ELECTRONIC HEALTHCARE LAW REVIEW

General Editor: Domenic A. Crolla, Gowling Lafleur Henderson LLP, Ottawa

VOLUME 4, NUMBER 1 Cited as (2013-14) 3 Electronic Healthcare Law Review AUGUST 2014

• ONTARIO COURT CONFIRMS THAT *PHIPA* DOES NOT PRECLUDE BREACH OF PRIVACY CLAIM •

Erica M. Stone

On January 31, 2014, the Ontario Superior Court of Justice (the "Court") held in *Hopkins v. Kay* [*Hopkins*][1] that the *Personal Health Information Protection Act, 2004* [*PHIPA*][2] did not preclude a class action concerning unauthorized access to personal health information from proceeding on the basis of the tort of intrusion upon seclusion. The Court found that even though *PHIPA* applied to the breaches in question, it did not entirely "occupy the field" so as to prevent the plaintiffs from making a claim based on the common law tort.

The Court's decision is noteworthy because it expands upon a recent decision of the Ontario Court of Appeal in *Jones v. Tsige* [*Jones*][3] in which the tort of intrusion upon seclusion (also known as breach of privacy) was first formally recognized as an actionable claim in Ontario. In *Jones*, the privacy breach concerned personal banking information to which federal privacy legislation was applicable. *Hopkins* is the first Ontario case to apply the ruling in *Jones* to breaches of personal health information governed by *PHIPA*.

Background

Between 2011 and 2012, approximately 280 medical records of the Peterborough Regional Health Centre (the "Hospital") were unlawfully accessed and disclosed to third parties without patient consent. The Hospital apologized for the privacy breaches, and the individual defendants

• In This Issue •

LexisNexis

Electronic Healthcare Law Review

Electronic Healthcare Law Review is published quarterly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Markham, Ontario L3T 7W8

ISBN: 0-433-46965-X
ISBN: 0-433-46967-6 (Print & PDF)
ISBN: 0-433-46969-2 (PDF)
Subscription rates: $220 per year (print or PDF)
$280 per year (print & PDF)

Please address all editorial inquiries to:

Boris Roginsky
LexisNexis Canada Inc.
Tel. (905) 479-2665; Toll-Free Tel. 1-800-668-6481
Fax (905) 479-2826 Toll-Free Fax 1-800-461-3275
Internet e-mail: ehlr@lexisnexis.ca.

who improperly accessed the records were dismissed.

The plaintiffs originally issued a statement of claim pleading several causes of action, including breach of *PHIPA*. The pleading was later amended, and at the hearing, the only claim before the Court was the tort of intrusion upon seclusion. The plaintiffs alleged psychological injury resulting from the privacy breach and also sought punitive and aggravated damages.

Decision in *Hopkins*

Justice Edwards was asked to rule on the Hospital's motion to strike the statement of claim on the basis that it disclosed no reasonable cause of action and was not a matter within the jurisdiction of the Court. The motion was dismissed on the grounds that it was not "plain and obvious" that the claim for breach of privacy would fail.

In coming to his decision, Edwards J. first reviewed the limitations of a claim for damages under *PHIPA*. *PHIPA* permits claimants to seek damages only if an order has first been made by the Information and Privacy Commissioner or if a person has first been convicted of an offence under *PHIPA*, and that order or conviction is final as a result of there being no further right of appeal.[4] Furthermore, damages may be sought only for "actual harm" suffered, thus presumably excluding future damages.[5] Damages for "mental anguish" suffered by claimants from the wilful and reckless contravention or offence are capped at $10,000.[6]

Justice Edwards compared the broader remedy provided by a breach of privacy claim as set out by the Court of Appeal in *Jones*. Proof of actual

pecuniary loss is not a required element of the cause of action for breach of privacy. In addition, the Court of Appeal held that non-pecuniary damages can go as high as $20,000. Claims for aggravated and punitive damages were also deemed compensable, although reserved for exceptional cases.

The Court in *Hopkins* next reviewed British Columbia and Alberta case law in which the relevant privacy statute was found to have created a comprehensive legislative scheme that precluded the plaintiff from pursuing a separate claim in tort for breach of privacy. Justice Edwards remarked that the Court in *Jones* was not referred to this jurisprudence. He held that despite this case law he was nonetheless bound to follow *Jones*, which confirmed the existence of a right of action for intrusion upon seclusion after referencing federal and provincial privacy legislation.

However, Edwards J. left the door open for an appeal of his decision. He noted the Hospital's argument that *Jones* was distinguishable because it concerned different facts and different legislation. Justice Edwards declared that the Hospital's position could be upheld only if the Court of Appeal were to render a decision like the British Columbia Court of Appeal[7] and determine that there is no claim for breach of privacy and that the claim must be based on the legislative scheme in *PHIPA*.[8] Given this encouragement for the parties to resolve the issue at the appellate level, it is not surprising that the decision of Edwards J. in *Hopkins* has been appealed to the Ontario Court of Appeal.

Could *Jones* Be Distinguished on Appeal?

The appeal in *Hopkins* will require a close examination of the *Jones* decision to determine its application to a claim for breach of privacy when *PHIPA* is applicable to the facts and provides an adequate remedy. It should be noted that in *Jones* the Court of Appeal was careful to state that its reasons were limited to the facts of the case before it. The Court said that it should restrict itself "to the particular issues posed by the facts of the case before us and not attempt to decide more than is strictly necessary to decide that case".[9]

The Court of Appeal in *Jones* made passing reference to *PHIPA* and held generally that existing federal and provincial privacy legislation did not prevent it from recognizing the tort of intrusion upon seclusion. However, it did not specifically address whether the cause of action was available in a case where the statutory privacy regime provides a suitable remedy for the breach. It is, therefore, arguable that the specific issue in *Hopkins* was not addressed and that *Jones* might be distinguishable on that basis.

The primary reason given by the Court of Appeal in *Jones* for permitting the plaintiff to pursue a claim for breach of privacy was its concern that the plaintiff would not otherwise have the remedy she sought if she were not allowed to pursue the common law claim. Unlike some other common law provinces,[10] Ontario does not have a *Privacy Act* that creates a statutory tort of invasion of privacy applicable to private individuals. In *Jones*, this was

an important factor, because the plaintiff wanted to pursue a co-worker at the Bank of Montreal who was in a relationship with the plaintiff's ex-husband and who had deliberately accessed her bank records on at least 174 occasions.

Further, the Court held that federal privacy legislation applicable to those records[11] did not provide her with an adequate remedy.[12] The primary reason given was that *PIPEDA* allowed the plaintiff to file a complaint against only the Bank, her current employer, whereas she wanted to pursue only the individual employee who perpetrated the invasion of privacy. Moreover, since the employee had acted in violation of the employer's policies, this would have provided the employer with a defense to any *PIPEDA* complaint made against it. The Court also held that the plaintiff could not obtain damages under *PIPEDA* for the harm caused.[13]

There is a good argument that the facts in *Hopkins* present a different scenario. First, Edwards J. acknowledged that *PHIPA* permits the plaintiffs to obtain damages albeit more limited than under the common law. Therefore, the plaintiffs would not be entirely without a monetary remedy if required to pursue a complaint under *PHIPA*. Second, unlike *Jones*, the plaintiffs have named as a defendant the same entity that is custodian of the records under *PHIPA* (the Hospital). As such, a remedy is available under *PHIPA* with respect to that defendant. The *Jones* decision might, therefore, be distinguished on the grounds that *PHIPA* provides the plaintiffs with an adequate remedy for the breach of privacy of their personal health information and that there is no deficiency in the law that needs to be addressed by the common law.[14]

It is also noteworthy that a special status has been attributed by the courts to privacy legislation. The Supreme Court of Canada has affirmed as follows:

> The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society [emphasis added].[15]

It is arguable that this quasi-constitutional character of privacy legislation requires courts to give it broad interpretation and to have serious and compelling reasons for displacing it in favour of the common law in cases in which the privacy statute provides a suitable remedy.

Conclusion

Both Justice Edwards in *Hopkins* and the Court of Appeal in *Jones* remarked on the ease with which access can be obtained to electronic information. It seems apparent that a motivating factor for the decision to allow a breach of privacy claim in both cases was to ensure that the law provides an appropriate remedy to respond to the threats to privacy posed by new technology.

It will be interesting to see how the Court of Appeal decides the *Hopkins* appeal after being presented with a different fact scenario and with case law from across Canada that was not reviewed in *Jones*. There are strong grounds for the Court to distinguish *Jones* on its facts and to require the plaintiffs to pursue a remedy under

PHIPA. The Court could well find that the cases are sufficiently factually dissimilar and that *PHIPA* creates a comprehensive and adequate scheme to address the privacy concerns at issue.

It will also be interesting to see whether and how the Court addresses the issue of deference to the legislature and the quasi-constitutional nature of privacy legislation. These principles may, at a minimum, require the Court to narrow the application of the tort if it finds the remedy available under *PHIPA* as insufficient to provide adequate justice in the case and if it allows the common law claim to proceed. In any event, if the class action in *Hopkins* is allowed to proceed, we may well see a marked increase in the number of breach of privacy claims in Ontario by plaintiffs who prefer the remedy available at common law over that obtainable under *PHIPA*.

[*Editor's Note*: **Erica M. Stone, LL.B., B.C.L., B.A. (Psych.)**, is a legal consultant in the areas of health law, professional regulation, and privacy law. She is a member of the Bars of Ontario, Quebec, and British Columbia.]

1 *Hopkins*, [2014] O.J. No. 485, 2014 ONSC 321, 119 O.R. (3d) 251.
2 *PHIPA*, S.O. 2004, c. 3, Schedule A.
3 [2012] O.J. No. 148, 2012 ONCA 32, 108 O.R. (3d) 241.
4 *Supra* note 2, ss. 65(1)–(2).
5 F. Dimitriadis, M. Orr, and H. Perun, *Guide to the Ontario Personal Health Information Protection Act* (Toronto: Irwin Law, 2005), 585.
6 *Supra* note 2, s. 65(3).
7 *Mohl v. University of British Columbia*, [2009] B.C.J. No. 1096, 2009 BCCA 249 (leave to appeal to S.C.C., [2009] S.C.C.A. No. 340, denied).
8 *Supra* note 1, para. 30.
9 *Supra* note 3, para. 21.
10 See, *e.g.*, *Privacy Act* of British Columbia, R.S.B.C. 1996, c. 373, *The Privacy Act* of Manitoba, C.C.S.M. c. P125, The Privacy Act of Saskatchewan, R.S.S. 1978, c. P-24, and *Privacy Act* of Newfoundland and Labrador, R.S.N.L. 1990, c. P-22.
11 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.
12 *Supra* note 3, para. 50.
13 The Court omitted reference to s. 16(c) *PIPEDA*, which permits a court to award non-pecuniary damages on judicial review of a Commissioner's decision. See M. Lapner and C. Armstrong, "The Tort of Invasion of Privacy in Ontario", *Ontario Bar Association Health Law Section Newsletter*, 2013.
14 *Supra* note 3, para. 69.
15 *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, [2013] S.C.J. No. 62, 2013 SCC 62, [2013] 3 S.C.R. 733, para. 19.

• SOCIAL MEDIA—HEALTHCARE LAW AND ETHICAL ISSUES •

Paul R. DeMuro, *Special Counsel*
Schwabe, Williamson & Wyatt

Law and ethics are related, and while "law refers to a set of governing rules used to protect the public, ethics refers to standards of behavior that develop as a result of one's concept of right or wrong".[1] The area of patient privacy and professionalism in the context of social media presents an interesting example of the intersection of healthcare law and ethics. The dramatic growth of social networking platforms and applications requires that healthcare professionals be mindful of both their ethical responsibilities and their patients' rights of privacy.[2] Privacy legislation addresses the use and disclosure of patients' protected health information (PHI).[3] The use of social media may result in violations of law, in run afoul of certain ethical considerations, or in both.

Physicians who use social media often do not understand how challenging it might be to adhere to the standards of medical professionalism.[4] Unfortunately, "posting of unprofessional content is common among medical students, residents, and other healthcare providers".[5] Some of this content may be unprofessional, such as off-duty drinking pictured on a social media site, but it does not violate established principles of medical professionalism.[6] Social media presents many positive opportunities to engage patients and provide better healthcare, but it also presents many legal and ethical risks for clinicians. Social networking sites make it difficult for clinicians to keep their professional and personal personas separate.[7]

Professional ethics seek to guide the activities of professionals who are members of a particular profession.[8] In Opinion 9.124 – Professionalism in the Use of Social Media, the American Medical Association (AMA) sets forth a number of considerations that physicians should weigh when maintaining a presence online.[9] These considerations include being cognizant of patient privacy and confidentiality, using appropriate privacy settings to safeguard personal information, maintaining appropriate boundaries of the patient-physician relationship, considering separating one's personal and professional content online, bringing to the attention of another professional that his or her content posted online appears unprofessional, and recognizing that actions online and content posted may affect one's reputation and career.[10] The Federation of State Medical Boards (FSMBs) has adopted *Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice*.[11] The Canadian Medical Association has also published guidelines on *Social Media and Canadian physicians – Issues and Rules of Engagement*.[12] Many of these guidelines overlap the AMA's Opinion. However, the guidelines promulgated by the AMA and the FSMB "do not address the range of likely professional consequences for specific violations".[13]

Medical licensing authorities have reported incidents of online violations by physicians, and many of these have resulted in serious disciplinary actions.[14] Some of these violations may result in physicians' losing their licences to practice medicine; some, particularly breaches with respect to patient privacy, may result in violations of law. Medical boards have been investigating physicians who use social media inappropriately. Such investigations have revealed inappropriate communications with patients online, posting unprofessional images, providing misleading information about clinical outcomes, misrepresenting credentials, and inappropriately contacting patients.[15] Depending upon the nature and extent, these inappropriate communications and other activities may be seen as violations of law and may result in sanctions by a medical board/licensing authority and/or loss of licence.

To limit their risk, some physicians have developed online physician-only communities that provide additional security and other controls over the information they process.[16] "The intersection of social media and healthcare is a dynamic one that can pose considerable benefit and potential risk to those physicians who elect

to participate in this space".[17] One consideration is the "ethical dilemma of trying to help patients while maintaining an appropriate distance from individualized medical information that may be misused in public social media forums".[18] Although physician-only communities might limit risk, they do not provide the same form of patient-physician engagement. One of the primary risks physicians face in participating in such sites may be the potential for violations of privacy legislation.[19] Ultimately, physicians have a personal responsibility for their conduct;[20] "a key problem is that regulatory statutes have not kept pace with the adoption of social media use".[21]

Indeed, many medical schools report incidents of unprofessional student online postings, but as of 2009, they did not have adequate policies in place with respect to such activity.[22, 23] For example, it has been noted that medical students and residents have posted photographs of their medical mission trips, which potentially violate patient privacy.[24] Medical professionals who use social networking sites could be involved in posting material that might violate patients' privacy; hence, they must personally consider their legal and professional responsibilities.[25]

The area of social media in healthcare taxes the relationship between law and ethics, because "ethical and legal obligations to maintain patient confidentiality have unique repercussions. Yet, defining unprofessionalism online is challenging".[26] The benefits of the professional use of social networking sites must also not be forgotten, given those sites' ability to facilitate the delivery of healthcare by making physicians more accessible to their patients.[27] In fact, one primary care practice has employed social media tools to transform its patient care delivery system to a patient-centered, paperless, concierge practice model.[28]

The intersection of healthcare law and ethics is quite apparent in the dynamic realm of social media in healthcare. What may seem like acceptable behaviour today may be the subject of a new ethical guideline tomorrow and even become illegal in the future. In the interim, prior to taking advantage of social networking platforms and applications, it is important for healthcare providers to consider not only current regulatory policies and legislation but also their professional obligations more generally.

[*Editor's Note:* **Paul DeMuro** is a National Library of Medicine post-doctoral fellow and PhD Candidate in Biomedical Informatics at the Oregon Health & Science University School of Medicine, Department of Medical Informatics & Clinical Epidemiology in Portland, Oregon. He practises law with the firm of Schwabe, Williamson & Wyatt, in Seattle, Washington, where he Co-chairs the Health Information & Technology Practice and has a national healthcare law practice in the areas of Health Information Technology, Biomedical Informatics, Clinical Integration, Physician Hospital Integration, M & A, and healthcare regulation. Paul can be reached at <pdemuro@schwabe.com> or at (206) 407-1569.]

[1] M. S. Brodnik, L. A. Rinehart-Thompson, and R. B. Reynolds, *Fundamentals of Law for Health Informatics and Information Management*, 2nd ed. (Chicago: AHIMA Press, 2013).

[2] A. L. Hader and E. D. Brown, "Patient Privacy and Social Media", *American Association of Nurse Anesthetists Journal* 78, no. 4 (August 2010): 270–74, <http://www.aana.com/newsandjournal/Documents/legbrfs_0810_p270-274.pdf>.

[3] *Health Insurance Portability and Accountability Act of 1996*, Pub.L. 104–191 (August 21, 1996).

[4] S. R. Greysen, T. Kind, K. C. Chretien, "Online Professionalism and the Mirror of Social Media", J. Gen. Intern. Med. 25, no. 11 (2010): 1227–29, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2947638/>.

[5] *Ibid*. at 1227.

[6] *Ibid*.

[7] S. H. Jain, "Practicing Medicine in the Age of Facebook", N. Engl. J. Med. 361, vol. 7 (August 13, 2009): 649–51, <http://www.nejm.org/doi/full/10.1056/NEJMp0901277>.

[8] *Supra* note 1.

[9] American Medical Association, "AMA Code of Medical Ethics Opinion 9.124 – Professionalism in the Use of Social Media" (November 2010), <http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page?>.

[10] *Ibid.*

[11] Federation of State Medical Boards, *Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice* (2011), <http://www.fsmb.org/pdf/pub-social-media-guidelines.pdf>.

[12] Canadian Medical Association, *Social Media and Canadian Physicians – Issues and Rules of Engagement* (2011), <http://policybase.cma.ca/dbtw-wpd/Policypdf/PD12-03.pdf>.

[13] S. R. Greysen *et al.*, "Online Professionalism Investigations by State Medical Boards: First, Do No Harm", Ann. Intern. Med. 158, no. 2 (January 15, 2013): 124–30.

[14] S. R. Greysen *et al.*, "Physician Violations of Online Professionalism and Disciplinary Actions: A National Survey of State Medical Boards", JAMA 307, no. 11 (March 21, 2012): 1141–42, <http://jama.jamanetwork.com/article.aspx?articleid=1105088>.

[15] D. Adams, "Medical Boards Keep Wary Eye on Doctors' Social Media Posts", *American Medical News*, January 28, 2013, <http://www.amednews.com/article/20130128/profession/130129957/7/>.

[16] J. L. Hyman, H. J. Luks, and R. Sechrest, "Online Professional Networks for Physicians: Risk Management", Clin. Orthop. Relat. Res. 470, no. 5 (May 2012):1386–92.

[17] *Ibid.*

[18] *Ibid.*

[19] *Ibid.*

[20] *Ibid.*

[21] *Ibid.*

[22] K. C. Chretian *et al.*, "Online Posting of Unprofessional Content by Medical Students", JAMA 302, no. 12 (September 23, 2009): 1309–15, <http://jama.jamanetwork.com/article.aspx?articleid=184624>.

[23] T. Kind *et al*., "Social Media Policies at U.S. Medical Schools", *Medical Education Online* 15, no. 1 (September 15, 2010): 1–8.

[24] L. A. Thompson *et al*., "Protected Health Information on Social Networking Sites: Ethical and Legal Considerations", J. Med. Internet Res. 13, no. 1 (January–March, 2011): e8, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3221358/?report=printable>.

[25] *Ibid.*

[26] *Supra* note 22.

[27] J. M. Farnan *et al*., "Commentary: The Relationship Status of Digital Media and Professionalism: It's Complicated", Acad. Med. 84, no. 11 (Nov 2009): 1479–81.

[28] C. Hawn, "Take Two Aspirin and Tweet Me in the Morning: How Twitter, Facebook, and Other Social Media Are Reshaping Health Care", HealthAffairs 28, no. 2 (March/April 2009): 361–68, <http://content.healthaffairs.org/content/28/2/361.full>.

• ELECTRONIC MEDICAL RECORDS: REQUESTING, REVIEWING, AND UNDERSTANDING •

Chris Rokosh, RN, PNC(C), *Legal Nurse Consultant*

Medical Records have been developed by putting pen to paper for centuries but are gradually being replaced by Electronic Medical Records (EMR) or Electronic Health Records (EHR). Signatures have been left behind for sign-ins, information is stored electronically, and documentation is completed with the click of a mouse. Most healthcare facilities across Canada now have a combination of paper and electronic files. In either format, the medical record is the foundation of most professional liability cases; hence, requesting, reviewing, and understanding it is key.

In 2011, the Federal/Provincial/Territorial Advisory Committee on Health Infostructure defined the electronic medical record as follows:

> A longitudinal collection of personal health information of a single individual, entered or accepted by health care providers, and stored electronically. The record may be made available at any time to providers, who have been authorized by the individual, as a tool in the provision of health care services. The individual has access to the record and can request changes to the content. The transmission and storage of the record is under strict security.

What distinguishes the EMR from the paper record is that it can contain voice, video, and diagnostic imaging. Data is collected over time, a variety of health care professionals can access the information, and it contains information from a variety of healthcare professionals. This can include physicians' offices, testing facilities, hospitals, health units, and pharmacies. Unique identifiers facilitate effective linking of information.

When requesting EMR, it's helpful to understand that it was originally developed to enhance information and improve communication between health providers. It was also designed to offer decision making support for health providers through prompts, alerts, and reminders and to assist with administrative, reporting, and research functions. The information is in an electronic code is made for data sharing and integration into other systems, such as billing, patient census, and other administrative functions. EMR were not developed with litigation in mind. In fact, it was hoped that EMR would reduce litigation by decreasing the types of healthcare errors associated with illegible handwriting and more technical errors, such as incorrect medication orders. In support of this, a 2008 study at Harvard Medical School revealed that physicians who used EMR paid smaller amounts for fewer malpractice claims than those physicians who used paper records. (Freeman) That said, the majority of malpractice claims stem from misdiagnoses—a problem that has yet proven to be solved by EMR.

While health authorities predicted that use of EMR might reduce litigation, some lawyers say that it is the overwhelming complexity of reviewing the records that will eventually drive numbers down. The traditional request for "any and all health information" can produce a crushing amount of paper in a highly confusing format. There's no single way to avoid this

problem, because software systems, reporting capabilities, and stages of conversion vary between regions. However, a discussion with health information, access, and disclosure specialists within the medical records department can help to ascertain the types of reports that are available and the formats in which they can be produced. Their advice to lawyers is to be as specific as possible. Along with dates and locations of facilities, the report should include information contained within the clinical record: personal demographics, hospital visits, surgeries, laboratory test results, diagnostic imaging results, medication information, drug alerts, allergies, and records from all health providers. Additional narrative records, internal staff communications, and graphic summaries may also be available.

The obvious advantage of EMR is, of course, readability. There's no doubt that printed text is easier to decipher than illegible handwriting and medical abbreviations. But the hard copy EMR printouts will not bear any resemblance to what the physician or nurse was looking at when he or she made clinical decisions. A careful review of each page will facilitate understanding of the information and will provide the details required to develop a chronology of events. Even then, an accurate picture of clinical status may not emerge due to the limitations of the predetermined parameters available in the drop-down menus. Most systems have capability for the input of free text, which, if available, can more adequately describe the clinical status; requesting and reviewing this information can be critical to understanding the case.

Most health record systems across Canada are still paper based or a combination of paper and EMR. As a result, records can be fragmented, and the hoped-for co-ordinated sharing of information has yet to be seen. Health records departments across the country say that it will be at least ten years before this goal is fully realized. But, EMR are here to stay along with the need for a new skillset and a new generation of IT, computer forensics, and medical and nursing informatics experts.

[*Editor's note*: **Chris Rokosh, RN, PNC(C)**, Legal Nurse Consultant, is President and CEO of CanLNC Incorporated, a national company that provides nursing and medical experts to lawyers involved in personal injury, medical malpractice, and class action litigation.

A version of this article appeared in the *Lawyers Weekly*, February 7, 2014.]

INVITATION TO OUR READERS

Have you written an article that you think would be appropriate for *Electronic Healthcare Law Review*?

Do you have any ideas or suggestions for topics you would like to see featured in future issues *of Electronic Healthcare Law Review*?

If any of the above applies to you, please to submit your articles, ideas, and suggestions to <ehlr@lexisnexis.ca>.

We look forward to hearing from you.