



Ordre des
denturologistes
du Québec

**GUIDE PRATIQUE D'UTILISATION D'UN SUPPORT INFORMATIQUE
POUR LA TENUE DES DOSSIERS PATIENTS**
(Règlement sur la tenue des dossiers et des cabinets
de consultation des denturologistes, articles 1.04. et 2.08.)

Septembre 2016

TABLE DES MATIÈRES

PRÉFACE.....	3
INTRODUCTION	4
1. TENUE DE DOSSIERS.....	6
2. SÉCURITÉ ET CONFIDENTIALITÉ DES INFORMATIONS.....	8
2.1 Code d'utilisateur et mot de passe	8
2.2 Limitation d'accès aux données confidentielles ou sensibles	8
2.3 Sauvegarde et restauration des données.....	8
2.4 Archivage des données	9
2.5 Impression de rapports et de dossiers patients.....	9
3. AUTHENTIFICATION ET POSSIBILITÉ DE RETRACER LES INFORMATIONS SAISIÉS	10
3.1 Inaltérabilité des informations et des documents joints	10
3.2 Le transfert d'un dossier patient informatisé	10
3.3 Disposition des matériels informatiques et logiciels	11
ANNEXE 1	12
ANNEXE 2.....	16

PRÉFACE

Depuis plusieurs années, beaucoup de cabinets de professionnel utilisent les « solution informatique » dans leur pratique de tous les jours.

A la suite de plusieurs demandes, nous avons cru bon de mettre sur papier les grandes lignes auxquelles un denturologiste pourrait se référer afin de se guider sur la « solution informatique » adéquate pour ses besoins.

Le *Règlement sur la tenue des dossiers et des cabinets de consultation des denturologistes* est clair :

« **1.04.** Rien dans le présent règlement ne doit être interprété comme excluant l'utilisation de l'informatique ou de toute autre technique pour la constitution et la tenue des dossiers d'un denturologiste. »

R.R.Q., 1981, c. D-4, r. 11, a. 1.04.

Ainsi que,

« **2.08.** Lorsque le denturologiste utilise l'informatique ou toute autre technique pour la constitution et la tenue de ses dossiers, il doit s'assurer que leur confidentialité soit respectée. »

D. 67-92, a. 2.

Alors que la principale mission de l'Ordre de denturologistes du Québec est de protéger le public, il est alors essentiel de s'assurer que confidentialité des renseignements que peuvent contenir un dossier patient détenu par un denturologiste soit sans faille.

Plusieurs règlements et normes énoncent déjà les pratiques de la denturologie, l'utilisation d'une « solution informatique » ne devrait pas changer les obligations du denturologiste.

À l'ère où nous vivons, l'informatique est omniprésente et les informations sur son utilisation sont déclinées partout sur le web, tant au point de vue de la sécurité que de ses avantages et sa facilité d'utilisation. Malgré ce fait, avons-nous réellement conscience de tout le danger qui nous guette?

Ce guide se veut un outil pour ceux et celles qui veulent s'orienter vers une « solution informatique » en les aidant à faire de bons choix, et ce, dans le respect des lois et règlements ainsi que des règles sur le secret professionnel.

Pour ces raisons, lorsque le denturologiste fait ce choix, plusieurs lectures devraient au préalable être faites, entre autres le document de référence *Guide des TI¹* du Barreau du Québec que vous pouvez consulter au <http://guideti.barreau.qc.ca>.

D'ailleurs, dans le but de vous aider à valider votre compréhension et l'application de ce guide, nous avons reproduit un petit questionnaire du Barreau du Québec qui vous est suggéré à l'annexe 2.

¹ Il est préférable de se référer à la version Web de ce document compte tenu des modifications qui pourraient lui être apportées lors de mise à jour.

INTRODUCTION

Étant donné que nous n'avons pas tous la même expertise, voire la même expérience dans l'utilisation de l'informatique, nous sommes d'avis que nous devrions parler de « solution informatique » et qu'elle s'inscrit dans une solution globale et complète, dont :

- ordinateur;
- logiciels;
- imprimante
- numériseur (pour les formulaires et signatures);
- système de sauvegarde (local ou en ligne);
- Internet (communication);
- graveur numérique (CD, DVD);
- mise à jour (logiciels et matériel);
- support informatique (technicien);
- caméras numériques;
- système de batterie de secours (UPS);
- ...

Selon le *Code de déontologie* :

« **40.1.** Le denturologiste doit prendre les moyens raisonnables pour faire respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession par toute personne qui coopère ou collabore avec lui ou exerce ses activités au sein de la société où il exerce ses activités professionnelles. »

D. 686-2008, a. 15.

Le *Code des professions* du Québec dit aussi :

« **60.4.** Le professionnel doit respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession.

Il ne peut être relevé du secret professionnel qu'avec l'autorisation de son client ou lorsque la loi l'ordonne ou l'autorise par une disposition expresse. [...] »

1994, c. 40, a. 51; 2001, c. 78, a. 5; 2008, c. 11, a. 33.

La *Loi sur la protection des renseignements personnels dans le secteur privé* (chapitre P-39.1) nous rappelle aussi certaines obligations que nous devons respecter.

Principalement aux articles 8 et 14 :

« **8.** La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer:

1° de l'objet du dossier;

2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;

3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification. »

1993, c. 17, a. 8.

« **14.** Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Un consentement qui n'est pas donné conformément au premier alinéa est sans effet. »

1993, c. 17, a. 14; 2006, c. 22, a. 115.

Ces moyens raisonnables doivent, entre autres, s'étendre aux équipements, aux systèmes et logiciels que le denturologiste et que les membres de son équipe utilisent.

Cet énoncé nous questionne sur le contrôle et la vigilance que le denturologiste doit faire preuve lors de l'utilisation des différents services informatiques, entre autres : hébergement des données, technicien informatique, accès Internet, etc.

Les données du dossier patient, si elles sont hébergées à l'extérieur des équipements de la clinique, devront demeurer au Canada pour être assujetties aux lois canadiennes, et ce, afin de respecter et préserver la confidentialité des documents qui y sont hébergés.

Il s'avère alors nécessaire de vérifier auprès de ses fournisseurs les ententes de services informatiques afin de prévoir les droits d'accès en tout temps et de propriété ainsi que la disposition des données par le fournisseur advenant la fin de l'entente, de la faillite du fournisseur ou toutes autres raisons. Le fournisseur ne doit avoir aucun droit de rétention des données.

Faut-il se rappeler que seuls les patients sous la responsabilité du denturologiste demeurent propriétaires des données contenues dans leur dossier patient, peu importe où sont stockées les données.

Il est alors important de bien comprendre et connaître les termes du contrat avec un fournisseur de services informatiques

Le *Guide des TP*² du Barreau du Québec traite bien de ce sujet à la SECTION 2 - Protection de l'accès aux données et plus particulièrement au chapitre sur l'entente avec les fournisseurs.

On comprendra alors qu'il est de la responsabilité du denturologiste de se conformer à son devoir envers la protection des renseignements privés de ses patients.

² Il est préférable de se référer à la version Web de ce document compte tenu des modifications qui pourraient lui être apportées lors de mise à jour.

1. TENUE DE DOSSIERS

Il appartient au denturologiste qui souhaite informatiser sa tenue de dossiers de s'assurer que la « solution informatique » qu'il utilise **réponde en totalité** aux différents règlements, lois et normes de l'Ordre des denturologistes du Québec (ODQ) et qu'elle puisse s'adapter et évoluer à tout changement que l'ODQ pourrait leur apporter éventuellement.

Les règles pour la tenue de dossiers sont les mêmes quel que soit le support utilisé.

De plus, le denturologiste doit s'acquérir les connaissances et compétences pour lui et son équipe dans l'utilisation de la « solution informatique » (annexe 2 – 24 questions pour évaluer votre utilisation des technologies de l'information).

Le denturologiste doit s'assurer que les fournisseurs avec lesquels il traite, et qui offrent des logiciels de tenue de dossiers ou de facturation auprès des différentes compagnies d'assurances, fournissent du matériel remplissant les exigences suivantes :

- sécurité et confidentialité des informations;
- limitation d'accès aux données confidentielles ou sensibles;
- sauvegarde et restauration des données;
- archivage des données;
- impression de rapports et de dossiers patients;
- authentification et possibilité de retracer les informations saisies;
- inaltérabilité des informations et des documents joints;
- enregistre et trace toutes les informations sur les modifications apportées aux données (log file);
- transfert d'un dossier patient informatisé;
- capacité de saisir la signature du patient et du denturologiste;
- afin d'enregistrer de façon structurée et par ordre chronologique les obligations de l'article 2.02. du règlement sur la tenue de dossiers (voir annexe 1), soit :
 - a) *la date d'ouverture du dossier;*
 - b) *le nom du client, son adresse, son numéro de téléphone, sa date de naissance et son sexe;*
 - c) *une description sommaire des motifs de la consultation;*
 - d) *une description des services professionnels rendus et leur date;*
 - e) *une description de la prothèse dentaire amovible fournie ou vendue, s'il y a lieu;*
 - f) *les recommandations faites au client;*
 - g) *les annotations, la correspondance et les autres documents relatifs aux services professionnels rendus; et*
 - h) *la signature du denturologiste qui a rendu les services professionnels;*
 - i) *le plan de traitement suggéré par le denturologiste et agréé par ce dernier et par le client;*
 - j) *l'information exigée par l'article 7 de la Loi sur la denturologie (chapitre D-4) consignée sur une formule analogue à celle apparaissant à l'annexe I.*

Le denturologiste devra aussi, entre autres, s'assurer :

- de la disposition sécuritaire du matériel informatique et des logiciels.

Il sera de la responsabilité du denturologiste de s'assurer que les exigences de l'ODQ soient remplies lors de ses négociations pour l'achat d'une telle solution.

Lors des visites d'inspections, l'inspecteur vérifiera que ces directives sont suivies et respectées.

Après l'implantation d'une solution informatique, il est probable que le denturologiste veuille archiver les dossiers papier d'anciens patients. Ceux-ci devraient être gardés pour une période minimale de cinq ans.

Selon le *Règlement sur la tenue des dossiers et des cabinets de consultation des denturologistes* :

« **2.04.** Un denturologiste doit conserver chaque dossier pendant au moins 5 ans à compter de la date du dernier service rendu ».

R.R.Q., 1981, c. D-4, r. 11, a. 2.04.

Le denturologiste doit consigner toutes les modifications qu'il apporte à un élément du dossier.

Il est important de recueillir au dossier patient toutes les informations qui sont en lien direct avec les actes posés et d'être prudent avec celles jugées non pertinentes afin de respecter et protéger les renseignements personnels de nos patients.

Le patient a en tout temps la possibilité de consulter son dossier et de demander le retrait de certains renseignements personnels, s'il le désire.

2. SÉCURITÉ ET CONFIDENTIALITÉ DES INFORMATIONS

Des règles de fonctionnement doivent être définies par le denturologiste quant à l'utilisation d'une « solution informatique » et surtout lorsqu'il y a plusieurs personnes qui utilisent cette solution. L'aide d'un technicien en informatique pourrait être essentielle afin de supporter le denturologiste.

Pour des fins d'efficacité, de support ou autre, un « administrateur du système » peut être désigné par le denturologiste. Le denturologiste demeurera toujours responsable de l'administrateur du système pour toute action ou intervention posée par ce dernier.

2.1 Code d'utilisateur et mot de passe

Il est de la responsabilité de l'administrateur du système de s'assurer que :

- chaque personne autorisée possède son propre code d'utilisateur;
- le code d'utilisateur est protégé par un mot de passe secret et unique à chaque usager;
- l'administrateur du système pourrait exiger que le logiciel demande à l'utilisateur de changer fréquemment son mot de passe;
- le mot de passe n'est pas lisible à l'écran;
- en cas de départ ou absence d'un usager, son code ne devrait pas être assigné à une autre personne afin de s'assurer de l'identité de la personne qui apporte des modifications au dossier;
- les données ne soient pas effaçables ni altérables sans laisser de traces.

2.2 Limitation d'accès aux données confidentielles ou sensibles

L'administrateur du système doit désigner les personnes qui ont l'autorisation d'accéder au dossier et sur quelles parties celles-ci ont accès dans le cadre de leurs fonctions, que ce soit simplement le pouvoir de consulter, de modifier ou d'ajouter des informations à un dossier.

2.3 Sauvegarde et restauration des données

Il est essentiel pour une sécurité maximale de la « solution informatique » qu'une procédure soit mise en place afin de sauvegarder les données, et ce, à tous les jours.

La copie de sauvegarde, de préférence incrémentale, doit être gardée en autre lieu que celui du système afin d'éviter le vol ou la destruction des systèmes par le feu ou autres bris.

Il existe plusieurs solutions et programmes de sauvegarde disponibles sur le marché, mais la solution ou le programme choisi pourrait aussi être fourni et intégré directement dans le logiciel de tenue de dossiers.

La « solution informatique » devra permettre la restauration des données rapidement et facilement en cas de problèmes.

2.4 Archivage des données

L'archivage permet de réduire les dossiers patients qui deviendraient volumineux ou lors de la fermeture d'un dossier, tout en conservant les informations.

Il est important de conserver les informations, même celles archivées, pour une période de cinq ans après sa dernière information consignée, comme le prévoit notre réglementation.

2.5 Impression de rapports et de dossiers patients

Le logiciel doit permettre d'imprimer un dossier patient complet et lisible, comprenant tous les éléments versés au dossier.

Il doit permettre aussi d'imprimer des rapports sur les inscriptions, les modifications ou la suppression de données et documents numériques.

Le logiciel restreint la production et l'impression de rapports aux utilisateurs autorisés.

3. AUTHENTIFICATION ET POSSIBILITÉ DE RETRACER LES INFORMATIONS SAISIES

L'administrateur du système doit s'assurer que le logiciel qu'il utilise :

- enregistre les informations relatives à l'utilisateur pour toute modification de données (saisie initiale, modification ou suppression);
- enregistre les informations relatives à la date et à l'heure de toute modification de données;
- enregistre les informations relatives à la nature exacte des modifications apportées aux données;
- permet de visualiser, de façon chronologique, l'historique complet des transactions effectuées dans un dossier;
- conserve l'original de tous les radiographies/photos et documents numérisés relatifs à un dossier;
- permet seulement au denturologiste ayant effectué un traitement de supprimer ou de modifier les informations relatives à ce traitement;
- ne permet pas à un utilisateur de changer la date et l'heure du système.

3.1 Inaltérabilité des informations et des documents joints

L'administrateur du système doit s'assurer que le logiciel qu'il utilise :

- permet de crypter les données relatives aux dossiers patients;
- permet de crypter les radiographies/photos et les documents numérisés;
- bloque l'accès à toute personne n'ayant pas les autorisations d'usage au système;
- enregistre et trace toutes les informations sur les modifications apportées aux données (log file).

3.2 Le transfert d'un dossier patient informatisé

Dans le cas où le denturologiste voudrait transférer ses dossiers à la suite de la vente de sa pratique ou de son départ de la clinique pour une autre, ou la cession de ses dossiers à un autre denturologiste, dû à son décès ou à sa radiation, et ce, soit à la demande d'un patient ou du syndic de l'ODQ, ou de toute personne autorisée à faire cette demande, l'administrateur du système doit s'assurer que le logiciel qu'il utilise :

- permet d'exporter et d'importer des données du dossier patient de façon encryptée :
 - pour un patient en particulier (dossier complet);
 - pour un patient en particulier, en incluant seulement l'information;
 - sur les traitements dispensés par un denturologiste en particulier (dossier partiel);
 - pour un patient, en incluant tous les dossiers le concernant;
 - pour tous les patients traités par un denturologiste en particulier;

- crée une copie lisible par un autre système informatique;
- s'assure que le système informatique a les équipements nécessaires pour permettre de transmettre rapidement les données, soit par Internet de façon sécuritaire ou de graver sur un CD les données à transférer.

3.3 Disposition des matériels informatiques et logiciels

Lors du remplacement d'une partie ou de l'ensemble de son système informatique, le denturologiste doit s'assurer que toutes les données confidentielles contenues dans son système soient totalement détruites selon les normes reconnues, soit :

- par un reformatage du disque dur ou l'exécution d'un script en plusieurs passes conforme à la norme canadienne CSEC ITSEG-06; ou
- par la destruction physique des composantes par déchiquetage.

N.B. Veuillez noter que ce guide pourrait faire l'objet d'une éventuelle révision.



chapitre D-4, r. 15

Règlement sur la tenue des dossiers et des cabinets de consultation des denturologistes

Loi sur la denturologie

(chapitre D-4, a. 3)

Code des professions

(chapitre C-26, a. 91)

SECTION I

DISPOSITIONS GÉNÉRALES

1.01. Le présent règlement est adopté en vertu de l'article 91 du Code des professions (chapitre C-26).

R.R.Q., 1981, c. D-4, r. 11, a. 1.01.

1.02. Dans le présent règlement, à moins que le contexte n'indique un sens différent, les mots suivants signifient:

- a) «Ordre»: l'Ordre des denturologistes du Québec;
- b) «denturologiste»: quiconque est inscrit au tableau de l'Ordre;
- c) «cabinet de consultation»: le lieu où un denturologiste dispense des services professionnels, à l'exclusion notamment du lieu mentionné à l'article 3.02 et de la salle de travail des employés de ce denturologiste.

R.R.Q., 1981, c. D-4, r. 11, a. 1.02.

1.03. La Loi d'interprétation (chapitre I-16) s'applique au présent règlement.

R.R.Q., 1981, c. D-4, r. 11, a. 1.03.

1.04. Rien dans le présent règlement ne doit être interprété comme excluant l'utilisation de l'informatique ou de toute autre technique pour la constitution et la tenue des dossiers d'un denturologiste.

R.R.Q., 1981, c. D-4, r. 11, a. 1.04.

1.05. La section III ne s'applique qu'au cabinet de consultation où un denturologiste exerce à son propre compte ou pour le compte d'un denturologiste ou d'une société de denturologistes.

R.R.Q., 1981, c. D-4, r. 11, a. 1.05.

SECTION II

TENUE DES DOSSIERS

2.01. Sous réserve de l'article 2.07, le denturologiste doit tenir, à l'endroit où il exerce sa profession, un dossier pour chacun de ses clients.

R.R.Q., 1981, c. D-4, r. 11, a. 2.01.

2.02. Le denturologiste doit consigner dans chaque dossier les éléments et renseignements suivants:

- a) la date d'ouverture du dossier;
- b) le nom du client, son adresse, son numéro de téléphone, sa date de naissance et son sexe;
- c) une description sommaire des motifs de la consultation;
- d) une description des services professionnels rendus et leur date;
- e) une description de la prothèse dentaire amovible fournie ou vendue, s'il y a lieu;
- f) les recommandations faites au client;
- g) les annotations, la correspondance et les autres documents relatifs aux services professionnels rendus; et
- h) la signature du denturologiste qui a rendu les services professionnels;
- i) le plan de traitement suggéré par le denturologiste et agréé par ce dernier et par le client;
- j) l'information exigée par l'article 7 de la Loi sur la denturologie (chapitre D-4) consignée sur une formule analogue à celle apparaissant à l'annexe I.

R.R.Q., 1981, c. D-4, r. 11, a. 2.02; D. 67-92, a. 1.

2.03. Un denturologiste doit tenir à jour chaque dossier jusqu'au moment où il cesse de rendre des services professionnels à la personne concernée par ce dossier.

R.R.Q., 1981, c. D-4, r. 11, a. 2.03.

2.04. Un denturologiste doit conserver chaque dossier pendant au moins 5 ans à compter de la date du dernier service rendu.

R.R.Q., 1981, c. D-4, r. 11, a. 2.04.

2.05. Un denturologiste doit conserver ses dossiers dans un local ou un meuble auquel le public n'a pas librement accès et pouvant être fermé à clef ou autrement.

R.R.Q., 1981, c. D-4, r. 11, a. 2.05.

2.06. Lorsqu'un client retire un document du dossier qui le concerne, le denturologiste doit insérer dans ce dossier une note signée par ce client indiquant la nature du document et la date du retrait.

R.R.Q., 1981, c. D-4, r. 11, a. 2.06.

2.07. Lorsqu'un denturologiste est membre ou à l'emploi d'une société, ou lorsqu'il est à l'emploi d'un autre denturologiste ou d'une personne morale, il peut utiliser les dossiers tenus par cette société ou cet employeur et y inscrire les éléments ou renseignements mentionnés à l'article 2.02 relativement aux personnes concernées par les services qu'il rend.

S'il ne peut le faire, il doit, aux fins du présent règlement, tenir un dossier pour chacune de ces personnes.

Le denturologiste doit signer ou parapher toute inscription ou tout rapport qu'il introduit dans un dossier conformément au premier alinéa.

R.R.Q., 1981, c. D-4, r. 11, a. 2.07.

2.08. Lorsque le denturologiste utilise l'informatique ou toute autre technique pour la constitution et la tenue de ses dossiers, il doit s'assurer que leur confidentialité soit respectée.

D. 67-92, a. 2.

SECTION III TENUE DES CABINETS DE CONSULTATION

3.01. Le denturologiste doit aménager son cabinet de consultation de façon à ce que l'identité et les conversations des personnes qui s'y trouvent ne puissent être perçues de l'extérieur de ce cabinet.

R.R.Q., 1981, c. D-4, r. 11, a. 3.01.

3.02. Le denturologiste doit aménager près de son cabinet de consultation une salle d'attente destinée à recevoir les personnes à qui il rend des services professionnels. L'aménagement de cette salle doit comprendre notamment des chaises ou des bancs et permettre un accès facile à des toilettes.

R.R.Q., 1981, c. D-4, r. 11, a. 3.02.

3.03. Le cabinet de consultation doit comprendre une salle pour prise d'empreintes et d'articulés, l'essai, la pose et l'adaptation de prothèses dentaires amovibles.

Cette salle doit également être pourvue d'une chaise dentaire appropriée à l'exercice de sa profession, d'une lampe directionnelle, d'un crachoir hygiénique, d'un lavabo pour l'hygiène personnelle du denturologiste, et d'un stérilisateur.

R.R.Q., 1981, c. D-4, r. 11, a. 3.03.

3.04. Le denturologiste doit, lorsqu'il rend des services professionnels à un client, changer ou stériliser les serviettes et les gobelets, après l'utilisation qu'en a faite un client.

R.R.Q., 1981, c. D-4, r. 11, a. 3.04.

3.05. Le cabinet de consultation du denturologiste et sa salle d'attente doivent être maintenus dans un bon état de propreté.

R.R.Q., 1981, c. D-4, r. 11, a. 3.05.

3.06. Le denturologiste doit afficher son permis à la vue du public.

R.R.Q., 1981, c. D-4, r. 11, a. 3.06.

3.07. Le denturologiste doit mettre à la vue du public dans le lieu mentionné à l'article 3.02 une copie du Code de déontologie de l'Ordre des denturologistes du Québec (chapitre D-4, r. 6) et du Règlement sur la procédure de conciliation et d'arbitrage des comptes des membres de l'Ordre des denturologistes du Québec (chapitre D-4, r. 12). Il doit également inscrire sur chacun de ces règlements l'adresse de l'Ordre.

R.R.Q., 1981, c. D-4, r. 11, a. 3.07.

3.08. Sous réserve des articles 3.06 et 3.07, le denturologiste, outre les objets décoratifs ou utilitaires, ne peut afficher dans son cabinet de consultation et dans les autres locaux reliés à la pratique de sa profession que les diplômes ayant un rapport avec l'exercice de sa profession.

R.R.Q., 1981, c. D-4, r. 11, a. 3.08.

3.09. Le denturologiste ne peut tenir dans son cabinet de consultation et dans les autres locaux reliés à la pratique de sa profession autre chose que des produits nécessaires à la fabrication, l'entretien, la réparation, l'essai, la pose, l'adaptation, le remplacement ou la vente de prothèses dentaires amovibles.

R.R.Q., 1981, c. D-4, r. 11, a. 3.09.

3.10. Le denturologiste qui s'absente de son cabinet de consultation pour plus de 5 jours ouvrables consécutifs doit prendre les mesures nécessaires pour informer les personnes qui tentent de le rejoindre, de la durée de cette absence.

R.R.Q., 1981, c. D-4, r. 11, a. 3.10.

ANNEXE I

(a. 2.02)

AVIS

J'ai subi un examen par un dentiste en vue de recevoir un service relatif à une prothèse partielle amovible.

OU

Je n'ai pas subi un examen par un dentiste en vue de recevoir un service relatif à une prothèse partielle amovible mais j'ai été informé de l'importance d'un tel examen.

Paraphe ou signature du patient

(Date).

D. 67-92, a. 3.

RÉFÉRENCES

R.R.Q., 1981, c. D-4, r. 11
D. 67-92, 1992 G.O. 2, 1049

24 questions pour évaluer votre utilisation des technologies de l'information

Répondez aux questions suivantes au meilleur de vos connaissances.

Si vous répondez **NON** ou si vous ignorez la réponse, suivez le **GUIDE DES TI en ligne!**

Rendez-vous au guideTI.barreau.qc.ca pour trouver l'information sur chacune des questions de ce test.

Dans votre cabinet ou votre organisation		OUI	NON	NE SAIS PAS	SUIVEZ LE GUIDE!
1	Avez-vous mis en place des mesures de sécurité pour protéger votre réseau informatique? Si oui, existe-t-il une politique sur l'utilisation des TI qui documente ces mesures de sécurité?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
2	Chaque utilisateur utilise-t-il un nom d'utilisateur et un mot de passe pour ouvrir une session de travail sur son ordinateur?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	• Mot de passe • Réseautique
3	Si oui, le mot de passe est-il obligatoirement : • Modifié au moins tous les 30 jours? • Composé d'un minimum de 10 caractères incluant au moins une majuscule, une minuscule, un chiffre et un symbole?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Mot de passe
4	Les sessions de travail sont-elles verrouillées automatiquement avec un écran de veille et un mot de passe lorsqu'un poste de travail reste inactif pendant une période maximale de trois minutes?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
5	Votre réseau est-il protégé par un pare-feu mis à jour régulièrement (aussi nommé coupe-feu ou <i>firewall</i> en anglais)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
6	Chaque poste de travail est-il protégé par un antivirus mis à jour automatiquement?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
7	Vos logiciels (ex. : Word ou Explorer) et vos systèmes d'exploitation (ex. : Windows ou Mac OS) sont-ils mis à jour automatiquement?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
8	Si vous avez un réseau sans fil (WiFi) : • Avez-vous modifié le code d'administrateur par défaut du routeur sans fil (point d'accès où les ordinateurs se connectent)? • Avez-vous modifié le mot de passe par défaut du routeur sans fil? • Avez-vous mis en place une méthode de chiffrement (cryptage) des données qui transitent sur le réseau sans fil? • Avez-vous configuré le routeur sans fil afin qu'il accepte seulement les communications en provenance des ordinateurs de votre réseau? • Avez-vous bloqué la diffusion publique du nom de votre réseau sans fil?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
9	Les données enregistrées par les utilisateurs sur un ordinateur portable, une tablette ou sur des supports amovibles (clé USB, disque dur externe, etc.) sont-elles chiffrées?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique
10	Autorisez-vous vos employés à travailler avec leur équipement informatique personnel? Si oui, avez-vous une politique permettant de vous assurer de la sécurité de ces appareils et de la gestion des risques?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Équipement personnel
11	Les utilisateurs qui travaillent de leur résidence disposent-ils d'une connexion RPV (Réseau privé virtuel – VPN en anglais) protégeant leur session de travail?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Réseautique

³ Tiré du Guide des TI du Barreau du Québec <http://guideti.barreau.qc.ca>

Dans votre cabinet ou votre organisation		OUI	NON	NE SAIS PAS	SUIVEZ LE GUIDE!
12	<p>En ce qui concerne les téléphones intelligents utilisés par les employés :</p> <ul style="list-style-type: none"> • Une authentification par un mot de passe sécuritaire (voir question 3) est-elle nécessaire pour accéder à leurs contenus? • La mise en veille automatique a-t-elle été configurée? • Le chiffrement des informations a-t-il été configuré? 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> • Cellulaire • Mot de passe • Chiffrement
13	Les connexions Bluetooth sont-elles configurées pour ne pas être disponibles par défaut et pour être sécurisées lorsqu'elles sont utilisées?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Cellulaire
14	L'accès aux documents électroniques et aux courriels conservés sur votre réseau est-il réservé aux personnes concernées seulement?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Communications électroniques
15	Les communications avec vos clients sont-elles protégées par un mot de passe, par l'utilisation d'un réseau fermé sécurisé avec le client ou par chiffrement?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Communications électroniques
16	Avez-vous mis en place une méthode de classement des documents enregistrés sur vos ordinateurs et de vos courriels conforme au <i>Règlement sur la comptabilité et les normes d'exercice professionnel des avocats</i> ?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> • Communications électroniques • Classement des documents
17	Avez-vous mis en place une méthode de gestion des copies de sauvegarde des données enregistrées sur votre réseau (ordinateurs, serveurs, téléphones intelligents, etc.)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Copie de sauvegarde des documents
18	Saviez-vous que certains documents contiennent des données confidentielles cachées qui peuvent être transmises à votre insu (commentaires ou suivi des corrections de Word, par exemple) et prenez-vous les mesures nécessaires afin d'éviter cela?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Métadonnées
19	Avez-vous des processus de sécurité informatique pour gérer le départ d'un employé (suppression de compte usager, de l'accès aux documents confidentiels, du compte de téléphonie, etc.)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Départ d'un employé
20	Les ententes conclues avec vos fournisseurs (p. ex. : technicien en informatique, service d'hébergement, infonuagique) sont-elles conformes à vos obligations déontologiques (confidentialité, etc.)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<ul style="list-style-type: none"> • Entente avec les fournisseurs • Infonuagique
21	Vos bureaux et votre équipement informatique sont-ils sécurisés?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Sécurisation des locaux et de l'équipement
22	Avez-vous une procédure de mise au rebut ou de recyclage sécurisé du matériel informatique?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Mise au rebut/ recyclage
23	Gérez-vous les alertes de sécurité concernant, par exemple, vos copies de sauvegarde ou les tentatives d'intrusion dans vos systèmes?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Surveillance et alertes
24	Disposez-vous d'un plan de continuité des affaires en cas de désastre?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Copie de sauvegarde des documents