, it is important that practice teams are aware of the steps that should be taken when a breach is identified. At a minimum:

1. Notify dentalcorp's Privacy Officer. The Privacy Officer will provide guidance and determine whether the impacted individual and any other external parties (such as the Privacy Commissioner) need to be notified.
2. Where technology is involved, notify the IT Department.

No two data breaches are the same. Depending on circumstances, additional steps may need to be taken. The Privacy Officer, Compliance team and IT Department will assist you if this is the case.

Appendix B: Examples and discussion points

Here are some case studies you can use to generate discussion as part of your huddles. In each case, the type of risk and its relevancy to the topic is highlighted.

Example:	Former employee uses previous access to view patient data
Category:	Intentional misuse/illegal access to data
Relevant session(s):	1: Our role in protecting privacy 2: Identifying common privacy risks – Intentional and accidental misuse of data 4: Responding to privacy breaches

Introduction: A Dental Hygienist was asked to leave the practice following repeated behavioural issues. The Practice Manager collected her devices and an access key. However, there was no process in place to record how many keys everyone had, so the Practice Manager did not realize that the Hygienist also had another key. The Dental Hygienist used the key to enter the practice before it opened. She went into the records room and photographed several patient files and confidential business documents. Another colleague was also there early and saw her take photos. They thought her behaviour was suspicious but didn't say anything as they did not realize she was no longer employed by the practice. The breach was identified when the former Dental Hygienist posted the images online to damage the practice's reputation.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- What do you think the repercussions for the practice are likely to be in this situation?
  - Financial impacts: If the Privacy Commissioner finds that the practice's process was insufficient,they may impose financial penalties on the practice. The practice could also have to pay damages to the impacted individuals
  - Reputational: The incident could lead to media coverage, which will impact the practice's reputation as a provider of excellent and confidential healthcare
- What are the roles and responsibilities of the practice team to ensure the incident is not repeated?
  - Practice Manager is responsible for ensuring that all access keys are collected from departing employees and that all staff are informed when a team member leaves
  - All team members should be vigilant and report suspicions or issues to the Practice Manager
- What could the practice have done differently to prevent this incident?
  - Ensure a thorough process is in place for restricting the access of all departing staff
  - Inform all team members when a member of staff leaves so everyone is aware that they should no longer be in the practice unaccompanied
  - All team members should report anything suspicious to the Practice Manager
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- What other situations do you think could pose similar risk?
  - Unaccompanied patients or visitors who may try and access secure areas within the practice
  - Current team members who use their access to snoop on private and confidential information
- Do you think we have the correct control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- If this had happened in our practice, what steps would we need to take in response?
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
  - Report the offending post and get it taken down as quickly as possible

Example:	Current employee using access to view data of patients not in their care
Category:	Intentional misuse/illegal access to data
Relevant session(s):	1: Our role in protecting privacy 2: Identifying common privacy risks – Intentional and accidental misuse of data 4: Responding to privacy breaches

Introduction: A Dentist becomes aware that her ex-husband's new partner is a patient at the practice. She is curious to know more about the new spouse, so she logs onto the system to browse their record and notes. She recognizes the information is confidential, so she briefly looks over the information with no intention of sharing it with anyone.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- Does the Dentist reviewing her ex-husband's new partner's records represent a privacy breach? If so, why?
  - Yes, it is a privacy breach
  - It is a common misconception that as a healthcare professional you have authorization to view any patient file as long as you keep the information confidential
  - You only have authorization to review the information of patients who are in your care and for legitimate purposes related to providing healthcare
- What could the practice have done differently to prevent this incident?
  - Ensure that everyone in the team is clear on what data they should and should not be accessing
  - Carry out access audits to ensure that all staff use their access appropriately
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- What other situations do you think could pose similar risk?
  - Members of the team snooping with the intention of using the information for nefarious purposes (example: **https://www.cbc.ca/news/canada/toronto/personal-data-of-8-300-new-moms-sold-to-financial-firm-in-hospital-security-breach-1.2665503**)
  - Members of the team snooping and using the information for personal gain
- If this had happened in our practice, what steps would we need to take in response?
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
- What do you think the repercussions could be?
  - As this is an isolated incident, it is unlikely the Privacy Officer would recommend notifying the Privacy Commissioner or the Dentist's regulator
  - Patterns of such behaviour, on the other hand, could trigger mandatory breach notification obligations
  - Potential reputational impact if the breach is discovered

Example:	A team member sends a patient file to the wrong recipient
Category:	Inadvertent disclosure by employees
Relevant session(s):	2: Identifying common privacy risks – Intentional and accidental misuse of data 4: Responding to privacy breaches

Introduction: A Dentist is sending a patient file to another provider. Their phone rings and they take the call while completing the task and click send before checking the details. Later that day, they review the email and realize they sent an incorrect file for a patient with a similar name to the new provider.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- What could the practice have done differently to prevent this incident?
  - Where available, use more secure platforms to transfer files to other providers
  - Where available, use encryption software to protect the information before sending it
  - Put in place a process to check the recipients and attachments before sending data via email
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- What other situations do you think could pose similar risk?
  - Posting or faxing files to other providers or patients
  - Not reviewing files ahead of sending and inadvertently sharing information that is not required by the recipient or including information about another individual within the same file
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support contact Compliance
- If this had happened in our practice, what steps would we need to take in response?
  - Immediately reach out to the unintended recipient and ask them to delete the information without viewing it
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
- What do you think the repercussions could be?
  - As this is an isolated incident, it is unlikely the Privacy Officer would recommend notifying the Privacy Commissioner or the Dentist's regulator
  - Potential reputational impact

Example:	A team member leaves identifiable information somewhere it could be viewed by another patient
Category:	Inadvertent disclosure by employees
Relevant session(s):	2: Identifying common privacy risks – Intentional and accidental misuse of data 4: Responding to privacy breaches

Introduction: A Dental Hygienist has a busy day with back-to-back patients. During his last appointment he needs to ask a colleague a question and leaves a patient unattended in the operatory. On his desk he has left out his notes from the previous patients, which outline the patients' names, dates of birth, medical history and dental hygiene diagnosis. When he returns to the operatory, he sees that the patient is looking at the notes.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- What could the practice have done differently to prevent this incident?
  - Have a clear desk policy so that information and notes are not left unsecured in rooms
  - Use anonymous patient identifiers instead of patient names so if the information is left where someone else could see it, it is not identifiable and, therefore, not personal data
  - Never leave a patient's records unattended in an unsecure area
- What other situations do you think could pose similar risk?
  - Not logging out of systems or leaving computer screens on with identifiable patient information where someone else can see them
  - Showing a patient something on a device with another patient's information still displayed
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support contact Compliance
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support contact Compliance
- If this had happened in our practice, what steps would we need to take in response?
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
- What do you think the repercussions could be?
  - As this is an isolated incident, it is unlikely the Privacy Officer would recommend notifying the Privacy Commissioner or the Dental Hygienist's regulator
  - Potential reputational impact

Example:	Talking about a patient with another healthcare provider
Category:	Failure to obtain required authorization and consent
Relevant session(s):	3: Identifying common privacy risks – Obtaining consent and using technology safely 4: Responding to privacy breaches

Introduction: A Dentist is referring one of their patients to another provider. She calls the new provider to discuss the requirements and relevant context. They begin discussing the individual's insurance coverage and ability to afford the treatment. The Dentist tells the new provider that the patient has recently undergone a long divorce and are paying a large sum of money in the settlement. They are still able to afford the treatment, but they thought the new provider would be interested to know. The fact that the patient's ex was unfaithful is also mentioned.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- Is the Dentist sharing information about their patient's divorce with the new provider a privacy breach? If so, why?
  - Yes, it is a privacy breach
  - Although there is implied consent to share Personal Information within the circle of care, this only applies to information directly related to the provision of care
  - The patient's recent divorce and ex-spouse's infidelity are not relevant and, therefore, should not have been shared
- What could the practice have done differently to prevent this incident?
  - Ensure that everyone in the team was clear on what information they should and should not be sharing within the circle of care
  - Get explicit consent to share any information that not clearly relevant to the ability of the new provider to meet the patient's healthcare needs
  - Do not share such information without explicit consent or at all
- What other situations do you think could pose similar risk?
  - Discussing patient care with a colleague somewhere you could be overheard
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- If this had happened in our practice, what steps would we need to take in response?
  - Review the rules around patient privacy with all team members
  - Ensure the concept of the Circle of Care is clearly understood by all clinicians
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
- What do you think the repercussions could be?
  - As this is an isolated incident, it is unlikely the Privacy Officer would recommend notifying the Privacy Commissioner or the Dentist's regulator
  - Potential reputational impact

Example:	Talking about a patient with another healthcare provider
Category:	Failure to obtain required authorization and consent
Relevant session(s):	3: Identifying common privacy risks – Obtaining consent and using technology safely 4: Responding to privacy breaches

Introduction: A member of the administrative team was collecting consent from a new patient at the practice. They were 16 years old and, when they first attended, their parent completed the privacy consent form for the collection and use of their data. When the minor attended their next appointment, they asked to withdraw their consent to share medical history information with their parents. The team member made a note but did not update the records. One of the minor's parents then requested to see the information and, because the system recorded that consent had been given, the information was disclosed.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- Is this disclosure to the minor patient's parent a privacy breach? If so, why?
  - Yes, it is a privacy breach
  - Minors who are "capable" can disagree with a decision made by their parents about the collection, use or disclosure of their PHI
  - In this case, it is the minor's choice that matters – not that of their custodial parents
  - The team should have updated the consent record and the files should not have been shared with the non-custodial parent
- What could the practice have done differently to prevent this incident?
  - Ensuring that everyone on the team is aware of how privacy legislation relates to minors
  - Ensuring there are clear processes and procedures in place to capture, store and update consent for data sharing
- What other situations do you think could pose similar risk?
  - Including one parent's Personal Information when sharing a minor's records with another parent. This is particularly problematic when the parents are divorced or separated
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- If this had happened in our practice, what steps would we need to take in response?
  - Inform the parent whose information was inadvertently shared and apologize
  - Contact the parent who received the information in error and ask them to destroy the documents without viewing them
  - Contact dentalcorp's Privacy Officer for advice and guidance on the investigation and next steps
- What do you think the repercussions could be?
  - The parent whose privacy was breach is likely to be very upset and may file a complaint
  - As this is an isolated incident, it is unlikely the Privacy Officer would recommend notifying the Privacy Commissioner or the Dentist's regulator
  - Potential reputational impact

Example:	Social engineering
Category:	IT-related risks
Relevant session(s):	3: Identifying common privacy risks – Obtaining consent and using technology safely 4: Responding to privacy breaches

Introduction: A member of the practice team receives an email that appears to be from the Practice Manager. It says the Practice Manager needs urgent support to complete a task and asks the team member to video call them using an enclosed link.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- What would you do in this scenario?
  - Check the email thoroughly for any signs it is not genuine, such as spelling errors or differences in the Practice Manager’s email address and signature
  - Consider whether the email is consistent with the type of communication the Practice Manager usually sends (i.e. are video calls out of character?)
  - Contact the Practice Manager separately, using verified contact details, to ask whether the email is genuine
- What other situations do you think could pose similar risk?
  - Targeted attempts such as this can occur over telephone or text message as well
  - Weak or publicly displayed passwords which mean systems can easily be hacked
  - Out-of-date virus protection which is not able to identify or remove IT risks
- Have you seen this or something similar happen in our practice?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- If the team member had clicked on the link, what steps should they follow?
  - Immediately contact the IT Department who will be able to provide guidance on steps to follow
  - Although it can be tempting, you should not turn off your computer or delete the email without consulting with the IT Department first
- What do you think the repercussions could be?
  - The link may give fraudulent individuals access to the practice’s systems and data which could lead to data being stolen.
  - If data is stolen, it may be necessary to report the privacy breach to the authorities

Example:	Ransomware attack
Category:	IT-related risks
Relevant session(s):	3: Identifying common privacy risks – Obtaining consent and using technology safely 4: Responding to privacy breaches

Introduction: A Practice Manager arrives at the practice in the morning and, when they try to log on, they get a message saying that their system has been hacked and that the practice's data has been stolen. The data will be returned if the practice pays a large ransom.

Discussion questions and points to highlight (select 3 or 4 which are relevant to the topic of the session):

- What would you do in this scenario?
  - Contact the IT Department immediately
  - You should not turn off the computer or disconnect it from the network without consulting IT as, in some cases, this can make the situation worse
- What steps do you think we can take to prevent this from happening at our practice?
  - Ensuring that we only use third-party platforms that have been procured and vetted for security by the IT Department
  - Being vigilant to IT threats to help protect systems
  - Regularly backing up data so it is not lost in the event of an attack
- Do you think we have all the control measures in place to prevent this from happening here?
  - If anything is raised here, make sure you capture it and consider whether any further action should be taken; if you need support, contact Compliance
- What do you think the repercussions could be?
  - Practice unable to provide care as cannot access patient records (Example: **CNN Ransomware Attack on Dental Offices**)
  - Impacted individuals may bring a class action suit which, if the practice cannot prove that they took all reasonable steps to protect the data
  - Such an event could have significant financial and reputational impacts
  - If the data was in fact viewed or accessed by the cyber criminals, the matter may have to be reported to the authorities

Appendix C: Privacy legislation resources

Jurisdiction	Legislation	Resources	Regulator Requirement/ Guidance Resources	Summary of Dental Regulations	Summary of Dental Hygiene Regulations
Federal	PIPEDA - Personal Information Protection and Electronic Documents Act	Office of Privacy Commissioner of Canada			
	Privacy Act	OIPC - Overview of Privacy Laws and Oversight across Canada			
Alberta	PIPA - Personal Information Protection Act	Alberta Health Services Guides to HIA and FOIP	ADA&C Standard of Practice - Privacy and Management of Patient Health Information	Registered members of the Alberta Dental Association and College are governed by applicable privacy legislation including Alberta's Health Information Act (HIA)	CRDHA - Practice Standards - Page 11 Documentation and Recordkeeping
	FOIPA Alberta	OIPC Alberta Guidance	Code of Ethics - Article A7 - deals with patient confidentiality		
	HIA - Health Information Act	OIPA Alberta Legislative Overview/Resources	ADA&C - Guide for HIA - Privacy and Management of Patient Health Information		
	HIA - Electronic Health Record Regulation		ADA&C Guide for Patient Records and Informed Consent		

Jurisdiction	Legislation	Resources	Regulator Requirement/ Guidance Resources	Summary of Dental Regulations	Summary of Dental Hygiene Regulations
British Columbia	**Freedom of Information and Protection of Privacy Act FIPA_BC**	OIPC Office	BC Dental Recordkeeping Guidelines	Dentists need to be aware of the requirements of the Personal Information Protection Act of British Columbia (PIPA) and other laws dealing with privacy such as the OIPC	CDHBC - Code of Ethics - Part 3 Confidentiality
	Personal Information Privacy Act	Doctors of BC Privacy Toolkit	Code of Ethics - Principle 13 - Protect confidentiality and personal health information		
	E-Health (Personal Health Information Access and Protection of Privacy Act)				
	Privacy Act				
Manitoba	Freedom of Information and Protection of Privacy Act - PIPPA	Office of the Ombudsman	Website has very little publicly accessible information	For dentists in Manitoba, each dental office will have a privacy officer. The privacy officer's main role is to ensure that all aspects of PIPEDA are adhered to within their dental office	Resources are behind a member login
	Personal Health Information Act - PHIA		Code of Ethics - Article 7 - Deals with Confidentiality and Release of Patient Information		
			Privacy Information for Patients		

Jurisdiction	Legislation	Resources	Regulator Requirement/ Guidance Resources	Summary of Dental Regulations	Summary of Dental Hygiene Regulations
New Brunswick	Personal Health Information Privacy and Access Act - PHIPA	Ombudsman Office	Website has no public facing information	The Government of NB and the Government of Canada have established standards in relations with the protection of personal health records of clients. New Brunswick Dentists are "custodians" of confidential personal health information and have legal obligations pursuant to the Personal Health Information Privacy and Access Act (PHIPAA)	The NB College of Dental Hygienists recommends that dental hygienists abide by the recommendation included in the PHIPAA and the PIPEDA concerning personal health information of their clients Standards of Practice
	Right to Information and Protection of Privacy Act	Ombudsman office - Guide to Personal Health Information Privacy and Access			
		Ombudsman Office - Resource Page on Right to Information and Protection of Privacy			

Jurisdiction	Legislation	Resources	Regulator Requirement/ Guidance Resources	Summary of Dental Regulations	Summary of Dental Hygiene Regulations
Newfoundland and Labrador	Access to Information and Protection of Privacy Act	OIPC Newfoundland and Labrador - Main resource page		Same as Nova Scotia, need to be aware of the requirements of PHIA	NLCHP - Privacy, Confidentiality and Consent
			Standards of Practice require confidentiality		
	Personal Health Information Act	OIPC Newfoundland and Labrador - Health Custodian Resources			
	Act respecting Access to Documents Held by Public Bodies and Protection of Personal Information		Guide to Using a Computer System for Keeping Patient Records		

	Three related Acts which in combination deal with health information –
	(1) Amending Legislation;
	(2) Health Insurance Act;
	(3) Oversight of Health Insurance and Related
			Code of Ethics - Section 6 - Professional Secrecy		

Jurisdiction	Legislation	Resources	Regulator Requirement/ Guidance Resources	Summary of Dental Regulations	Summary of Dental Hygiene Regulations
Nova Scotia	Freedom of Information and Protection of Privacy Act - FOIPA	OIPC Nova Scotia - Tools for Health Custodians	Code of Ethics - Article 9 - Requires information to be kept confidential	All dentists in Nova Scotia must comply with the requirements of PHIA regarding patient information and dental records, including the disclosure and transfer of patient information and dental records	CDHNS - Recordkeeping, pg. 7 & C
	Personal Health Information Act - PHIA_NS		Record Keeping Guidelines		
	Personal Information International Disclosure Protection Act				
Saskatchewan	Freedom of Information and Protection of Privacy Act - FOIPA	OIPC Saskatchewan	Website has almost no public facing information	Members of the College of Dental Surgeons of Saskatchewan are governed by the Health Information Protection Act (HIPA) and other laws dealing with privacy such as OIPC	References to https://www.oipc.bc.ca/
	Local Authority FOIPA - LAFOIP	OIPC - Guide to FOIPA	CDSS - Retention of Records		
	Health Information Protection Act - HIPA	OIPC Guide to LA - FOIPA			
		Ombudsman Office - Resource Page on Right to Information and Protection of Privacy			