Privacy Interests in Prescription Data, Part I

Prescriber Privacy

For several years, concern has been growing about the privacy implications that arise from the use and disclosure of prescription data. More specifically, the impugned transactions involve the sale or transfer of prescription data from pharmacies to commercial data brokers, subsequent processing of the data by commercial data brokers, and their eventual resale to pharmaceutical companies in the form of prescribing patterns or practices. These patterns or practices provide pharmaceutical companies with the historical trends they need to better target marketing efforts aimed at individual physicians through more intense, precise, and unique detailing strategies. Evidence suggests that such strategies are successful in influencing physicians’ prescribing habits.\textsuperscript{1-4}

Whether this influence gives rise to professional conflicts of interest, introduces undue bias in clinical decisions by favoring brand-name drugs over generic equivalents, results in less-than-optimal treatment for patients, and ultimately increases healthcare costs are important ethical and policy issues that extend beyond this article’s scope. The purpose of this two-part article is to focus only on the privacy implications arising from the sale or transfer of prescription data, with respect to both prescribers and patients in Canada and the US.

Prescription Records and Related Privacy Issues

Most privacy laws generally define personal information as identifiable information about an individual and require that individual’s consent before such personal information can be collected, used, or disclosed, absent some applicable exception. The release of prescription data to commercial data brokers raises two different privacy issues, one with respect to prescribers and the other with respect to patients.

There are two types of prescription data depending on the source: retail pharmacies and hospital pharmacies. In both cases, prescription data will typically include some unique identifier of the prescriber, which, in combination with other available data, can easily reveal the prescriber’s name. So, although prescription information is clearly—or at least readily—identifiable with respect to the prescriber, the first privacy issue is whether it constitutes information about that prescriber rather than merely information about his or her work.

Prescription data, which include drug details and possibly diagnoses, are more clearly information about a patient; less clear, however, is whether such data can identify the specific patient in question. Prescription data, as they are released to commercial data brokers, won’t contain any directly identifiable information, but will include information such as age and gender. Geographic information about where the patient lives is sometimes inferable based on the location of the dispensing pharmacy and prescriber. Even such limited information might, in some circumstances, be sufficient to re-identify patients. So, although prescription data are clearly about the patient, the second privacy issue that arises is whether such data contain fields—taken together or combined with other publicly available data—that—taken together or combined with other publicly available data—can possibly identify the individual involved.

In this first part of our series, we focus on physicians’ privacy interests in prescription data.

Prescriber Information in Canada

In Canada, the commercial sale of prescription data is presently governed by private-sector privacy legislation or other related laws and regulations. Different jurisdictions have taken different approaches.

Federally, the Personal Information Protection and Electronic Documents Act (PIPEDA; http://laws.justice.gc.ca/en/P-8.6/) de-
fines personal information broadly to mean information about an identifiable individual. In 2001, Canada’s former privacy commissioner, George Radwanski, found that prescription data, whether individual prescriptions or overall prescription patterns, don’t constitute physicians’ personal information within the meaning of PIPEDA. In the context of a specific complaint against IMS Health Canada (a global company that provides “market intelligence” to pharmaceutical and healthcare industries), the former commissioner didn’t regard prescription data as information about the physician in any meaningful sense, but rather as information about something “once removed, namely the professional process that led to its issuance.” In Radwanski’s view, this information was conceptually more akin to work-product information than personal information. Consequently, he concluded that such data fall outside PIPEDA’s scope and could be disclosed without consent. For a good overview of the present commissioner’s position on the concept of “work product,” as it has evolved over time, see www.privcom.gc.ca/parl/2007/sub_070222_e.asp.)

More recently, the Alberta Court of Queen’s Bench adopted a more technical approach in answering a similar question. Applying specific provisions in Alberta’s Health Information Act (HIA), the court found that all the prescription data elements IMS Health had collected from pharmacies across Alberta, only the physician’s name constituted “health services provider information” as expressly defined in the act (see www.qp.gov.ab.ca/Documents/acts/H05.CFM). However, because the physician’s name is also among the types of health provider information that can be disclosed under the available business-card exception, the court held the non-consensual sale of prescription records to third parties to be permissible. It rejected the counter-argument that the business-card exception shouldn’t apply in this case because releasing the physician’s name with all the other data elements in the prescription record would reveal “other information about the health services provider.” The court refused to interpret this phrase broadly enough to mean any other information about the provider but rather chose to limit its analysis to only those prescribed elements contained within the statutory definition of “health services provider information.” (Recently, Alberta’s government introduced Bill 52, which would amend HIA by, among other things, removing “health services provider information” from the definition of personal information altogether; see www.assembly.ab.ca/bills/2008/pdf/bill-052.pdf.)

In British Columbia, the Personal Information Protection Act (PIPA) expressly excludes both contact and work-product information from its definition of personal information (see www.webcitation.org/5dpX47Weo). Whether prescription data constitutes physicians’ personal information, which requires their consent before third parties can use or disclose it, or whether they escape the consent requirement by falling under PIPA’s contact or work-product exclusions, has never undergone formal examination. In British Columbia, the release of prescription records for commercial purposes is prohibited altogether under By-Law 5 of the Council of the College of Pharmacists of British Columbia (see www.webcitation.org/5dpVugOMF). The professional prohibition is worded broadly enough to ban any commercial “release of information or an abstract of information obtained from a prescription, which would permit the identity of the practitioner or the patient to be determined” (see subsection 35(3) of the by-laws).

In Quebec, the Act Respecting the Protection of Personal Information in the Private Sector takes yet another approach by treating professional information as the professional’s personal information and expressly allowing third parties to collect, use, and disclose it, but subject to the conditions listed in Article 21.1 (see www.webcitation.org/5dpVpGzhC). Quebec’s Commission d’accès à l’information (CAI) might, after consulting with the relevant professional bodies, authorize persons to collect information about professionals’ activities (in this case, physicians’ prescribing data) without consent, provided that

- the individual client (here, the patient) receiving the professional service can’t be identified;
- the professional receives periodic notification about intended uses and valid opportunity to opt out; and
- security measures are in place to ensure that the personal information remains confidential.

The authorized person can in turn disclose professional information

Although prescription information is identifiable with respect to the prescriber, the first privacy issue is whether it constitutes information about that prescriber rather than merely information about his or her work.

<table>
<thead>
<tr>
<th>Privacy Interests</th>
</tr>
</thead>
<tbody>
<tr>
<td>• the individual client (here, the patient) receiving the professional service can’t be identified;</td>
</tr>
<tr>
<td>• the professional receives periodic notification about intended uses and valid opportunity to opt out; and</td>
</tr>
<tr>
<td>• security measures are in place to ensure that the personal information remains confidential.</td>
</tr>
</tbody>
</table>

The authorized person can in turn disclose professional information
The provisions aim to restrict the use and transfer of prescription information for narrowly defined commercial ends to level the bargaining power between sellers and buyers.

Privacy Interests

The plaintiffs, who are in the business of harvesting, refining, and selling this commodity, ask us in essence to rule that because their product is information instead of, say, beef jerky, any regulation constitutes a restriction of speech. We think that such an interpretation stretches the fabric of the First Amendment beyond any rational measure.9

Furthermore, the majority decision of the Court of Appeals went on to hold that even if the law did infringe on commercial speech, it’s nonetheless constitutionally permissible because it directly advances a substantial governmental interest and restricts speech no more than necessary. Of the several governmental interests advanced by the US Attorney General, the majority of the Court of Appeals restricted its analysis to only healthcare costs. It didn’t address the important privacy arguments raised by the Attorney General or the Electronic Privacy Information Centre (EPIC) that intervened as amicus curiae, or “friend of the court.” Consequently, this case provides no further enlightenment on the risks to prescriber or patient privacy posed by the commercial use, transfer, or sale of prescription data.

Interestingly, the majority of the Court of Appeals in this case appeared more willing than the lower court to grant New Hampshire some legislative discretion. As the first state that attempted to formulate novel public policy on this cutting-edge issue, New Hampshire should be granted some “elbow room” in the legislative approach it chooses to adopt to deal with the growing social and economic problems associated with detailing practices. Indeed, other states that have since followed suit by introducing similar laws are looking to the New
Hampshire experiment to determine how to move forward.

For instance, Maine’s Act to Amend the Prescription Privacy Law also forbids prescription drug information intermediaries from using, selling, or transferring— for any marketing purpose—prescription information, but only of those prescribers who have chosen to opt out of such transactions by filing for confidentiality protection. In this respect, the Maine law is less prohibitive than its New Hampshire equivalent, which doesn’t have a similar opt-out provision. The Maine law is also consistent with the opt-out approach facilitated by the American Medical Association through its Physician Data Restriction Program (see www.ama-assn.org/ama/pub/category/12054.html). Companies nonetheless challenged the Maine law on the grounds that it, too, violates their right to free speech. In a motion for preliminary injunction, the US District Court of Maine heard several policy arguments, including claims both for and against prescribers’ right to privacy, and considered whether the sale of prescription data constitutes unauthorized use of a professional work product. The court found sufficient evidence to conclude that the Maine law violates companies’ First Amendment right and granted a temporary injunction against its enforcement until the case could be permanently decided on its merits.11 The ultimate outcome of this case will likely be affected by the result of the New Hampshire appeal.

As you can see from our survey, the commercial use, transfer, and sale of prescription data have come under significant legal scrutiny in several jurisdictions across both Canada and the US, but through a different lens.

In Canada, legal analyses have turned mostly on assessing the privacy interests at stake. If we were to draw a conclusion based on the Canadian jurisprudence to date, the practice appears to be generally permissible in most jurisdictions we surveyed (with the exception of British Columbia), either because it is excluded from the scope of privacy regulation altogether, is exempt from consent requirements on an exceptional basis, or is permitted subject to numerous conditions, checks and balances.

In the US, legal analyses have been mostly constitutional in nature, based on First Amendment arguments raised by commercial data brokers. In light of the recent US Court of Appeals’ decision, such constitutional arguments might have received a fatal blow, and laws restricting the use and transfer of prescription data for commercial uses could be here to stay. Although patient and prescriber privacy interests were among the broad public policy arguments raised by parties seeking to support the legislative intent, these privacy arguments were seemingly not the most persuasive. Rather, in the end, it was the state’s interest to contain healthcare costs that carried the day, not its interest in protecting privacy.

So far, what appears to be common in both Canada and the US is this: in cases in which decision-makers have expressly examined privacy arguments raised by various parties, their rationale consistently began with the assumption that patient-related information is clearly nonidentifiable. For the most part, they regarded patient re-identifiability as unlikely and set it aside as a nonissue from the outset, moving on rather hastily to address the issue of prescriber privacy. In the second part of this article, we will begin to question this assumption and challenge the basic premise that patients can never be re-identified from prescription data disclosed to commercial data brokers.

Acknowledgments

The views expressed in this article are the authors’ own and do not represent the official positions of their employer organizations.

References

5. “Privacy Commissioner Releases
Privacy Interests

7. Prescription Information Law, New Hampshire Revised Statutes Annotated, 2006, sections 318, 47-f, 47-g, and B:12.

Patricia Kosseim is the chief GE3LS Of - cial at Genome Canada, where she holds the position of General Counsel. Kosseim has degrees in business and law from McGill University and a master’s degree in medical law and ethics from King’s College, University of London. She is a member of the Barreau du Québec and the Canadian Bar Association. Contact her at pkosseim@genomecanada.ca.

Khaled El Emam is a senior scientist at the Children’s Hospital of Eastern Ontario Research Institute, and is a Canada research chair and associate professor in the Faculty of Medicine at the University of Ottawa. His research interests include re-identification risk assessment and developing practical de-identification techniques for health information. El Emam has a PhD in electrical and electronic engineering from King’s College, University of London. Contact him at kelemam@uottawa.ca; www.ehealthinformation.ca.

### Advertiser Index
**January/February 2009**

<table>
<thead>
<tr>
<th>Advertiser</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black Hat 2009</td>
<td>Cover 4</td>
</tr>
<tr>
<td>Infosec World 2009</td>
<td>Cover 2</td>
</tr>
<tr>
<td>MIT Press</td>
<td>11</td>
</tr>
</tbody>
</table>

### Advertising Personnel
Marion Delaney  
EEC Media, Advertising Dir.  
Phone: +1 415 863 4717  
Email: md.ieeemedia@ieee.org

Marian Anderson  
Sr. Advertising Coordinator  
Phone: +1 714 821 8380  
Fax: +1 714 821 4010  
Email: amanderson@computer.org

Sandy Brown  
Sr. Business Development Mgr.  
Phone: +1 714 821 8380  
Fax: +1 714 821 4010  
Email: sb.ieeemedia@ieee.org

### Advertising Sales Representatives
**Recruitment:**

Mid Atlantic  
Lisa Rinaldo  
Phone: +1 732 772 0160  
Fax: +1 732 772 0164  
Email: lr.ieeemedia@ieee.org

New England  
John Restchack  
Phone: +1 212 419 7578  
Fax: +1 212 419 7589  
Email: j.restchack@ieee.org

Southeast  
Thomas M. Flynn  
Phone: +1 770 645 2944  
Fax: +1 770 993 4423  
Email: flynttom@mindspring.com

Midwest/Southwest  
Darcy Giovingo  
Phone: +1 847 498-4520  
Fax: +1 847 498-5911  
Email: dg.ieeemedia@ieee.org

Northwest/Southern CA  
Tim Matteson  
Phone: +1 310 836 4064  
Fax: +1 310 836 4067  
Email: tm.ieeemedia@ieee.org

Japan  
Tim Matteson  
Phone: +1 310 836 4064  
Fax: +1 310 836 4067  
Email: tm.ieeemedia@ieee.org

Europe  
Hilary Turnbull  
Phone: +44 1875 825700  
Fax: +44 1875 825701  
Email: impress@impressmedia.com

**Product:**

US East  
Joseph M. Donnelly  
Phone: +1 732 526 7119  
Email: jmd.ieeemedia@ieee.org

US Central  
Darcy Giovingo  
Phone: +1 847 498-4520  
Fax: +1 847 498-5911  
Email: dg.ieeemedia@ieee.org

US West  
Lynne Stickrod  
Phone: +1 415 503 3936  
Fax: +1 415 503 3937  
Email: l.stickrod@intermediapartners.de

Europe  
Sven Anacker  
Phone: +49 202 27169 11  
Fax: +49 202 27169 20  
Email: sanacker@intermediapartners.de