



College of Nursing
of New Brunswick

Practice Guideline: **Safe Use of Digital Technologies**



Mandate

Public protection through regulation of nurses in New Brunswick

Under the *Nurses Act*, the College of Nursing of New Brunswick (CNNB) is legally responsible for protecting the public by regulating registrants of the nursing profession in New Brunswick. Regulation makes this profession, as well as individual registered nurses and nurse practitioners, responsible for safe, competent, compassionate and ethical nursing practice.

Acknowledgements

Some content within this guideline has been adapted from the Nova Scotia College of Nursing (NSCN), [Social Media Practice Guideline](#) (2025).

© College of Nursing of New Brunswick 2026.

Copyright © The College of Nursing of New Brunswick (CNNB), Fredericton, NB.

Commercial or for-profit redistribution of this document in part or in whole is prohibited except with the written consent of CNNB. This document may be reproduced in part or in whole for personal or educational use without permission, provided that:

- due diligence is exercised in ensuring the accuracy of the materials reproduced;
- CNNB is identified as the source; and
- the reproduction is not represented as an official version of the materials reproduced, nor as having been made in affiliation with, or with the endorsement of CNNB.

Table of Contents

Introduction.....	4
E-professionalism.....	4
Digital Technologies	5
Guiding Principles for Safe Use of Digital Technologies	5
Benefits of Digital Technologies	5
Risks of Digital Technologies	6
Key Considerations When Using Digital Technologies.....	7
Professional Responsibilities	7
Accountability.....	7
Professional Presence and Conduct.....	8
Confidentiality and Security	9
Professional Boundaries.....	9
Freedom of Expression.....	10
Appropriate Use of Specific Digital Technologies	11
Mobile Devices.....	11
Electronic Communications.....	11
Photos and Videos.....	12
Applications and Digital Tools	12
Social Media	13
Artificial Intelligence Tools.....	13
Telenursing Practice.....	14
Electronic Health Records and Documentation	14
Glossary	15
References	16
Appendix A: Tools to Support E-Professionalism and Safe Use of Digital Technologies	17
Appendix B: Applying the Digital Technology Decision Making Checklist into Practice	18

This practice guideline supports the application of relevant legislation, the [Code of Conduct for Registered Nurses and Nurse Practitioners](#) and the [standards of practice](#) in digital contexts. Failure to meet professional expectations when using digital technologies may result in regulatory action.

Introduction

[Digital technologies](#) are integrated into many areas of [nursing practice](#), including the expanding use of [artificial intelligence](#), widespread engagement with mobile devices, [social media](#) and other online platforms, and the growing reliance on [information and communication technology](#) in health care service delivery. While these tools can enhance communication, support decision-making, and improve efficiency, they also introduce risks related to [privacy](#), [confidentiality](#), e-professionalism, misinformation, and the blurring of [boundaries](#) (Booth et al., 2021; O'Connor et al., 2020).

This guideline applies to all RNs/NPs¹ who are practicing in New Brunswick or providing nursing services to clients located in New Brunswick. It applies across all practice settings and includes both employer-provided and personal technologies, whether used inside or outside the workplace, where there is a connection to the RN/NP professional role or identity.

E-professionalism

E-professionalism is the application of professional [values](#), behaviours, judgment, and regulatory expectations in digital environments (Makondo, 2026; Park & Kim, 2025). It includes accountability, consistency between online and in-person conduct, self-regulation, privacy and boundary management, reflective practice, and [digital literacy](#). Together, these attributes underpin [professional conduct](#) in digital environments.

E-professionalism is demonstrated when RNs/NPs:

- uphold respect, integrity, trust, and partnership in all digital interactions;
- take accountability for all digital actions and decisions;
- maintain a consistent professional presence online as they do in practice;
- engage in reflective practices regarding digital behaviour;
- protect privacy and confidentiality in all digital environments;
- maintain [professional boundaries](#); and
- develop and maintain digital competence to use technology safely and ethically.

¹ The CNNB is responsible for regulating registered nurses, graduate nurses, nurse practitioners and graduate nurse practitioners in New Brunswick, as such the abbreviation “RNs/NPs” is used in this document and refers to all aforementioned designations. Licensed practical nurses in New Brunswick are regulated by the Association of New Brunswick Licensed Practical Nurses.

Digital Technologies

Digital technologies include any electronic systems and tools used to communicate, document, store, or access information. Examples include: [digital health technologies](#), mobile devices, [applications](#), social media, online platforms, and [information and communication technologies](#) used in professional practice and everyday life.

Organizational policies may not apply to all personal uses of digital technologies. However, RNs/NPs remain accountable for meeting applicable professional, ethical, legal, and regulatory responsibilities whenever their digital conduct is connected to nursing practice, their professional role or identity, client safety, public protection, or public trust.

The following guiding principles support the application of e-professionalism in both professional and personal digital contexts.

Guiding Principles for Safe Use of Digital Technologies

- [Client safety](#) and public protection are the primary considerations in all digital interactions.
- RNs/NPs apply professional judgment and maintain the [competence](#) needed to use digital technologies safely.
- RNs/NPs protect privacy and maintain confidentiality in all digital contexts.
- RNs/NPs use digital technologies in accordance with applicable legislation, the Code of Conduct, practice standards and other regulatory requirements and organizational policies.
- Accountability remains with the RN/NP, regardless of the technology used.



The safe and [evidence-informed](#) use of digital technologies depends on RNs'/NPs' digital literacy, professional judgment, and commitment to applying these tools in ways that protect the public, support quality practice, and uphold e-professionalism.

Benefits of Digital Technologies

Digital technologies can enhance the delivery of safe and effective nursing practice. When selected and used appropriately, digital technologies may improve access to information and services, enhance communication and collaboration, support clinical decision-making, support education, simulation, research, and quality improvement, and improve workflow efficiency (Ventola, 2014).

Risks of Digital Technologies

Digital technologies introduce risks that can affect client safety, privacy and confidentiality, and professional integrity. RNs/NPs recognize these risks and apply professional judgment and digital literacy when using digital technologies (Ventola, 2014).

- *Privacy breaches²* – Digital technologies can expose **personal health information (PHI)**³ through unsecured devices, networks, or applications. Risks include unauthorized access, accidental disclosure (e.g., misdirected texts/emails, screenshots showing client information), and use of platforms that do not meet legislative or organizational requirements.
- *Misinformation and inaccurate data* – Information shared or accessed digitally may be incomplete, outdated, or inaccurate. Clients may misinterpret digital advice, and decision-support tools may contain errors or biases that influence clinical decision-making.
- *Boundary violations* – Digital communication, particularly through personal devices or social media, can blur professional boundaries. Tone and intent may be misinterpreted, and online interactions may create the perception of a personal relationship.
- *Reputational harm* – Online behaviour, whether personal or professional, can impact public trust. Digital content may remain accessible, searchable, reproducible, or recoverable after it is posted or deleted. It may also be copied, altered, or redistributed without the author's knowledge or consent. Association with misinformation or inappropriate content can undermine credibility.
- *Security vulnerabilities* – Cyberattacks, phishing, malware, and device loss or theft can compromise sensitive information. Using unapproved apps or cloud-based tools increases the risk of breaches and system vulnerabilities.
- *Inequitable access to care* – Not all clients have equal access to technology, reliable internet access, or digital literacy. Overreliance on digital technologies may disadvantage individuals with limited resources, language barriers, or accessibility needs.

² For additional information on privacy breaches, consult [CNNB's Fact Sheet: How Much Do You Know About Privacy Breaches?](#) and consult [CNNB's Practice Guideline: Privacy and Confidentiality](#)

³ For additional information on legislation of PHI, please refer to the [Personal Health Information Privacy and Access Act](#)

Key Considerations When Using Digital Technologies

- Offering guidance outside an established [nurse-client relationship](#) may establish professional responsibilities such as a [duty to provide care](#)⁴, expose the RN/NP to liability, or constitute practicing outside the jurisdiction in which the RN/NP is authorized.
- Breaches of confidentiality, inaccurate advice, failure to meet professional expectations, or unauthorized practice may result in organizational, regulatory, or legal consequences.
- Digital content may be retained, copied, redistributed, altered, or accessed beyond the intended audience, regardless of privacy settings.



When uncertain, pause and seek guidance before proceeding.

To support the application of this guideline in practice, [Appendix A](#) provides a Digital Technology Decision-Making Checklist. [Appendix B](#) provides case studies that illustrate how the checklist can be used to analyze situations involving digital technologies and support safe, ethical, and professional nursing practice.

Professional Responsibilities

E-professionalism requires RNs/NPs to apply their professional responsibilities when using digital technologies. These responsibilities may extend to personal digital conduct, where there may be an impact on client safety, public protection, professional integrity, or public trust.

Accountability

RNs/NPs remain accountable for all decisions and actions involving digital technologies. Consistent with the principle of [professional accountability](#), RNs/NPs are responsible for ensuring that digital technologies support, rather than replace, clinical judgment. This accountability includes understanding the capabilities, limitations, and risks associated with the technologies used.

⁴ For additional information on duty to provide care, consult [CNNB's Practice Guideline: Duty to Provide Care](#)

Professional accountability in digital environments includes:

- using technologies in accordance with applicable legislation, regulatory requirements, and organizational policies;
- advocating for the development of organizational policies when guidance for digital technology use is lacking;
- verifying the accuracy, reliability, and appropriateness of information obtained or generated through digital technologies;
- understanding the capabilities, limitations, and risks of digital technologies;
- recognizing that personal and professional online activities can have professional consequences;
- maintaining competence in the safe use of digital technologies and seeking guidance when unfamiliar situations, risks, or limitations are identified; and
- documenting relevant information exchanged through digital communications in accordance with CNNB's [Standards for Documentation](#) and organizational policies.

Professional Presence and Conduct

Professional presence⁵ includes awareness of how an RN's/NP's conduct may be perceived by clients, colleagues, the [health care team](#), the regulatory body, and the public. This expectation extends to online activities and digital communications, where the same professional standards apply.

Professional presence in digital environments is demonstrated by:

- communicating respectfully, professionally, and ethically;
- avoiding posting or sharing content that could undermine public trust in the profession;
- maintaining appropriate boundaries with clients and colleagues;
- not providing individualized nursing or health advice through social media or other public⁶ or non-secure⁷ digital environments; and
- avoiding situations that may cause a [conflict of interest](#)⁸.



Statements made online may be interpreted as representing an employer or the profession, even when posted anonymously, under a pseudonym, or through a personal account.

⁵ For additional information on professional presence, consult [CNNB's Fact Sheet: Professional Presence](#).

⁶ Public digital environment is a digital space in which content is accessible or visible to a broad or undefined audience. Examples include public websites, social media, blogs and online forums. A digital environment should not be assumed to be private based solely on account or privacy settings.

⁷ Non-secure digital environment is a public or private space, platform, application, device, or system that is not authorized for the intended purpose or does not have the privacy and security safeguards required for the information or activity involved.

⁸ For additional information on conflicts of interest, consult [CNNB's Practice Guideline: Conflict of Interest](#).

Confidentiality and Security

RNs/NPs must use authorized technologies and take reasonable safeguards to protect information against unauthorized access, use, disclosure, loss, alteration, or destruction. They must recognize and report suspected privacy or security incidents in accordance with applicable requirements and organizational policies.

Protecting privacy, confidentiality, and information security includes:

- using only organization-approved platforms to communicate PHI;
- ensuring devices are password-protected, secure, and encrypted, as appropriate;
- using a personal device to access, collect, capture, store, or transmit PHI only when this is authorized and appropriate safeguards are in place; and
- recognizing and responding appropriately to potential security risks and reporting security incidents in accordance with organizational policies.



RNs/NPs share client information only through authorized and secure platforms appropriate to the purpose. De-identification or client consent does not, on its own, eliminate privacy and confidentiality risks.

Professional Boundaries

Professional boundaries apply equally in digital and in-person interactions. Online conduct, whether intentional or unintentional, may affect the nurse-client relationship⁹.

Maintaining professional boundaries in digital environments includes:

- avoiding personal online interactions with current clients and their families, and carefully considering interactions with former clients where a power imbalance, vulnerability, or residual therapeutic relationship may remain;
- keeping personal and professional communications separate;
- recognizing and managing situations where personal and professional roles overlap;
- establishing and communicating clear limits for digital communication with clients; and
- avoiding online content or conduct that could compromise the nurse-client relationship or public trust in the profession.



Before connecting or communicating online, consider the purpose of the interaction and its potential impact on the client, professional boundaries, and the nurse-client relationship.

⁹ For additional information on professional boundaries, consult [CNNB's Standards for the Nurse-Client Relationship](#)

Freedom of Expression

The [Canadian Charter of Rights and Freedoms](#) protects freedom of thought, belief, opinion, and expression, including through digital and other media. This freedom is not absolute and may be subject to reasonable limits prescribed by law (Rosen Sunshine LLP, 2023). RNs/NPs are responsible for considering how their public or digital expression may affect client safety, privacy and confidentiality, professional integrity, and public trust (Nova Scotia College of Nursing, 2025).

Applying professional judgment when expressing views in public or digital environments includes:

- protecting privacy and confidentiality, including not disclosing PHI;
- communicating in a manner that maintains public trust in the nursing profession;
- complying with applicable legislation, regulatory requirements, and organizational policies;
- not communicating misinformation or disinformation¹⁰ that may affect client safety or public protection;
- clearly distinguishing personal views from those of an employer, organization, regulatory body, or the nursing profession;
- considering the potential impact of digital expression on professional credibility and therapeutic relationships; and
- expressing personal views in a manner consistent with professional, ethical, and legal responsibilities.



Freedom of expression does not remove an RN's/NP's professional responsibilities.

¹⁰ For additional information on misinformation/disinformation, consult [CNNB's Fact Sheet: Misinformation and Disinformation](#)

Appropriate Use of Specific Digital Technologies

Digital technologies are used in various ways across nursing practice. Although each technology presents distinct opportunities, limitations, and risks, the professional, ethical, legal, and regulatory responsibilities of RNs/NPs remain the same. The following considerations support the safe, effective, and appropriate use of commonly used digital technologies in professional practice.

The professional responsibilities described earlier in this guideline apply to every digital technology. The following sections identify additional considerations associated with particular technologies.

Examples are provided for illustrative purposes only. CNNB does not endorse, recommend, or promote any specific product, platform, application, system, or technology.



Self-employed RNs/NPs are responsible for establishing the policies and safeguards needed to support the safe use of digital technologies in their practice.

Mobile Devices

When using mobile devices in professional practice, RNs/NPs:

- use mobile devices responsibly and in accordance with organizational policies;
- ensure device use does not compromise client safety, privacy, confidentiality, or professional responsibilities;
- use personal devices for professional purposes only when authorized and when required privacy and security safeguards are in place;
- minimize distractions and ensure device use does not interfere with safe care or therapeutic communication; and
- consider the legal, ethical, and professional risks associated with mobile device use.

For information about legal considerations, consult the following Canadian Nurses Protective Society (CNPS) resources:

- [InfoLAW: Mobile Devices in the Workplace](#)
- [Legal case study: Distraction by cell phone](#)

Electronic Communications

When using electronic communications (e.g., email, text messaging) for professional communication, RNs/NPs:

- use secure communication platforms that are authorized by the organization and appropriate for the nature and purpose of the communication;

- ensure PHI is shared only with authorized individuals and only to the minimum amount necessary for the identified purpose;
- obtain and document informed consent for electronic communications¹¹;
- communicate clearly, accurately, professionally, and in a manner appropriate to the context;
- recognize that messaging platforms may present risks related to privacy, confidentiality, and miscommunication;
- establish and communicate expectations for digital communication, including its purpose, appropriate use, when messages are monitored and the expected response time, and alternative options for accessing care when the RN/NP is unavailable;
- verify the identity of the intended recipient before transmitting client information and verify the sender/client identity where clinically relevant; and
- document relevant exchanges in accordance with CNNB's [Standards for Documentation](#) and organizational policies.

For information about legal considerations, consult the following CNPS resources:

- [Ask a lawyer: Texting updates to other health professionals](#)
- [InfoLAW: Legal Risks of Email - Part 1: Privacy Concerns](#)
- [InfoLAW: Legal Risks of Email - Part 2: Practical Considerations](#)

Photos and Videos

When capturing, storing, or sharing photos or videos as part of professional practice, RNs/NPs:

- obtain and document informed consent and any other authorization required by legislation or organizational policy;
- use authorized devices and platforms in accordance with organizational policies;
- protect privacy and confidentiality of clients depicted or otherwise identifiable in photos and videos throughout collection, access, use, storage, transmission, retention, and secure disposal;
- ensure photos and videos are used only for legitimate clinical, educational, or organizational purposes with appropriate authorization; and
- consider whether a photo or video is necessary before capturing it.

Applications and Digital Tools

When using applications and other digital tools, RNs/NPs:

- use applications and tools from reliable and evidence-informed sources;
- verify the accuracy and appropriateness of information obtained or generated;
- use organization-approved applications and tools;
- recognize that digital technologies support but do not replace professional judgment;
- review and apply appropriate privacy and security settings;
- do not enter identifiable PHI into public or non-secure applications or systems; and
- recommend only applications and tools that are appropriate, reliable, and consistent with organizational requirements.

¹¹ RNs/NPs may refer to the CNPS [Template Form: Consent to use electronic communications](#) to support consent documentation.

For information about legal considerations, consult the following CNPS resources:

- [InfoLAW: Mobile Healthcare Apps](#)

Social Media

When using social media, RNs/NPs:

- do not post or share information, images, or other content that identifies a client or could reasonably allow a client to be identified, even when direct identifiers have been removed;
- maintain professional conduct and uphold public trust in the profession;
- use professional titles and designations accurately and in accordance with regulatory requirements;
- do not initiate or accept personal social-media connections with current clients, and carefully assess any proposed connection with a former client in accordance with professional-boundary expectations; and
- recognize that content shared online may be permanent, searchable, and redistributed beyond the original audience.

For information about legal considerations, consult the following CNPS resources:

- [InfoLAW: Social Media](#)
- [Ask a lawyer: Social media](#)

Artificial Intelligence Tools

When using artificial intelligence (AI) in professional practice, RNs/NPs:

- use only AI tools authorized for the intended purpose;
- protect privacy and confidentiality and do not enter PHI into public or non-secure AI tools;
- understand the tool's intended purpose, capabilities, limitations, and risks;
- independently verify AI-generated information for accuracy, reliability, appropriateness, and potential bias;
- apply critical thinking and clinical expertise when interpreting or acting on AI-generated content;
- meet applicable transparency, informed consent, and documentation requirements when AI is used in client care;
- remain accountable for AI-supported decisions, actions, communications, and documentation; and
- apply the expectations and guidance set out in CNNB's [Fact Sheet: Artificial Intelligence](#).

For information about legal considerations, consult the following CNPS resources:

- [Artificial Intelligence in Healthcare: Legal Risk Management Considerations in Nursing Practice](#)



AI supports, but does not replace, nursing knowledge, judgment, accountability, or the therapeutic relationship. RNs/NPs must review and validate AI-generated information before using it in practice.

Telenursing Practice

When providing care through telenursing technologies, RNs/NPs:

- meet the same standards of practice that apply to in-person care;
- ensure the technology is appropriate, secure, and capable of supporting safe care;
- assess client suitability and address consent, identity verification, privacy, confidentiality, security, and documentation requirements;
- determine and meet the registration, legal, regulatory, liability, and organizational requirements that apply in each relevant jurisdiction; and
- follow CNNB's [*Practice Guideline: Telenursing Practice*](#).

For information about legal considerations, consult the following CNPS resources:

- [*InfoLAW: Telepractice*](#)
- [*Twelve Things to Consider Before Joining a Virtual Care Practice*](#)

Electronic Health Records and Documentation

When accessing or documenting in electronic health records (EHRs), RNs/NPs:

- access a client's health record only when authorized, for a legitimate professional purpose, and only to the extent necessary for that purpose;
- protect login credentials and use secure access methods;
- lock the screen or log out before leaving an EHR or device unattended;
- comply with privacy, confidentiality, and information security requirements;
- comply with organizational requirements for EHR access, use, and information management; and
- recognize that EHR access and activity may be monitored and audited.

For information about legal considerations, consult the following CNPS resources:

- [*InfoLAW: Privacy and Electronic Medical Records*](#)
- [*Ask a Lawyer: Electronic Medical Records and Independent Practice*](#)
- [*Ask a Lawyer: Documentation of Late Entries*](#)
- [*InfoLAW: Quality Documentation: Your Best Defence - Canadian Nurses Protective Society*](#)

Glossary

Please note: The glossary below contains proposed new and revised terms that are not yet included in the CNNB online glossary. These definitions are being circulated as part of the external consultation process and are subject to revision prior to publication.

Applications (Apps)

A software program that performs a specific function that is used on a computer or mobile device.

Artificial Intelligence (AI)

AI broadly refers to computer programs performing tasks historically undertaken by human intelligence. AI is computer code that carries out rapid analysis and evaluation of data, similar to human intelligence processes, such as reasoning, decision-making, or learning from prior experiences. These processes result in outputs such as written information, robots performing tasks, pictures, predictions based on historical data, or other outputs.

Digital health technologies

Are information and communication tools, systems, and services used to collect, store, exchange, and analyze health information to support the delivery, coordination, and evaluation of care. In nursing practice, their use is guided by professional and ethical obligations to protect privacy, maintain confidentiality, ensure informed consent, and uphold safe, competent, and compassionate care.

Digital literacy

The knowledge, skills and judgment required to access, evaluate, understand and use digital technologies safely, effectively, and ethically. It includes recognizing the benefits, limitations, risks, reliability, and appropriate use of digital tools and information.

Digital technologies

Electronic systems, devices, applications, platforms, and tools used to create, collect, access, store, process, share, transmit, or manage information. In nursing practice, digital technologies may be used for communication, documentation, education, decision-making, care delivery, administration, research, and other professional or personal purposes. Their use requires the application of professional judgment, digital literacy, and applicable ethical, legal, regulatory, and organizational requirements.

References

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

Makondo, C. (2026). Digital professionalism: Maintaining professional standards when using digital messaging platforms. *Nursing Standard*, 41(5), 47–54. (193502385). <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., Chu, C. H., Thilo, F., Lee, J. J., Mather, C., & Topaz, M. (2020). Professionalism in a digital and mobile world: A way forward for nursing. *Journal of Advanced Nursing*, 76(1), 4–6. <https://doi.org/10.1111/jan.14224>

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

Rosen Sunshine LLP. (2023). Peterson v. College of Psychologists of Ontario [Law Firm]. *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*, 39(7), 491–520.

Appendix A: Tools to Support E-Professionalism and Safe Use of Digital Technologies

Digital Technology Decision-Making Checklist

Before you...

- | | | | |
|---|--|--|---|
|  Send a text/email |  Take/share a photo/video |  Use AI tools |  Use a mobile device for work purposes |
|  Access an EHR |  Post/share on social media |  Provide virtual care | |

Take a **PAUSE** and **ASK YOURSELF**:

- ☐ **Compliant** - Does this comply with legislation, organizational policies, and regulatory standards?
- ☐ **Secure** - Is this platform secure and appropriate for the identified purpose?
- ☐ **Accurate** - Is the information accurate and evidence-informed?
- ☐ **Confidential** - Am I sharing PHI or other confidential information only when authorized, for clinical or other authorized professional purposes, and through secure channels?
- ☐ **Professional** - Is this within my professional role, boundaries, and scope?
- ☐ **Appropriate** - Is my use or action appropriate and respectful?
- ☐ **Public Trust** - Will this action maintain public trust in the nursing profession?

PROCEED

If all applicable answers = YES

Proceed while continuing to apply professional judgment and monitor for changing risks.

CONSULT

If UNSURE about one or more answers

Pause; review policies, legislation, and seek guidance (leadership/[CNPS](#)/[CNNB](#)).

STOP!

If one or more answers = NO

Do not proceed; address the concerns and seek guidance before continuing.

Quick Accountability Check

- ✓ Would I be comfortable explaining this action to my employer?
- ✓ Would I be comfortable documenting this action in the client health record?
- ✓ Would I be comfortable if this action were reviewed by my employer, CNNB, or in a legal proceeding?

Key Reminders

- Protect privacy, confidentiality, and PHI.
- Apply professional judgment.
- Verify accuracy of digital information.
- Use secure and authorized technologies.
- Follow legislation, policies, and standards.
- Maintain professional boundaries.
- Document relevant information.
- Remain professionally accountable.



Digital conduct that compromises client privacy, professional integrity, or public trust may result in regulatory action.



Digital content may remain permanent, searchable, and shareable regardless of privacy settings. It can be copied, altered, or shared without your knowledge or consent.

WHEN IN DOUBT, PAUSE and seek guidance before proceeding!

Appendix B: Applying the Digital Technology Decision Making Checklist into Practice

Note: Our case studies are fictional educational resources. While we strive to make the scenarios as realistic as possible, any resemblance to actual people or events is coincidental.

Case Study 1: Taking and Sharing a Client Photo

John, an emergency department RN, uses his cell phone to take a photo of a client receiving care after a car accident. The photo is not required for the client's care or another authorized clinical purpose. John did not obtain the client's informed consent or authorization to take or share the photo.

John sends the photo to colleagues through a group chat, describing the client's injuries, and proceeds to discuss the accident. The discussion is unrelated to providing or coordinating care, and the messaging application is not an approved clinical communication system. Although the client's name is not included, the photo and accompanying details could allow the client to be identified. Once shared, John can no longer control whether the photo or messages are saved, copied, altered or redistributed beyond the intended recipients.

Key considerations

- Taking a client photo without clinical purpose
- Using personal device to store/share PHI
- Discussing PHI for a purpose unrelated to care
- Lack of consent or appropriate authorization
- Sharing outside approved and secured system
- Potential identification through shared details

Applying the Decision-Making Checklist

Before taking or sharing the photo, John should have applied the Decision-Making Checklist. For example:

CHECKLIST RESULT	
❌ Compliant ❌ Secure – Accurate → not applicable ❌ Confidential ❌ Professional ❌ Appropriate ❌ Public trust One or more answers = NO STOP!	Why the answers are “NO” <i>The action does not meet the checklist because the photo and related client information were captured and shared for a non-clinical purpose, without appropriate consent or authorization, and through an unapproved personal device and messaging application. The disclosure was not required for care, did not protect privacy or confidentiality, and was inconsistent with professional responsibilities, organizational policies, and public trust.</i> Outcome: Stop. Do not take or share the photo

Learning Points

This scenario demonstrates why the tool requires all YES answers to applicable questions before proceeding; client information may only be captured, accessed, used, stored, or shared through an approved, secure method with appropriate authorization in place. Omitting the client's name, limiting distribution to colleagues, or obtaining consent does not, on its own, make the purpose, device, platform, or disclosure appropriate.

Case Study 2: Confidentiality Breach in a Facebook Group

Ella, RN, joined a Facebook group created by young mothers she works with. She was concerned when Kim, a client of hers, posted she was having a rough time and feeling very low. Ella, trying to be supportive, commented, “I know last week was difficult. Are you still on your meds? Why don’t you drop in tomorrow and we can talk?”

After work, another mom stopped Ella in the grocery store and said, “I didn’t know Kim was on meds!” Ella was horrified to realize that her supportive comment on Facebook unintentionally disclosed PHI and violated confidentiality. She told the mom that she could not speak about another client. She now questions whether she should have accepted the invitation to join the group.

She immediately deleted her comment, removed herself from the group, and followed her employer’s policy to address the breach of confidentiality. When speaking with her manager about the incident, they noticed the organization did not have a policy on safe social media use.

Key considerations

- Client relationship extending into personal social media
- Public visibility of comments
- Disclosure of PHI
- Informal communication outside approved channels
- Boundary crossing

Applying the Decision-Making Checklist

Before joining the Facebook group and responding to the client’s post, Ella should have applied the Digital Technology Decision-Making Checklist.

CHECKLIST RESULT	Why the answers are “NO”
❌ Compliant ❌ Secure – Accurate → not applicable ❌ Confidential ❌ Professional ❌ Appropriate ❌ Public trust	<i>The action does not meet the checklist because Ella disclosed client-specific treatment and medication information without authorization in a social media group. The platform was not approved or appropriate for clinical communication, the disclosure did not protect confidentiality, and the interaction crossed professional boundaries. The conduct could also undermine the client’s trust and public trust in the nursing profession.</i>
One or more answers = NO STOP!	Outcome: Stop. Do not communicate client-specific information through the social media group. Report and address the privacy breach.

Learning Points

This case illustrates that good intentions do not remove an RN’s/NP’s responsibility to protect confidentiality and maintain professional boundaries. Applying the checklist may help identify risks before communicating with clients on social media. Where organizational guidance is lacking, the RN/NP should advocate for clear policies on professional social media use.

Case Study 3: Secure Digital Communication with a Client

Anna, an RN in a community clinic, is preparing to discharge a client who requires follow-up after a medication change. The client asks to receive appointment reminders and follow-up instructions by text message. Anna is unsure whether the clinic's messaging platform is authorized or what consent, documentation, and response-time requirements apply.

Anna pauses and applies the Digital Technology Decision-Making Checklist. She reviews the organizational policy with her manager and privacy officer. After confirming that the secure client portal is authorized, Anna obtains and documents the client's consent, verifies the client's contact information, explains when messages will be reviewed and how to access urgent care, and documents clinically relevant communication in the client's health record. Once all applicable checklist questions can be answered "YES," Anna proceeds using the secure client portal.

Key considerations

- Authorization and security of the platform
- Informed consent
- Verification of client contact information
- Expectations for response times
- Alternative options for urgent care
- Documentation of clinical communication

Applying the Decision-Making Checklist

Before beginning electronic communication with the client, Anna applied the Digital Technology Decision-Making Checklist.

CHECKLIST RESULT ? Compliant ? Secure ? Accurate ? Confidential ✓ Professional ? Appropriate ✓ Public trust one or more applicable answers = UNSURE CONSULT	Why the initial answers are "UNSURE" <i>Anna initially cannot confirm whether the messaging platform is authorized and secure or what consent, documentation, and response-time requirements apply. Anna pauses, reviews organizational policies, and consults the manager and privacy officer.</i> Initial outcome: Pause and consult. Seek guidance before beginning electronic communication.
CHECKLIST RESULT ✓ Compliant ✓ Secure ✓ Accurate ✓ Confidential ✓ Professional ✓ Appropriate ✓ Public trust All applicable answers = YES PROCEED	Why the answers became "YES" <i>After confirming that the secure client portal is authorized, obtaining and documenting informed consent, establishing communication expectations, and explaining how to access urgent care, all applicable checklist questions can be answered YES.</i> Outcome: Proceed. Using the authorized secure client portal.

Learning Points

An "UNSURE" answer does not necessarily mean that an action is prohibited. It means the RN/NP should pause, identify the missing information, and seek appropriate guidance. The action may proceed when the uncertainty has been resolved and all checklist questions can be answered "YES".



**College of Nursing
of New Brunswick**

590 Brunswick St.
Fredericton, New Brunswick
Canada E3B 1H5