



Ordre de la pratique infirmière
du Nouveau-Brunswick

Directive professionnelle : **Utilisation sécuritaire des technologies numériques**

Mandat

Protection du public par la réglementation des infirmières¹ au Nouveau-Brunswick.

La *Loi sur les infirmières et infirmiers* confère à l'Ordre de la pratique infirmière du Nouveau-Brunswick (OPINB) la responsabilité de protéger le public par la réglementation des membres de la profession infirmière au Nouveau-Brunswick. La réglementation rend cette profession dans son ensemble, de même que les infirmières immatriculées et infirmières praticiennes à titre individuel, responsables d'offrir des soins sécuritaires et éthiques avec compétence et compassion.

Remerciements

Certains éléments de la présente directive professionnelle ont été adaptés du document [Social Media Practice Guideline](#) (2025) du Nova Scotia College of Nursing (NSCN).

© Ordre de la pratique infirmière du Nouveau-Brunswick, 2026.

Droit d'auteur © Ordre de la pratique infirmière du Nouveau-Brunswick (OPINB), Fredericton (N.-B.).

Il est interdit de reproduire ce document, en tout ou en partie, à des fins commerciales ou lucratives sans l'autorisation écrite de l'OPINB. On peut toutefois le reproduire, intégralement ou partiellement, à des fins personnelles ou éducatives sans autorisation expresse, aux conditions suivantes :

- faire tout effort raisonnable pour en assurer la reproduction fidèle;
- préciser que l'OPINB en est l'auteur;
- préciser que le document reproduit n'est pas une version officielle et qu'il n'a pas été fait en collaboration avec l'OPINB ou avec son appui.

¹ Dans le présent document, le féminin prévaut pour ne pas nuire à la lecture et en reconnaissance de la réalité majoritairement féminine de la profession, mais est employé sans préjudice et désigne aussi les hommes et les membres des communautés 2ELGBTQI+.

Table des matières

Introduction.....	4
Professionalisme numérique.....	4
Technologies numériques.....	5
Principes directeurs d'une utilisation sécuritaire des technologies numériques.....	6
Avantages des technologies numériques.....	6
Risques des technologies numériques.....	6
Principales considérations liées à l'utilisation des technologies numériques	7
Responsabilités professionnelles	8
Responsabilité	8
Présence et conduite professionnelles.....	9
Confidentialité et sécurité.....	10
Limites professionnelles	10
Liberté d'expression	11
Utilisation appropriée de certaines technologies numériques	13
Appareils mobiles.....	13
Communications électroniques	14
Photos et vidéos	14
Applications et outils numériques.....	15
Médias sociaux	15
Outils d'intelligence artificielle	15
Télépratique infirmière	16
Dossiers médicaux électroniques et tenue de dossiers.....	17
Glossaire	18
Références	19
Annexe A : Outils pour favoriser le professionnalisme numérique et l'utilisation sécuritaire des technologies numériques	20
Annexe B : Mettre en pratique la liste de vérification pour la prise de décisions relatives aux technologies numériques	22

La présente directive professionnelle soutient l'application des lois pertinentes, du [Code de conduite des infirmières immatriculées et infirmières praticiennes](#) des [normes d'exercice](#) dans les contextes numériques. Le non-respect des attentes professionnelles lors de l'utilisation des technologies numériques peut donner lieu à des mesures réglementaires.

Introduction

Les [technologies numériques](#) sont intégrées à de nombreux aspects de la [pratique infirmière](#). On peut notamment penser au recours croissant à l'[intelligence artificielle](#), à l'utilisation généralisée des appareils mobiles, des [médias sociaux](#) et d'autres plateformes en ligne, ainsi qu'à l'usage de plus en plus marqué des [technologies de l'information et de la communication](#) dans la prestation des services de santé. Bien que ces outils puissent améliorer la communication, faciliter la prise de décisions et accroître l'efficacité, ils présentent également des risques liés à la protection de la [vie privée](#), à la [confidentialité](#), au professionnalisme numérique, à la mésinformation et au brouillage des [limites](#) (Booth et coll., 2021; O'Connor et coll., 2020).

La présente directive s'applique à toute II/IP² qui exerce la profession au Nouveau-Brunswick ou qui fournit des soins à des clients se trouvant au Nouveau-Brunswick. Elle s'applique à tous les milieux de pratique et englobe tant les technologies fournies par l'employeur que les technologies personnelles, qu'elles soient utilisées à l'intérieur ou à l'extérieur du milieu de travail, dès lors qu'il existe un lien avec le rôle professionnel ou l'identité professionnelle de l'II/IP.

Professionnalisme numérique

Le professionnalisme numérique désigne l'application des [valeurs](#), des comportements et du jugement professionnels ainsi que des attentes réglementaires dans les environnements numériques (Makondo, 2026; Park et Kim, 2025). Cela englobe la responsabilisation, la cohérence entre la conduite en ligne et en personne, l'autorégulation, la gestion de la vie privée et des limites, la pratique réflexive et la [littératie numérique](#). Ensemble, ces attributs sous-tendent la [conduite professionnelle](#) dans les environnements numériques.

²L'OPINB est l'organisme de régie des infirmières immatriculées, des infirmières diplômées, des infirmières praticiennes et des infirmières praticiennes diplômées du Nouveau-Brunswick. Les abréviations « II/IP » sont utilisées dans le présent document et désignent l'ensemble de ces désignations. Au Nouveau-Brunswick, les infirmières auxiliaires autorisées sont régies par l'Association des infirmier(ère)s auxiliaires autorisé(e)s du Nouveau-Brunswick.

Les II/IP font preuve de professionnalisme numérique lorsqu'elles :

- font preuve de respect et d'intégrité et favorisent la confiance et le partenariat dans toutes leurs interactions numériques;
- assument la responsabilité de l'ensemble de leurs actions et décisions dans les environnements numériques;
- maintiennent une présence professionnelle cohérente en ligne et dans leur pratique;
- adoptent une pratique réflexive à l'égard de leurs comportements dans les environnements numériques;
- veillent à la protection de la vie privée et de la confidentialité dans tous les environnements numériques;
- maintiennent des limites professionnelles;
- acquièrent et maintiennent les compétences numériques nécessaires pour utiliser les technologies de façon sécuritaire et éthique.

Technologies numériques

Les technologies numériques comprennent tout système ou outil électronique utilisé pour communiquer, consigner, stocker ou consulter de l'information. On peut citer en exemple les technologies numériques de la santé, les appareils mobiles, les applications, les médias sociaux, les plateformes en ligne ainsi que les technologies de l'information et de la communication utilisées dans la pratique professionnelle et la vie quotidienne.

Les politiques organisationnelles peuvent ne pas s'appliquer à toutes les utilisations personnelles des technologies numériques. Toutefois, les II/IP demeurent tenues de respecter leurs obligations professionnelles, éthiques, juridiques et réglementaires lorsque leur conduite dans les environnements numériques est liée à la pratique infirmière, à leur rôle ou à leur identité professionnelle, à la sécurité des clients, à la protection du public ou à la confiance du public.

Les principes directeurs suivants encadrent l'application du professionnalisme numérique dans les contextes numériques tant professionnels que personnels.

Principes directeurs d'une utilisation sécuritaire des technologies numériques

- La **sécurité des clients** et la protection du public doivent primer dans toutes les interactions numériques.
- Les II/IP font preuve de jugement professionnel et maintiennent les **compétences** nécessaires pour utiliser les technologies numériques de façon sécuritaire.
- Les II/IP veillent à la protection de la vie privée et de la confidentialité dans tous les contextes numériques.
- Les II/IP utilisent les technologies numériques conformément aux lois applicables, au Code de conduite, aux normes d'exercice ainsi qu'aux autres exigences réglementaires et politiques organisationnelles.
- Les II/IP demeurent responsables de leurs actions et de leurs décisions, quelle que soit la technologie utilisée.



*L'utilisation sécuritaire et **fondée sur des données probantes** des technologies numériques repose sur la littératie numérique et le jugement professionnel des II/IP, ainsi que sur leur engagement à utiliser ces outils de manière à protéger le public, à favoriser une pratique de qualité et à maintenir leur professionnalisme numérique.*

Avantages des technologies numériques

Les technologies numériques peuvent améliorer la prestation de soins infirmiers sécuritaires et efficaces. Lorsqu'elles sont choisies et utilisées de façon appropriée, les technologies numériques peuvent améliorer l'accès à l'information et aux services, favoriser la communication et la collaboration, éclairer la prise de décisions cliniques, soutenir la formation, la simulation, la recherche et l'amélioration de la qualité, et accroître l'efficacité des processus de travail (Ventola, 2014).

Risques des technologies numériques

Les technologies numériques présentent des risques susceptibles d'avoir une incidence sur la sécurité des clients, la protection de la vie privée et la confidentialité, ainsi que sur l'intégrité professionnelle. Les II/IP reconnaissent ces risques et font preuve de jugement professionnel et de littératie numérique lorsqu'elles utilisent ces technologies (Ventola, 2014).

- **Atteintes à la vie privée**³ – Les technologies numériques peuvent exposer des **renseignements personnels sur la santé**⁴ (RPS) lorsque des appareils, des réseaux ou des applications non sécurisés sont utilisés. Les risques comprennent notamment l'accès non autorisé, la divulgation accidentelle (p. ex. messages textes ou courriels envoyés au mauvais destinataire, captures

³Pour en savoir plus au sujet des atteintes à la vie privée, veuillez consulter la [Fiche d'information : Que savez-vous sur les atteintes à la vie privée?](#) et la [Directive professionnelle : Vie privée et confidentialité](#) de l'OPINB.

⁴Pour plus d'information sur les dispositions législatives relatives aux renseignements personnels sur la santé, veuillez consulter la [Loi sur l'accès et la protection en matière de renseignements personnels sur la santé](#).

d'écran affichant des renseignements sur les clients) et l'utilisation de plateformes qui ne respectent pas les exigences législatives ou organisationnelles.

- *Mésinformation et données inexacts* – Les renseignements communiqués ou consultés par voie numérique peuvent être incomplets, désuets ou inexacts. Les clients peuvent mal interpréter les conseils reçus par voie numérique, et les outils d'aide à la décision peuvent comporter des erreurs ou des biais susceptibles d'influencer la prise de décisions cliniques.
- *Franchissement des limites professionnelles* – Les communications numériques, particulièrement celles effectuées au moyen d'appareils personnels ou des médias sociaux, peuvent brouiller les limites professionnelles. En effet, le ton et l'intention peuvent être mal interprétés, et les interactions en ligne peuvent donner l'impression qu'il existe une relation personnelle.
- *Atteinte à la réputation* – Les comportements en ligne, qu'ils soient d'ordre personnel ou professionnel, peuvent avoir une incidence sur la confiance du public. Le contenu numérique peut demeurer accessible, consultable, reproductible ou récupérable après sa publication ou sa suppression. Il peut également être copié, modifié ou diffusé à nouveau à l'insu de son auteur ou sans son consentement. Le fait d'être associé à de la mésinformation ou à du contenu inapproprié peut nuire à la crédibilité.
- *Faibles de sécurité* – Les cyberattaques, l'hameçonnage, les logiciels malveillants ainsi que la perte ou le vol d'un appareil peuvent compromettre des renseignements sensibles. L'utilisation d'applications ou d'outils infonuagiques non approuvés accroît les risques d'atteinte à la sécurité et de vulnérabilité des systèmes.
- *Accès inéquitable aux soins* – Les clients n'ont pas tous le même accès aux technologies ou à une connexion Internet fiable ni le même niveau de littératie numérique. Une dépendance excessive aux technologies numériques peut désavantager les personnes qui disposent de ressources limitées, qui doivent composer avec des barrières linguistiques ou qui ont des besoins particuliers en matière d'accessibilité.

Principales considérations liées à l'utilisation des technologies numériques

- Le fait de fournir des conseils en dehors d'une [relation infirmière-client](#) établie peut entraîner des responsabilités professionnelles, notamment le [devoir de fournir des soins](#)⁵, engager la responsabilité de l'II/IP ou constituer un exercice de la profession à l'extérieur du territoire où l'II/IP est autorisée à exercer.
- Les atteintes à la confidentialité, les conseils inexacts, le non-respect des attentes professionnelles ou l'exercice non autorisé de la profession peuvent entraîner des conséquences sur les plans organisationnel, réglementaire ou juridique.
- Le contenu numérique peut être conservé, copié, rediffusé, modifié ou consulté par des personnes autres que le public visé, et ce, quels que soient les paramètres de confidentialité.

⁵ Pour plus d'informations sur le devoir de fournir des soins, veuillez consulter la [Directive professionnelle : le devoir de fournir des soins](#) de l'OPINB.



En cas de doute, prenez le temps de demander conseil avant d'aller de l'avant.

Afin de faciliter l'application de la présente directrice dans la pratique, l'[annexe A](#) propose une liste de vérification pour la prise de décisions relatives aux technologies numériques. L'[annexe B](#) présente des études de cas qui illustrent comment utiliser la liste de vérification afin d'analyser des situations mettant en jeu des technologies numériques et de favoriser une pratique infirmière sécuritaire, éthique et professionnelle.

Responsabilités professionnelles

Le professionnalisme numérique exige des II/IP qu'elles s'acquittent de leurs responsabilités professionnelles lorsqu'elles utilisent des technologies numériques. Ces responsabilités peuvent également s'appliquer aux comportements numériques d'ordre personnel lorsque ceux-ci sont susceptibles d'avoir une incidence sur la sécurité des clients, la protection du public, l'intégrité professionnelle ou la confiance du public.

Responsabilité

Les II/IP demeurent responsables de toutes leurs décisions et actions liées à l'utilisation des technologies numériques. Conformément au principe de [responsabilité professionnelle](#), les II/IP doivent veiller à ce que les technologies numériques appuient leur jugement clinique plutôt que de s'y substituer. Cette responsabilité suppose notamment de comprendre les capacités, les limites et les risques associés aux technologies utilisées.

Dans les environnements numériques, la responsabilité professionnelle consiste notamment à :

- utiliser les technologies numériques conformément aux lois applicables, aux exigences réglementaires et aux politiques organisationnelles;
- préconiser l'élaboration de politiques organisationnelles lorsqu'il n'existe pas de directives encadrant l'utilisation des technologies numériques;
- vérifier l'exactitude, la fiabilité et la pertinence des renseignements obtenus ou générés au moyen de technologies numériques;
- comprendre les capacités, les limites et les risques associés aux technologies numériques;
- reconnaître que les activités en ligne, qu'elles soient d'ordre personnel ou professionnel, peuvent avoir des conséquences sur le plan professionnel;
- maintenir les compétences nécessaires à l'utilisation sécuritaire des technologies numériques et demander conseil en présence de situations, de risques ou de limites qui ne sont pas familiers;
- consigner les renseignements pertinents échangés au moyen de communications numériques conformément aux [Normes pour la tenue de dossiers](#) de l'OPINB et aux politiques organisationnelles.

Présence et conduite professionnelles

La **présence professionnelle**⁶ suppose d'être consciente, à titre d'II/IP, de la façon dont sa propre conduite peut être perçue par les clients, les collègues, l'**équipe de soins de santé**, l'organisme de réglementation et le public. Cette attente s'applique également aux activités en ligne et aux communications numériques, qui sont assujetties aux mêmes normes professionnelles.

Pour maintenir une présence professionnelle dans les environnements numériques, il faut notamment :

- communiquer de façon respectueuse, professionnelle et éthique;
- éviter de publier ou de partager du contenu susceptible de miner la confiance du public envers la profession;
- maintenir des limites appropriées dans les relations avec les clients et les collègues;
- éviter de fournir des conseils personnalisés en matière de soins infirmiers ou de santé sur les médias sociaux ou dans d'autres environnements numériques publics ou ⁷non sécurisés⁸;
- éviter les situations susceptibles de créer un **conflit d'intérêts**⁹.

⁶ Pour en savoir plus au sujet de la présence professionnelle, veuillez consulter la [Fiche d'information : La présence professionnelle](#) de l'OPINB.

⁷ Un environnement numérique public est un espace numérique dans lequel le contenu est accessible ou visible à un vaste public ou à un public indéterminé. Il peut notamment s'agir de sites Web publics, de médias sociaux, de blogues et de forums en ligne. Un environnement numérique ne doit pas être considéré comme privé du seul fait des paramètres du compte ou de confidentialité.

⁸ Un environnement numérique non sécurisé est un espace, une plateforme, une application, un appareil ou un système, public ou privé, qui n'est pas autorisé aux fins prévues ou qui ne comporte pas les mesures de protection de la vie privée et de sécurité requises pour les renseignements ou l'activité en question.

⁹ Pour en savoir plus au sujet des conflits d'intérêts, veuillez consulter la [Directive professionnelle : conflits d'intérêts](#) de l'OPINB.



Les déclarations faites en ligne peuvent être perçues comme représentant le point de vue d'un employeur ou de la profession, même lorsqu'elles sont publiées de façon anonyme, sous un pseudonyme ou à partir d'un compte personnel.

Confidentialité et sécurité

Les II/IP doivent utiliser des technologies autorisées et prendre des mesures raisonnables pour protéger les renseignements contre tout accès, toute utilisation ou toute divulgation non autorisée, ainsi que contre la perte, la modification ou la destruction. Elles doivent reconnaître et signaler toute atteinte présumée à la vie privée ou à la sécurité conformément aux exigences applicables et aux politiques organisationnelles.

Pour protéger la vie privée et assurer la confidentialité et la sécurité des renseignements, il faut notamment :

- s'assurer d'utiliser uniquement des plateformes approuvées par l'organisation pour communiquer des RPS;
- veiller à ce que les appareils utilisés soient protégés par un mot de passe, sécurisés et, s'il y a lieu, chiffrés;
- utiliser un appareil personnel pour consulter, recueillir, saisir, stocker ou transmettre des RPS uniquement lorsqu'une telle utilisation est autorisée et que des mesures de protection appropriées sont en place;
- reconnaître les risques pour la sécurité, y réagir de façon appropriée et signaler les incidents de sécurité conformément aux politiques organisationnelles.



Les II/IP communiquent les renseignements sur les clients uniquement au moyen de plateformes autorisées et sécurisées qui conviennent à l'usage prévu. La dépersonnalisation des renseignements ou le consentement du client ne suffisent pas, à eux seuls, à éliminer les risques liés à la protection de la vie privée et à la confidentialité.

Limites professionnelles

Les limites professionnelles s'appliquent de la même façon aux interactions numériques et aux interactions en personne. Les comportements en ligne, qu'ils soient intentionnels ou non, peuvent avoir une incidence sur la relation infirmière-client¹⁰.

¹⁰ Pour en savoir plus au sujet des limites professionnelles, veuillez consulter les [Normes pour la relation infirmière-client](#) de l'OPINB.

Pour maintenir des limites professionnelles dans les environnements numériques, il faut notamment :

- éviter les interactions personnelles en ligne avec les clients actuels et leur famille, et faire preuve de discernement dans les interactions avec d'anciens clients lorsqu'un déséquilibre de pouvoir, une situation de vulnérabilité ou des éléments de la relation thérapeutique peuvent subsister;
- maintenir une séparation claire entre les communications personnelles et professionnelles;
- reconnaître et gérer les situations où les rôles personnels et professionnels se chevauchent;
- préciser clairement aux clients les limites à respecter dans les communications numériques;
- éviter tout contenu ou comportement en ligne susceptibles de compromettre la relation infirmière-client ou la confiance du public envers la profession.



Avant d'établir un contact ou de communiquer en ligne, il convient de réfléchir au but de l'interaction et à ses répercussions possibles sur le client, les limites professionnelles et la relation infirmière-client.

Liberté d'expression

La [Charte canadienne des droits et libertés](#) protège la liberté de pensée, de croyance, d'opinion et d'expression, notamment dans les médias numériques et autres. Cette liberté n'est toutefois pas absolue et peut être assujettie à des limites raisonnables prescrites par la loi (Rosen Sunshine LLP, 2023). Les II/IP doivent tenir compte des répercussions que leurs propos publics ou leurs communications numériques peuvent avoir sur la sécurité des clients, la protection de la vie privée et la confidentialité, l'intégrité professionnelle et la confiance du public (Nova Scotia College of Nursing, 2025).

Pour faire preuve de jugement professionnel au moment d'exprimer son point de vue en public ou dans des environnements numériques, il faut notamment :

- protéger la vie privée et la confidentialité, notamment en évitant de divulguer des RPS;
- communiquer de manière à préserver la confiance du public envers la profession infirmière;
- respecter les lois applicables, les exigences réglementaires et les politiques organisationnelles;
- éviter de communiquer toute mésinformation ou désinformation¹¹ susceptible de compromettre la sécurité des clients ou la protection du public;
- distinguer clairement ses opinions de celles de son employeur, de son organisation, de son organisme de réglementation ou de la profession infirmière;
- tenir compte des répercussions possibles de ses propos en ligne sur sa crédibilité professionnelle et ses relations thérapeutiques;
- exprimer ses opinions d'une manière qui concorde avec ses responsabilités professionnelles, éthiques et juridiques.



La liberté d'expression ne soustrait pas les II/IP à leurs responsabilités professionnelles.

¹¹ Pour en savoir plus au sujet de la mésinformation et de la désinformation, veuillez consulter la [Fiche d'information sur la mésinformation et la désinformation](#) de l'OPINB.

Utilisation appropriée de certaines technologies numériques

Les technologies numériques sont utilisées de diverses façons dans la pratique infirmière. Bien que chaque technologie présente des possibilités, des limites et des risques qui lui sont propres, les responsabilités professionnelles, éthiques, juridiques et réglementaires des II/IP demeurent les mêmes. Les considérations suivantes favorisent une utilisation sécuritaire, efficace et appropriée des technologies numériques couramment employées dans la pratique professionnelle.

Les responsabilités professionnelles décrites précédemment dans la présente directive s'appliquent à toutes les technologies numériques. Les sections qui suivent présentent des considérations supplémentaires propres à des technologies en particulier.

Les exemples sont fournis à titre indicatif seulement. L'OPINB n'approuve ni ne recommande aucun produit, aucune plateforme, aucune application, aucun système ni aucune technologie en particulier, et n'en fait pas la promotion.



Les II/IP en pratique autonome doivent établir les politiques et les mesures de protection nécessaires pour assurer une utilisation sécuritaire des technologies numériques dans leur pratique.

Appareils mobiles

Lorsqu'elles utilisent des appareils mobiles dans leur pratique professionnelle, les II/IP doivent :

- le faire de façon responsable et dans le respect des politiques organisationnelles;
- veiller à ce que l'utilisation des appareils ne compromette pas la sécurité des clients, la protection de la vie privée, la confidentialité ou leurs responsabilités professionnelles;
- utiliser leurs appareils personnels à des fins professionnelles uniquement lorsque cette utilisation est autorisée et que les mesures requises pour protéger la vie privée et assurer la sécurité sont en place;
- réduire au minimum les distractions et veiller à ce que l'utilisation des appareils ne nuise pas à la prestation de soins sécuritaires ni à la communication thérapeutique;
- tenir compte des risques juridiques, éthiques et professionnels associés à l'utilisation des appareils mobiles.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés à l'utilisation des appareils mobiles, veuillez consulter les ressources suivantes de la Société de protection des infirmières et infirmiers du Canada (SPIIC) :

- [InfoDROIT: Appareils mobiles au travail](#)
- [Legal case study: Distraction by cell phone](#) (disponible en anglais seulement au moment de la rédaction du présent document)

Communications électroniques

Lorsqu'elles utilisent des moyens de communication électroniques (p. ex., courriels, messages textes) à des fins professionnelles, les II/IP doivent :

- utiliser des plateformes de communication sécurisées, autorisées par l'organisation et adaptées à la nature et à l'objectif de la communication;
- veiller à ce que les RPS soient communiqués uniquement aux personnes autorisées et se limitent au minimum nécessaire pour atteindre l'objectif déterminé;
- obtenir et consigner le consentement éclairé aux communications électroniques¹²;
- communiquer de façon claire, exacte et professionnelle, et adaptée au contexte;
- reconnaître que les plateformes de messagerie peuvent présenter des risques liés à la protection de la vie privée, à la confidentialité et aux malentendus;
- établir et communiquer les attentes relatives aux communications numériques, notamment leur objectif, leur utilisation appropriée, les périodes de surveillance des messages et les délais de réponse prévus, ainsi que les autres moyens d'accéder aux soins lorsque l'II/IP n'est pas disponible;
- vérifier l'identité du destinataire avant de transmettre des renseignements sur le client et vérifier l'identité de l'expéditeur ou du client lorsque cela est pertinent sur le plan clinique;
- consigner les échanges pertinents conformément aux [Normes pour la tenue de dossiers](#) de l'OPINB et aux politiques organisationnelles.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés aux communications électroniques, veuillez consulter les ressources suivantes de la SPIIC :

- [Question juridique : Mises à jour par SMS à d'autres professionnels de la santé](#)
- [InfoDROIT: Risques juridiques liés à l'utilisation du courrier électronique – Première partie: Préoccupations relatives à la protection des renseignements personnels](#)
- [InfoDROIT: Risques juridiques liés à l'utilisation du courrier électronique – Deuxième partie: Considérations d'ordre pratique](#)

Photos et vidéos

Lorsqu'elles prennent, conservent ou partagent des photos ou des vidéos dans le cadre de leur exercice professionnel, les II/IP doivent :

- obtenir et consigner le consentement éclairé ainsi que toute autre autorisation exigée par les lois applicables ou les politiques organisationnelles;
- utiliser des appareils et des plateformes autorisés conformément aux politiques organisationnelles;
- protéger la vie privée et la confidentialité des clients représentés ou autrement identifiables sur les photos et les vidéos à toutes les étapes de leur collecte, de leur consultation, de leur utilisation, de leur stockage, de leur transmission, de leur conservation et de leur destruction sécurisée;
- veiller à ce que les photos et les vidéos soient utilisées uniquement à des fins cliniques, éducatives ou organisationnelles légitimes, avec les autorisations appropriées;
- évaluer la nécessité de prendre une photo ou une vidéo avant de le faire.

¹²Les II/IP peuvent consulter le modèle de formulaire de la SPIIC intitulé [Consentement à l'utilisation des communications électroniques](#) pour faciliter la consignation du consentement.

Applications et outils numériques

Lorsqu'elles utilisent des applications et d'autres outils numériques, les II/IP doivent :

- utiliser des applications et des outils provenant de sources fiables et fondées sur des données probantes;
- vérifier l'exactitude et la pertinence des renseignements obtenus ou générés;
- utiliser des applications et des outils approuvés par l'organisation;
- reconnaître que les technologies numériques soutiennent le jugement professionnel, mais ne le remplacent pas;
- examiner et appliquer les paramètres appropriés de protection de la vie privée et de sécurité;
- ne pas saisir de RPS permettant d'identifier les clients dans des applications ou des systèmes publics ou non sécurisés;
- recommander uniquement des applications et des outils appropriés, fiables et conformes aux exigences de l'organisation.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés aux applications et aux outils numériques, veuillez consulter les ressources suivantes de la SPIIC :

- [*InfoDROIT: Applications de santé mobiles*](#)

Médias sociaux

Lorsqu'elles utilisent les médias sociaux, les II/IP doivent :

- éviter de publier et de partager des renseignements, des images ou d'autres contenus identifiant un client ou qui pourraient raisonnablement permettre de l'identifier, même lorsque les éléments d'identification directs ont été supprimés;
- adopter une conduite professionnelle et préserver la confiance du public envers la profession;
- utiliser les titres professionnels et les désignations professionnelles de façon exacte et conformément aux exigences réglementaires;
- ne pas établir ni accepter de liens personnels sur les médias sociaux avec leurs clients actuels et évaluer soigneusement toute possibilité d'établir un tel lien avec un ancien client, conformément aux exigences relatives aux limites professionnelles;
- reconnaître que le contenu publié en ligne peut être permanent, consultable au moyen d'une recherche et rediffusé au-delà du public initialement visé.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés aux médias sociaux, veuillez consulter les ressources suivantes de la SPIIC :

- [*InfoDROIT: Médias sociaux*](#)
- [*Question juridique : Médias sociaux*](#)

Outils d'intelligence artificielle

Lorsqu'elles utilisent l'intelligence artificielle (IA) dans leur pratique professionnelle, les II/IP doivent :

- utiliser uniquement des outils d'IA autorisés aux fins prévues;

- s'assurer de protéger la vie privée et la confidentialité et de ne pas saisir de RPS dans des outils d'IA publics ou non sécurisés;
- comprendre l'utilisation prévue de l'outil, ses capacités, ses limites et les risques qui y sont associés;
- vérifier de manière indépendante l'exactitude, la fiabilité et la pertinence des renseignements générés par l'IA, ainsi que les biais potentiels qu'ils peuvent comporter;
- faire preuve d'esprit critique et mettre à profit leur expertise clinique lorsqu'elles interprètent du contenu généré par l'IA ou prennent des mesures en fonction de celui-ci;
- respecter les exigences applicables en matière de transparence, de consentement éclairé et de tenue de dossiers lorsque l'IA est utilisée dans le cadre des soins aux clients;
- demeurer responsables des décisions, des mesures, des communications et de la documentation produites avec l'aide de l'IA;
- respecter les attentes et les lignes directrices énoncées dans la [Fiche d'information : l'intelligence artificielle](#) de l'OPINB.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés aux outils d'IA, veuillez consulter les ressources suivantes de la SPIIC :

- [L'intelligence artificielle dans les soins de santé : considérations pour la gestion des risques juridiques dans l'exercice des soins infirmiers](#)



L'IA appuie les connaissances, la responsabilité et le jugement professionnels des infirmières ainsi que la relation thérapeutique, sans toutefois s'y substituer. Les II/IP doivent examiner et valider les renseignements générés par l'IA avant de les utiliser dans leur pratique.

Télépratique infirmière

Lorsqu'elles prodiguent des soins au moyen des technologies de télépratique infirmière, les II/IP doivent :

- respecter les mêmes normes d'exercice que celles qui s'appliquent aux soins en personne;
- s'assurer que la technologie utilisée est appropriée, sécurisée et adaptée à la prestation de soins sécuritaires;
- évaluer si la télépratique infirmière convient au client et respecter les exigences relatives au consentement, à la vérification de l'identité, à la protection de la vie privée, à la confidentialité, à la sécurité et à la tenue de dossiers;
- déterminer et respecter les exigences en matière d'immatriculation, les exigences légales et réglementaires, ainsi que celles relatives à la responsabilité professionnelle et aux politiques organisationnelles applicables dans chaque territoire de compétence concerné;
- agir en conformité avec la [Directive professionnelle : Télépratique infirmière](#) de l'OPINB.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés à la télépratique infirmière, veuillez consulter les ressources suivantes de la SPIIC :

- [InfoDROIT: Télépratique](#)
- [Douze éléments à considérer avant de se joindre à un cabinet de soins de santé virtuels](#)

Dossiers médicaux électroniques et tenue de dossiers

Lorsqu'elles consultent les dossiers médicaux électroniques (DME) ou y consignent des renseignements, les II/IP doivent :

- accéder au dossier médical d'un client uniquement lorsqu'elles y sont autorisées, à des fins professionnelles légitimes et dans la mesure nécessaire à ces fins;
- protéger leurs identifiants de connexion et utiliser des méthodes d'accès sécurisées;
- verrouiller l'écran ou fermer leur session avant de laisser un DME ou un appareil sans surveillance;
- respecter les exigences relatives à la protection de la vie privée, à la confidentialité et à la sécurité de l'information;
- respecter les exigences organisationnelles relatives à l'accès aux DME, à leur utilisation et à la gestion de l'information;
- reconnaître que l'accès aux DME et les activités qui y sont effectuées peuvent faire l'objet d'une surveillance et d'une vérification.

Pour en savoir plus au sujet des enjeux d'ordre juridique liés aux dossiers médicaux électroniques et à la tenue de dossiers, veuillez consulter les ressources suivantes de la SPIIC :

- [*InfoDROIT: Protection de la vie privée et les dossiers médicaux électroniques*](#)
- [*Question juridique : Dossiers médicaux électroniques dans la pratique privée*](#)
- [*Question juridique: Notes tardives*](#)
- [*InfoDROIT: Une documentation de qualité: votre meilleure défense*](#)

Glossaire

Veillez noter que le glossaire ci-dessous contient des termes nouveaux ou révisés qui sont proposés, mais qui ne figurent pas encore dans le glossaire en ligne de l'OPINB. Ces définitions sont diffusées dans le cadre du processus de consultation externe et pourraient être révisées avant leur publication.

Application (appli)

Programme informatique conçu pour remplir une fonction précise et utilisé sur un ordinateur ou un appareil mobile.

Intelligence artificielle (IA)

L'IA désigne, au sens large, les programmes informatiques capables d'accomplir des tâches traditionnellement associées à l'intelligence humaine. Elle repose sur du code informatique qui permet d'analyser et d'évaluer rapidement des données, selon des processus semblables à ceux de l'intelligence humaine, comme le raisonnement, la prise de décisions ou l'apprentissage à partir d'expériences antérieures. Ces processus peuvent produire divers résultats, notamment des textes, des images, des prédictions fondées sur des données historiques ou encore l'exécution de tâches par des robots.

Littératie numérique

Terme désignant les connaissances, les compétences et le jugement nécessaires pour accéder aux technologies numériques, les évaluer, les comprendre et les utiliser de manière sécuritaire, efficace et éthique. Cela comprend notamment la capacité de reconnaître les avantages, les limites, les risques, la fiabilité et les utilisations appropriées des outils et des renseignements numériques.

Technologies numériques

Systèmes, appareils, applications, plateformes et outils électroniques utilisés pour créer, recueillir, consulter, stocker, traiter, partager, transmettre ou gérer de l'information. Dans la pratique infirmière, les technologies numériques peuvent être utilisées à des fins de communication, de tenue de dossiers, de formation, de prise de décisions, de prestation de soins, d'administration, de recherche ou à d'autres fins professionnelles ou personnelles. Leur utilisation exige l'exercice du jugement professionnel, une bonne littératie numérique et le respect des exigences déontologiques, légales, réglementaires et organisationnelles applicables.

Technologies numériques de la santé

Outils, systèmes et services d'information et de communication utilisés pour recueillir, stocker, échanger et analyser des renseignements sur la santé afin de soutenir la prestation, la coordination et l'évaluation des soins. Dans la pratique infirmière, leur utilisation est encadrée par les obligations professionnelles et déontologiques relatives à la protection de la vie privée, au respect de la confidentialité, au consentement éclairé et à la prestation de soins sécuritaires, administrés avec compétence et compassion.

Références

Booth, R. G., G. Strudwick, S. McBride, S. O'Connor et A. L. S. López (2021). « How the nursing profession should adapt for a digital future », *The BMJ*, vol. 373, article n1190.
<https://doi.org/10.1136/bmj.n1190>

Makondo, C. (2026). « Digital professionalism: Maintaining professional standards when using digital messaging platforms », *Nursing Standard*, vol. 41, n° 5, p. 47-54.
<https://doi.org/10.7748/ns.2026.e12620>

Nova Scotia College of Nursing (2025). *Social Media Practice Guideline*.
<https://www.nsnmr.ca/sites/default/files/documents/resources/Social-Media.pdf>

O'Connor, S., C. H. Chu, F. Thilo, J. J. Lee, C. Mather et M. Topaz (2020). « Professionalism in a digital and mobile world: A way forward for nursing », *Journal of Advanced Nursing*, vol. 76, n° 1, p. 4-6.
<https://doi.org/10.1111/jan.14224>

Park, Y. et I. Kim (2025). « E-Professionalism in Nursing: A Concept Analysis Using Walker and Avant's Method », *Journal of Korean Academy of Psychiatric & Mental Health Nursing*, vol. 34, numéro spécial, p. 1-8. <https://doi.org/10.12934/jkpmhn.2025.34.S1.1>

Rosen Sunshine LLP (2023). « Peterson v. College of Psychologists of Ontario », *Rosen Sunshine LLP*.
<https://www.rosensunshine.com/blog/peterson-v-college-of-psychologists-of-ontario>

Ventola, C. L. (2014). « Social Media and Health Care Professionals: Benefits, Risks, and Best Practices », *Pharmacy and Therapeutics*, vol. 39, n° 7, p. 491-520.

Annexe A : Outils pour favoriser le professionnalisme numérique et l'utilisation sécuritaire des technologies numériques

Liste de vérification pour la prise de décisions relatives aux technologies numériques

Avant...

 D'envoyer un message texte ou un courriel

 D'accéder à un DME

 De prendre ou partager une photo ou une vidéo

 De publier ou partager du contenu sur les médias sociaux

 D'utiliser des outils d'IA

 De fournir des soins virtuels

 D'utiliser un appareil mobile à des fins professionnelles

ARRÊTEZ-VOUS UN INSTANT ET POSEZ-VOUS LES QUESTIONS SUIVANTES :

- ☐ **Conformité** – Est-ce conforme à la législation, aux politiques organisationnelles et aux normes réglementaires?
- ☐ **Sécurité** – Cette plateforme est-elle sécurisée et adaptée à l'utilisation prévue?
- ☐ **Exactitude** – Les renseignements sont-ils exacts et fondés sur des données probantes?
- ☐ **Confidentialité** – Est-ce que je communique des RPS ou d'autres renseignements confidentiels uniquement lorsque j'y suis autorisée, à des fins cliniques ou à d'autres fins professionnelles autorisées, et par des moyens de communication sécurisés?
- ☐ **Professionnalisme** – Est-ce que cela respecte mon rôle professionnel, mes limites professionnelles et mon champ d'exercice?
- ☐ **Caractère approprié** – Mon utilisation ou mon intervention est-elle appropriée et respectueuse?
- ☐ **Confiance du public** – Cette action contribuera-t-elle à maintenir la confiance du public envers la profession infirmière?

ALLEZ-Y

Si la réponse à toutes les questions applicables est OUI.

Allez-y, tout en continuant à exercer votre jugement professionnel et à surveiller l'évolution des risques.

CONSULTEZ

Si vous avez des DOUTES quant à une ou plusieurs réponses.

Prenez un temps d'arrêt, consultez les politiques et la législation applicables et demandez conseil à la direction, à la [SPIIC](#) ou à l'[OPINB](#).

ARRÊTEZ!

Si la réponse à une ou plusieurs questions est NON.

N'allez pas plus loin; réglez les préoccupations soulevées et demandez conseil avant de poursuivre.

Vérification rapide de la responsabilité professionnelle

- ✓ Serais-je à l'aise d'expliquer cette action à mon employeur?
- ✓ Serais-je à l'aise de consigner cette action dans le dossier médical du client?
- ✓ Serais-je à l'aise si cette action faisait l'objet d'un examen par mon employeur ou l'OPINB, ou dans le cadre d'une procédure judiciaire?

Rappels importants

- Protéger la vie privée, la confidentialité et RPS.
- Exercer son jugement professionnel.
- Vérifier l'exactitude des renseignements numériques.
- Utiliser des technologies sécurisées et autorisées.
- Respecter les lois, politiques et normes applicables.
- Maintenir les limites professionnelles.
- Consigner l'information pertinente.
- Assumer sa responsabilité professionnelle.



Tout comportement en ligne qui compromet la vie privée des clients, l'intégrité professionnelle ou la confiance du public peut entraîner des mesures réglementaires.



Le contenu numérique peut demeurer accessible en permanence, être repérable au moyen d'une recherche et être partagé, quels que soient les paramètres de confidentialité. Il peut être copié, modifié ou partagé à votre insu ou sans votre consentement.

EN CAS DE DOUTE, PRENEZ LE TEMPS de demander conseil avant d'aller de l'avant!

Annexe B : Mettre en pratique la liste de vérification pour la prise de décisions relatives aux technologies numériques

Remarque : Nos études de cas se veulent des ressources pédagogiques fictives. Bien que nous nous efforcions de rendre les scénarios aussi réalistes que possible, toute ressemblance avec des personnes ou des événements réels serait purement fortuite.

Étude de cas 1 : Prise et transmission d'une photo d'un client

Jean, II au service des urgences, utilise son téléphone cellulaire pour prendre une photo d'un client qui reçoit des soins à la suite d'un accident de voiture. La photo n'est pas nécessaire à la prestation des soins au client ni à toute autre fin clinique autorisée. Jean n'a pas obtenu le consentement éclairé ni l'autorisation du client pour prendre ou transmettre la photo.

Jean envoie la photo à des collègues dans une conversation de groupe, décrit les blessures du client et se met à parler de l'accident. La discussion n'a aucun lien avec la prestation ou la coordination des soins, et l'application de messagerie utilisée n'est pas un système de communication clinique approuvé. Même si le nom du client n'est pas mentionné, la photo et les renseignements qui l'accompagnent pourraient permettre de l'identifier. Une fois la photo et les messages partagés, Jean ne peut plus contrôler leur enregistrement, leur copie, leur modification ou leur redistribution à des personnes autres que les destinataires prévus.

Éléments clés à considérer

- Prise d'une photo d'un client sans justification clinique
- Absence de consentement ou d'autorisation appropriée
- Utilisation d'un appareil personnel pour stocker ou communiquer des RPS
- Communication de renseignements au moyen d'un système non approuvé et non sécurisé
- Discussion de RPS à des fins sans lien avec les soins
- Risque d'identification du client à partir des renseignements communiqués

Utilisation de la liste de vérification pour la prise de décisions

Avant de prendre ou de transmettre la photo, Jean aurait dû utiliser la liste de vérification pour la prise de décisions relatives aux technologies numériques. Voici à quoi cela pourrait ressembler :

RÉSULTAT DE LA LISTE DE VÉRIFICATION	Pourquoi les réponses sont « NON »
❌ Conformité ❌ Sécurité – Exactitude → sans objet ❌ Confidentialité ❌ Professionnalisme ❌ Caractère approprié ❌ Confiance du public La réponse à une ou plusieurs questions est NON. ARRÊTEZ!	<i>L'action ne satisfait pas aux critères de la liste de vérification, puisque la photo et les renseignements connexes sur le client ont été recueillis et communiqués à des fins non cliniques, sans l'autorisation ou le consentement appropriés, au moyen d'une application de messagerie et d'un appareil personnel non approuvés. La communication de ces renseignements n'était pas nécessaire aux fins des soins, ne protégeait pas la vie privée ni la confidentialité et était incompatible avec les responsabilités professionnelles, les politiques organisationnelles et la confiance du public.</i> Résultat : Arrêtez. Ne prenez pas et ne transmettez pas la photo.

Étude de cas 1 : Prise et transmission d'une photo d'un client (suite)

Points d'apprentissage

Ce scénario démontre pourquoi l'outil exige une réponse OUI à toutes les questions applicables avant d'aller de l'avant; les renseignements sur un client ne peuvent être recueillis, consultés, utilisés, stockés ou communiqués qu'au moyen d'une méthode approuvée et sécurisée, avec les autorisations appropriées en place. Le fait d'omettre le nom du client, de limiter la diffusion à des collègues ou d'obtenir le consentement ne suffit pas, à lui seul, à rendre appropriés la finalité, l'appareil, la plateforme ou la communication des renseignements.

Étude de cas 2 : Atteinte à la confidentialité dans un groupe Facebook

Julie, II, a rejoint un groupe Facebook créé par de jeunes mères auprès desquelles elle travaille. Elle s'est inquiétée lorsque Kim, une cliente, a publié un message indiquant qu'elle traversait une période difficile et qu'elle se sentait très mal. Julie, dans le but d'offrir son soutien, a commenté : « Je sais que la semaine dernière a été difficile. Prends-tu toujours tes médicaments? Passe me voir demain, on pourrait en parler. »

Après le travail, une autre mère a abordé Julie à l'épicerie en lui disant : « J'ignorais que Kim prenait des médicaments! » Julie a été choquée de constater qu'en formulant son commentaire de soutien sur Facebook, elle avait involontairement divulgué des RPS et porté atteinte à la confidentialité. Elle a expliqué à la mère qu'elle ne pouvait pas parler d'une autre cliente. Elle se demande maintenant si elle avait bien fait d'accepter l'invitation à se joindre au groupe.

Elle a immédiatement supprimé son commentaire, quitté le groupe et suivi la politique de son employeur pour traiter l'atteinte à la confidentialité. En discutant de l'incident avec sa gestionnaire, les deux ont constaté que l'organisation ne disposait pas d'une politique sur l'utilisation sécuritaire des médias sociaux.

Éléments clés à considérer

- Relation avec une cliente qui s'étend aux médias sociaux personnels
- Communication informelle en dehors des canaux approuvés
- Visibilité publique des commentaires
- Transgression des limites
- Divulgaration de RPS

Utilisation de la liste de vérification pour la prise de décisions

Avant de se joindre au groupe Facebook et de répondre à la publication de la cliente, Julie aurait dû utiliser la liste de vérification pour la prise de décisions relatives aux technologies numériques.

RÉSULTAT DE LA LISTE DE VÉRIFICATION	Pourquoi les réponses sont « NON »
✗ Conformité ✗ Sécurité – Exactitude → sans objet ✗ Confidentialité ✗ Professionnalisme ✗ Caractère approprié ✗ Confiance du public	Cette action ne satisfait pas aux critères de la liste de vérification, car Julie a divulgué sans autorisation des renseignements sur le traitement et la prise de médicaments d'une cliente dans un groupe sur les médias sociaux. <i>La plateforme n'était ni approuvée ni appropriée pour les communications cliniques, la divulgation ne respectait pas la confidentialité et l'interaction outrepassait les limites professionnelles. Ce comportement pourrait également miner la confiance de la cliente ainsi que celle du public envers la profession infirmière.</i>
La réponse à une ou plusieurs questions est NON. ARRÊTEZ!	Résultat : Arrêtez. Ne communiquez aucun renseignement propre à la cliente par l'intermédiaire du groupe sur les médias sociaux. Signalez l'atteinte à la vie privée et prenez les mesures nécessaires pour y remédier.

Points d'apprentissage

Ce cas illustre que les bonnes intentions ne dégagent pas les II/IP de leur responsabilité de protéger la confidentialité et de maintenir les limites professionnelles. L'utilisation de la liste de vérification peut aider à cerner les risques avant de communiquer avec les clients sur les médias sociaux. En l'absence de directives organisationnelles, les II/IP devraient préconiser l'adoption de politiques claires sur l'utilisation des médias sociaux à des fins professionnelles.

Étude de cas 3 : Communications numériques sécurisées avec un client

Anne, une II travaillant dans une clinique communautaire, prépare le congé d'un client qui nécessite un suivi à la suite d'un changement de médicament. Le client demande de recevoir des rappels de rendez-vous et des consignes de suivi par message texte. Anne ne sait pas si l'utilisation de la plateforme de messagerie de la clinique est autorisée ni quelles sont les exigences applicables en matière de consentement, de tenue de dossiers et de délais de réponse.

Anne prend le temps de consulter la liste de vérification pour la prise de décisions relatives aux technologies numériques. Elle examine la politique de l'organisation avec sa gestionnaire et la personne responsable de la protection de la vie privée. Après avoir confirmé que l'utilisation du portail client sécurisé est autorisée, Anne obtient et consigne le consentement du client, vérifie ses coordonnées, lui explique à quel moment les messages seront consultés et comment accéder à des soins urgents, puis consigne les communications cliniquement pertinentes dans le dossier médical du client. Une fois qu'elle peut répondre « OUI » à toutes les questions applicables de la liste de vérification, Anne utilise le portail client sécurisé pour communiquer avec le client.

Éléments clés à considérer

- Autorisation et sécurité de la plateforme
- Consentement éclairé
- Vérification des coordonnées du client
- Attentes relatives aux délais de réponse
- Autres options pour obtenir des soins urgents
- Consignation des communications cliniques

Utilisation de la liste de vérification pour la prise de décisions

Avant de commencer à communiquer par voie électronique avec le client, Anne a utilisé la liste de vérification pour la prise de décisions relatives aux technologies numériques.

RÉSULTAT DE LA LISTE DE VÉRIFICATION ? Conformité ? Sécurité ? Exactitude ? Confidentialité ✓ Professionnalisme ? Caractère approprié ✓ Confiance du public Une ou plusieurs réponses aux questions applicables : « INCERTAINE » CONSULTEZ	Pourquoi les réponses initiales sont « INCERTAINE » Au départ, Anne ne peut confirmer si la plateforme de messagerie est autorisée et sécurisée ni quelles exigences s'appliquent en matière de consentement, de tenue de dossiers et de délais de réponse. Anne prend le temps d'examiner les politiques de l'organisation et de consulter sa gestionnaire ainsi que la personne responsable de la protection de la vie privée. Résultat initial : Prenez le temps de consulter. Demandez conseil avant de commencer à communiquer par voie électronique.
RÉSULTAT DE LA LISTE DE VÉRIFICATION ✓ Conformité ✓ Sécurité ✓ Exactitude ✓ Confidentialité ✓ Professionnalisme ✓ Caractère approprié ✓ Confiance du public Toutes les réponses aux questions applicables : « OUI » ALLEZ-Y	Pourquoi les réponses sont devenues « OUI » Après avoir confirmé que l'utilisation du portail client sécurisé est autorisée, obtenu et consigné le consentement éclairé du client, établi les attentes en matière de communication et expliqué comment accéder à des soins urgents, Anne peut répondre « OUI » à toutes les questions applicables de la liste de vérification. Résultat : Allez-y. Utilisez le portail client sécurisé autorisé.

Étude de cas 3 : Communications numériques sécurisées avec un client (suite)

Points d'apprentissage

Une réponse « INCERTAINE » ne signifie pas forcément que l'action est interdite. Elle signifie que l'II/IP devrait prendre le temps de cerner les renseignements manquants et d'obtenir les conseils appropriés. L'action peut être entreprise une fois les incertitudes levées et lorsqu'il est possible de répondre « OUI » à toutes les questions de la liste de vérification.

DRAFT



**Ordre de la pratique infirmière
du Nouveau-Brunswick**

590, rue Brunswick
Fredericton (Nouveau-Brunswick) E3B 1H5
Canada