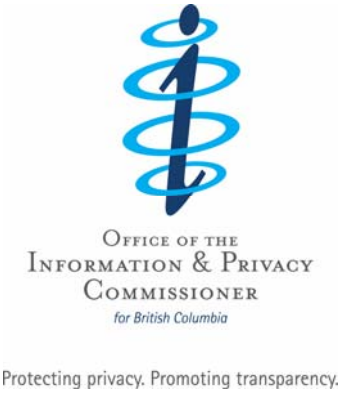

CHECK AGAINST DELIVERY

PRESENTATION TO ISACA VANCOUVER

PRIVACY AND SECURITY IN HEALTHCARE

FEBRUARY 9, 2017

DREW MCARTHUR
ACTING INFORMATION AND PRIVACY COMMISSIONER FOR B.C.

Introduction

Thank you for that kind introduction. I appreciate the opportunity to be here with you today. Some of you may know that I have been the Acting Commissioner since July last year. Prior to that I was semi-retired after spending most of my career with TELUS and the former BC TEL.

Soon, perhaps within weeks, a permanent commissioner will be selected, based on a unanimous recommendation from an all-party committee. Once that happens, I will go back into retirement. I'll admit… I do love this job. If I didn't love retirement more, I would have seriously considered applying for it myself.

But back to why I'm here today…. to share my perspective as a regulator on the very important area of health information privacy. Actually, I'm playing in a bit of a double header. I've just come from the annual Reboot Privacy & Security conference in Victoria, where I addressed an audience of about 1,000 privacy, security and access to information professionals who are facing a variety of issues in both the public and private sectors.

Now I hope to address some of the unique issues and challenges that you and your colleagues face in the health care sector.

Given the volume and sensitivity of personal information collected, used, and disclosed in the health care system, what I'm going to say next shouldn't come as a big surprise to anyone in this room: We must all be vigilant in protecting personal health information.

Privacy protection, after all, is not only the right thing to do, it's the law. And I want to stress, it goes beyond the practice of patient confidentiality. While patient confidentiality is important, and is a solid foundation for privacy, privacy includes additional principles such as minimum collection, limited use, authorized disclosures, and allowing individuals to control their own personal information.

In British Columbia, we have a patchwork of different laws that apply to personal health information, which sometimes makes compliance challenging. I'll get into this in greater detail a bit later.

But first, I want to address a misconception that you may or may not have about my office. When some people hear the word "regulator," they assume "rigidity" and the imposition of barriers. Trust me, I understand that initial instinct: When I was working at TELUS as Chief Privacy Officer, I can remember feeling resistant to the idea of regulation. But over time, I began to see the broader impact of privacy regulation, that it was much larger than me, and my team, and my business. I came to see that privacy regulation holds everyone to a higher standard than they may hold themselves.

I've learned that in the health sector, rigidity is not the reality. Generally, the existing legislation already authorizes the data flows needed to deliver health care services within our publicly-funded system. It also enables health care authorities to disclose health information to researchers.

Public bodies and organizations, like our host today, who are responsible for the data flows of personal health information must comply with both the Freedom of Information and Protection of Privacy Act and the Personal Information Protection Act, as well as with the E-Health Act and other applicable pieces of health legislation.

But just achieving compliance is the minimum. We want to see the best possible privacy protection for the very sensitive personal information collected for the purpose of delivering health services. British Columbians expect it and they deserve nothing less.

We want to see the implementation of best practices and a gold-standard privacy and security framework. This is essential to maintain public trust and confidence in health care providers and the health care system itself.

This afternoon, I'd like to share some of my office's initiatives to promote this gold-standard privacy and security framework in the health sector. Let's get started.

Health authority audit

As some of you know, my office has closely examined privacy and security frameworks in both health authorities and the Ministry of Health.

In 2015, we completed an important audit of how health authorities manage privacy breaches. In case you're not familiar with it, the report can be found on our website.

But here's the short version: We found that while B.C.'s health authorities were doing a lot of things right, there were some significant gaps in governance, compliance monitoring, notification and reporting, and training and confidentiality agreements.

All of the health authorities have taken steps toward implementing our 13 recommendations for improvement. The key takeaway was that health authorities need to pay more attention to breach prevention, so they can move from being reactive about privacy breaches to being proactive about preventing them in the first place.

I like this approach – I would much rather catch people doing something right!

Reviews of eHealth systems

My office also looks closely at electronic health systems, which involves evaluating Privacy Impact Assessments and Security Threat Risk Assessments. If you're responsible for these documents, you'll be relieved to know that we don't expect them to be legal opinions or weighty tomes. But here's what we do like to see: full descriptions of all data flows, proper authorities cited, and all the elements of a privacy and security framework. Most importantly, we need your documents to identify the privacy risks and the steps that are being taken to mitigate them.

You may recall that we conducted a review in 2010 of Vancouver Coastal's Primary Access Regional Information System or "PARIS." This investigation report really set our baseline for how we expect personal information to be protected in an eHealth system.

When we found that some of the data flows weren't legally authorized, government responded. While they did enact new legislation, our exact recommendations were not followed. We also identified areas for improvement with role-based data access and security protection, which Vancouver Coastal addressed in a timely manner.

My office did discover some positive things with our review. We found the privacy management program at Vancouver Coastal to be a good one where a corporate culture of privacy was being nurtured. That report is also available on our website if you're interested in learning more about it.

More recently, we examined Panorama, a joint B.C. and Yukon electronic health record system that's partially funded by Canada Health Infoway. We made a number

of suggestions to the Ministry of Health in the implementation of that system and the Provincial Health Services Authority is now the data custodian. The Yukon Commissioner and I are following up with the PHSA and the Yukon Department of Health and Social Services to see what progress is being made.

When we review electronic health records systems, we want to see role-based access to health records with technical controls and automated auditing. An eHealth system can flag unusual activity far more efficiently than a privacy officer manually sifting through endless piles of paper.

While automation will never replace the need for robust privacy training, it is critical to a modern, computerized record system and should be utilized by health authorities and the Ministry of Health.

I just wanted to note a couple of other aspects of our work with eHealth. We are monitoring the implementation of B.C.'s E-Health Act as we wish to see more designation orders and health information banks. We're also an active participant in the Privacy Forum of Canada Health Infoway. The Forum allows us to learn about pan-Canadian eHealth projects that we will want to review at the conceptual and design phases, before they are deployed in BC.

Physician Privacy Toolkit

Now I'd like to share our work with another key group of stakeholders – doctors. We're currently working with the Doctors of BC and the College of Physicians and Surgeons to update the 2009 Physician Privacy Toolkit.

What's in this toolkit? Guidance to physicians working in offices or clinics that are governed by the Personal Information Protection Act.

Most offices today have electronic medical record systems, which present unique challenges for privacy protection as I described. The new Toolkit outlines the elements of a privacy management program that should be in place to address these and other challenges.

Once we've completed some additional consultations with our external stakeholders, the toolkit will also be available on our website. As our recent audit of a medical clinic showed, this guidance document can't be published soon enough!

Video surveillance audit report

Our first-ever private sector audit examined a medical clinic's use of video and audio surveillance. The clinic had installed 8 video surveillance cameras on their premises, including the lobby, hallways, back exits, and fitness rooms.

Even though we've become accustomed to seeing video cameras everywhere these days, that's pretty concerning. We found the clinic's use of their surveillance system

to be unauthorized and excessive and I recommended it immediately stop collecting personal information in this way.

Our findings prompted us to issue guidelines for organizations in conjunction with the report. I hope public bodies and organizations take note, as these guidelines are the criteria we will use to evaluate overt surveillance in the future.

The bottom line is that video surveillance should only be used as a last resort after exploring other less privacy-invasive options. There are links to the report and Guidelines on the home page of our website.

Health Research Roundtable and Health Data Research Forum

Turning now to health research in B.C.…

We've had to do a little myth-busting in this area, because some researchers and members of the media believe that privacy protection is a barrier to health research.

It isn't, by the way.

My office is actually very supportive of health research that's in the public interest. We don't believe health research and privacy protection are mutually exclusive, because health research can be conducted in a privacy respectful manner.

As an aside, this is particularly important to me, as I am on the board of a health charity – the national Arthritis Society.

In 2012, my predecessor Liz Denham brought stakeholders from government and the research community together with privacy experts for a Health Research Roundtable. This event was followed a year later by a Health Data Research Forum. Stakeholders at these two events made recommendations to improve researchers' access to data while still protecting privacy.

Among other things they called for more resources for data stewards and a transparent and consistent approval process.

What a win-win. By the end of these meetings, there was also an important general agreement that while privacy laws are not a barrier to research, the legal requirements are not well understood by health researchers.

Guidance for health researchers

To that end, my office is in the process of finalizing a guidance document for health researchers. It will clarify how B.C.'s privacy laws enable health research by explaining the statutory terms and conditions for disclosure without consent for research purposes.

This guidance will also outline the approval process for when researchers recruit participants for research studies. When researchers want to use personal information to contact patients directly, they must get approval from our office. Data Stewardship Committee of the Ministry of Health advises us whether it supports the request, and we ensure that the manner of contact is as non-privacy invasive as possible.

We make these requests a high priority because we want to facilitate health research as much as we can. Yes, it adds a bit of bureaucracy, but the process doesn't need to be onerous. What's important is that it adds a level of oversight for the protection of patient personal information. After all, we did learn that researchers don't always understand their legal obligations.

Advocating for a stand-alone health information privacy law

As you may know, my office has also strongly advocated for a new stand-alone health information privacy law in this province. This type of legislation already exists in most other Canadian jurisdictions. It properly recognizes that the health sector is unique and requires special rules for sharing patient information among providers, eHealth systems, and health researchers, among other things.

A new, comprehensive health information privacy law would also alleviate the confusion caused by our current patchwork of legislation.

My predecessor released a report in 2014 called *A Prescription for Legislative Reform* that made the case for a new health information privacy law. It also made specific recommendations on what provisions the new law should contain.

Shortly afterward, she submitted her recommendations to the Special Committee to Review FIPPA. The Committee accepted those recommendations and, in its May 2016 report, recommended that government enact a new stand-alone health information privacy law at the earliest opportunity.

I am hopeful that we will have this new privacy law fairly soon. Perhaps not during my tenure as Acting Commissioner(!) but at least in the foreseeable future. It will be interesting to see how government responds to our recommendations.

Closing

I see my office as a partner in the protection of health information. We devote a great deal of time to reviewing, advising, and guiding the implementation of best practices. And we know data custodians, for the most part, care just as much about privacy as we do.

Our focus is ensuring that privacy protection is a priority of any initiative that involves the collection, use, and disclosure of personal information. We understand that the delivery of health care needs to be efficient and cost effective – but it also needs to be privacy protective.

So while we support health research that has the potential to reduce illnesses and mortality – the data needs to be handled properly.

I know that an eHealth system is expensive to implement, but cost-cutting should never affect its privacy and security framework.

My office will continue to be active in the area of health privacy. New eHealth projects keep us busy, as do reviews of privacy management programs within public bodies and organizations in the health sector.

And of course there are privacy breaches from time to time. I am particularly disappointed by the snooping incidents in various health authorities that continue to occur. This is one of the reasons why we have also recommended monetary penalties or fines for such inappropriate actions. These individuals are not following well-established rules… rules they would want respected if it was their personal health information at stake.

There are many other emerging issues in the health sector. Big data is an area of interest across all of our work and raises many issues, including those about its appropriate use. Together, Canada's privacy commissioners are studying the privacy and ethical implications of big data.

A subset of Big Data in the health sector is the rapidly expanding science of genomics and personalized medicine. At issue is the disclosure of genetic information, including whole genome sequencing data and analyses of human tissue in biobanks.

There are many conversations to be had around the appropriate consent requirements for genetic information. One involves the "duty to warn." Should, for instance, your genetic information be disclosed without your consent if doing so could reduce a health or safety threat to one of your relatives?

It's my belief that guidelines - like those issued in Australia in 2009 by the National Health and Medical Research Council with the approval of the Australian Privacy Commissioner - should be developed in consultation with genome scientists, clinicians, research ethics boards, Privacy Commissioners, and the public.

There are of course many other emerging issues that challenge and engage my office. Not every day is a double header, like today, but life as a privacy commissioner is never dull.

Thank you for your attention this afternoon. I would be more than happy to answer any questions you may have.