Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

SPEECH TO THE

IOT/BIG DATA HEALTHCARE SUMMIT, WESTERN CANADA

NOVEMBER 29, 2017

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

Good morning, everyone. Thank you, Paul (Gallant) for inviting me to speak with you. It's great to be with you and to be part of this important conversation.

I'm here today as BC's Acting Information and Privacy Commissioner to offer my perspective on Big Data and the Internet of Things…. well, let's be honest and call it what it **really** is - the Internet of EVERYthing. From the rubber ducky in your child's bathtub to your smart tea kettle, connected devices truly are everywhere.

In the not so distant past, the internet of things and big data were two of many topics on a healthcare conference agenda. Now they've become the over-arching theme of conferences like this one.

These developments are obviously extremely important in both the private and public sectors. In the healthcare sector, Big Data has the possibility to offer valuable new insights and solutions to researchers and clinicians, save time and money, and dramatically improve patient outcomes.

Yesterday, from perusing your agenda, you heard about machine learning, creating adaptive health systems, enhancing healthcare through the internet of things, and harnessing big data to advance health care outcomes…. Smart Hospitals and the

integration of IoT into healthcare systems…. And today, you no doubt will be impressed by the innovation showcase.

The array of connected devices on the market today seems almost limitless. And there are some incredible new applications in the healthcare sector, from Smart hospital beds and artificial intelligence tools for diabetes management to connected spoons and forks for Parkinson patients and the industry's first digital pill.
Yes, a digital pill, designed for schizophrenia patients, to ensure they take their medication.

The sensor in this pill, which recently received FDA approval, is the size of a grain of sand… believe it or not, it's activated by the patient's gastric juices. The sensor sends a unique, identifying signal to a wearable patch, which then tells the patient's physician that the medication has been consumed.

Then there's the new Scripps Research Institute smartphone app. Have you heard of this one? It can calculate your risk of heart disease by using your data from 23andMe.

As we all know, home DNA tests like 23andMe, AncestryDNA, and others have become incredibly popular. Here in Canada a new DNA test is even being offered by some pharmacies. MyDNA is said to better assess how we will react to the medicines we take, based on our genetics.

BUT there can be privacy concerns with genotyping. Which is why my Office, the Alberta Privacy Commissioner's Office, and the Office of the Privacy Commissioner of Canada are working together on a guidance document about direct-to-consumer genetic testing.

Are all data-driven devices and apps **privacy** invasive? In the rush to market, is privacy becoming an after-thought? These are some of the questions we're considering at my Office.

But before I go any further, I feel the need to add a disclaimer:
My Office is not anti-Big Data or anti-Internet of Things.

We are NOT a group of Luddites who distrust or dislike technology.

Many of us wear Fitbit activity trackers and use smart devices in our own homes and offices. For example, I can see the status of my front door lock from my mobile phone.

So I hope you understand that I am not here to be critical of technology….
Rather, I'd like to share my perspective as a regulator on the very important topic of health information privacy. My role as Acting Information and Privacy Commissioner is to monitor the administration of the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*, yes, to ensure compliance –

– but ALSO to maintain the public's trust and confidence in health care providers and the health care system itself.

In our view, these laws are not a barrier to the use of Big Data; in fact, they are an enabler, because individuals can be assured that their personal information must be used and disclosed in a privacy protective manner.

Like you, we see the potential of Big Data to improve patient outcomes. We see its benefits to health research. And we see, particularly with the evolution of **personalized** medicine, that it has tremendous **PROMISE** for health research. But we also see that there are risks.

The more we learn about genetics, in particular, the more complicated these risks become. And it's now possible to imagine a future when we will have DNA records for EVERY patient. That's why we need to ask ourselves NOW… what do we really need to consider around the collection, storage and release of that data?

The government of Canada, for instance, recently introduced an act to "prohibit and prevent genetic discrimination." The enactment amends the Canada Labour Code, in a nutshell, "to protect employees from being required to undergo or to disclose the results of a genetic test." It's a step in the right direction. I'm here today to ask all of you to protect patient privacy when implementing the latest and greatest smart device or application… to carefully weigh the risks associated with some of these new technologies against their potential benefits.

My Office has been involved in the Big Data/Internet of Things conversation for many years – perhaps even longer than it's been a topic at healthcare conferences.
We work with industry and public bodies to ensure that this brave new world of connected *everything* is also **privacy protective** and **safe** for citizens. It is a matter of doing things in the right way, for the right reasons. In my remarks here today, I'll tell you about some of these relationships. I'll share information about our work on this issue over the last few years. I'll offer information about practical guidance for those of you who are actively working with patient data. And finally, I'll tell you about a resource we launched just yesterday with Doctors of BC and the College of Physicians and Surgeons of BC.

Let's start with an example of a research project that takes the right approach….
Some time ago, we were asked by the BC provincial government to review their new Data Innovation Program.

This initiative is designed to provide a secure environment for data scientists, analysts and researchers in government and academia to access and generate insights from high value de-identified data from across the public sector.
The key word here? **"Deidentified."**

Research and analysis in the Data Innovation Program will only use **linked, de-identified** data in a **highly secure** research environment.

And there will be other safeguards, too: **only anonymized, non-personal information will ever leave the secure environment. This** program is about **population-level research and analysis, never individual-level decisions**. It can't be used to track or monitor or make any decisions about individuals.

This is a **great** example of built-in **privacy**: both privacy **and** security have been considered at **all** stages of the program's design and build….

For instance, even though the data is de-identified it is still protected as though it is personal information. It's also important to note that the program's privacy and security measures will not compromise the efforts of researchers.

The program builds on the efforts of Population Data BC, or POPData, who work with the Ministry of Health to provide privacy protective access to academic researchers. While PopData meets current needs, the province requires a secure, scalable environment to support use across both government and academia. That's why they worked with PopData and the Ministry of Health to co-design this next generation program.

My Office was consulted on the program's Privacy Impact Assessment or PIA. For those of you who are unfamiliar with PIAs – they are important documents that help to identify and address potential privacy risks before programs are up and running. We have also learned that the Data Innovation Program will ensure compliance through third party certification and that a Chief Privacy and Security Officer will be appointed. This individual will be responsible for ensuring that best practices are continuously followed.

I must say these are good, precedent setting examples on how we can properly conduct research in a privacy sensitive way.

While we're on the topic of research, I wanted to let you know that my Office is about to release a guidance document for researchers about how BC laws enable health research while protecting privacy. If you are a data custodian, it's important that you feel comfortable every step of the way when you're asked to disclose data to researchers. Holding sensitive data places a moral responsibility on your shoulders. We want researchers AND data custodians to know that there are appropriate ways to manage this process and ease that burden. Data access requests must be carefully vetted. There's more demand than ever to use the treasure trove of data collected for the purpose of delivering health services. And patients more often than not are unaware of this secondary use.

Data custodians must take their obligations to protect health data very seriously. The public expects no less. And the potential negative consequences of breaches are enormous and far reaching.

Stay tuned for this release.

The other complexity of course about the use of Big Data for health research in BC concerns our current patchwork of health information legislation. The *Freedom of Information and Protection of Privacy Act* governs the personal information in the custody or control of the Ministry of Health, health authorities, and professional regulatory bodies. The *Personal Information Protection Act* governs health professionals in private practice and the personal information they collect in their delivery of health services. And then there are the separate pieces that govern specific types of health information such as the E-Health Act, the *Public Health Act*, the *Medicare Protection Act*, and the *Pharmaceutical Services Act*.

We have been advocating for stand-alone health privacy law in this province for some time. We believe a single, modern, consistent legislative framework for all of the data flows within the BC health sector would alleviate much of the confusion we see about legal authorities, consent, and the standards that are required. We discussed our specific recommendations as to what a new piece of stand-alone health information legislation should look like in a special report on our website entitled, A *Prescription for Legislative Reform*.

I know many of you are here today from BC's health authorities and the Ministry of Health. You may recall that back in 2015 we conducted an important audit of your privacy and security frameworks.

Our examination took a look at BC health authorities' compliance with relevant legislation, my Office's guidelines, and your own policies and procedures with respect to managing and reporting privacy breaches. We also made recommendations to strengthen and improve privacy management practices.

My Office found that health authorities were doing many things that were consistent with good privacy breach management. We also identified some significant gaps in terms of governance, compliance monitoring, notification and reporting, and training and confidentiality agreements. I'm pleased to say that these gaps have since been addressed by the health authorities.

Managing patient privacy is not an easy job, given the vast amount of highly sensitive personal information that health authorities collect, use, and disclose every single day. I acknowledge the efforts of those present who are involved in this important work.

Now I'd like to take you to the frontlines of patient care and privacy protection – the physician's office. Just yesterday, my office, the BC College of Physicians and Surgeons, and Doctors of BC released a joint guidance document to assist physicians who work in private practice. The *BC Physician Privacy Toolkit* describes the privacy issues associated with the collection, use, disclosure, retention, and protection of personal information.

As we all know, health information is one of the most sensitive forms of personal information. It includes the physical, mental, and emotional health histories of patients, and can span a lifetime.

Protecting this information is absolutely foundational to the doctor-patient relationship. We know that if patients do not trust the safeguards physicians put in place to protect their personal information they will withhold information, refuse to provide consent, or opt not to seek treatment.

We also know that things are so much more complex today for doctors. They are accustomed to protecting their patients' confidentiality. But gone are the days when the only copies of a patient's medical records are securely housed in a physician's office - under strict lock and key.

Today, for good reasons, patient data is often housed in multiple locations and can be accessed and disclosed in emails, faxes, and databases. There is so much potential for it to go astray – lost or stolen laptops, intercepted mobile communications, and unencrypted memory sticks are just a few of the many ways privacy breaches can occur.

This resource is designed to help physicians make their way through these challenges. It contains separate modules for each of the privacy principles, tips, checklists, webinars, searchable FAQs, and customizable templates.

The Toolkit covers topics like electronic records, responding to complaints and privacy breaches, and the use of mobile devices. And it outlines **10 essential steps** in plain language that physicians in private practice should take in order to comply with the *Personal Information Protection Act*.

The first step - "**Be Accountable**" - underscores the importance of creating a comprehensive privacy management program. This truly should be the number one priority for anyone who manages personal information. We have some great resources on our website, should you need further assistance with this step.

The person who is responsible for structuring and managing the privacy management program would normally be the **privacy officer** – in a private medical practice, this would be the **physician**.

Our Toolkit offers useful guidelines for demonstrating accountability, such as formulating privacy policies and procedures for using or disclosing personal information for research, protecting medical records outside the practice, and developing technological controls.

You'll find this resource on our website and on the Doctors of BC's website. We welcome your feedback and suggestions.

[Closing remarks]

None of us has a crystal ball when it comes to forecasting how technology will evolve in the future. But we can predict with certainty that Big Data and the Internet of Things -- "the Internet of **Everything**" -- will continue to dominate our discussions.

As you navigate your way between rubber ducks and digital pills, my Office will be here to help. For instance, our policy team can provide advice to data custodians and researchers about the responsible use and disclosure of patient data for research. We can approve requests for the use of contact information for participant recruitment. And, if you are considering the implementation of a new app or device, we are happy to review and comment on your organization's privacy impact assessment.

Thank you for inviting me here to speak with you…. I'd be pleased to take your questions now.