OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

**CHECK AGAINST DELIVERY**

## SPEECH TO

## CANADIAN HEALTH INFORMATION MANAGEMENT ASSOCIATION

## February 7, 2025

## MICHAEL HARVEY

## INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Hello, my name is Michael Harvey, and I'm the Information and Privacy Commissioner for British Columbia.

I would like to acknowledge that I am speaking to you from the traditional territories of the Lekwungen people, of the Songhees and Esquimalt First Nations.

As an Officer of the BC Legislature, I also acknowledge that I am privileged to work with people across many traditional Indigenous territories, covering all regions of our province.

I'm grateful to be here – to work and live on this beautiful land – and also for the opportunity to benefit from the knowledge shared with us by Indigenous communities throughout British Columbia and Canada.

Today I want to talk to you about the principles I believe should guide the handling of personal health information today, and into the future.

1. There is no privacy without access.

2. There is no such thing as the health information system – it's just the health system.

3. Virtual care is care, and it is integral to mainstream health care.

And

4. Trust or social licence will be the most important element going forward, given our data-rich health system.

But before I get started, I wanted to tell you about my role as BC's Information and Privacy Commissioner.

My wider mandate is centered around protecting and promoting the privacy and access rights of people living in British Columbia as they are set out in two laws:

- the *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to more than 2,900 public bodies in BC, including health authorities,
- and the *Personal Information Protection Act* (PIPA), which governs the private sector and applies to physicians in private practice.

However:

We are not government.

We don't make the laws.

If we did, BC would already have health privacy legislation.

Rather, as an independent officer of the Legislature, we enforce these two laws, and are accountable to the Legislature as a whole, not to any one sitting government.

The aim of our office and the other statutory officers in BC is to help ensure a more transparent and accountable government.

We mediate and investigate access and privacy issues, issue legally binding orders, and conduct in-depth investigations and audits into compliance with our laws.

I'd like to tell you a bit more about my background, and what brought me to this work. Some of you may know me. For those who do not, I'm not a lifelong privacy professional like many in my field – I'm a public policy generalist.

Prior to this role, which I have been in only since last May, I served for almost five years as Information and Privacy Commissioner for Newfoundland and Labrador – the province in which I was raised.

Before that, I was Assistant Deputy Minister of Health and Community Services for Policy and Performance Monitoring. When you are an ADM of Health in a small province, you end up with a very broad range of responsibilities.

At different points in my time in health I was responsible for everything from negotiating with doctors and dealing with health regulatory bodies to promoting health research and information management and e-health. I also sat on the boards of the Newfoundland and Labrador Centre for Health Information and the Health Research Ethics Authority.

It was because of this experience that I was asked by the federal government, while I was a Commissioner in Newfoundland and Labrador, to serve as part of the Expert Advisory Group on a pan-Canadian Health Data Strategy.

So that's a bit of background about my role and my background, and why I was asked me to speak with you today.

During my term as Commissioner, Newfoundland and Labrador experienced the most devastating cyberattack in the history of Canadian healthcare.

The 2021 cyberattack came at tremendous costs to taxpayers, but the impact on people was more significant – medical procedures, cancer treatments, diagnostic imaging appointments and more were delayed or cancelled altogether.

Then there was the damage done to the public's trust in the healthcare system. That we can't easily quantify, but it's a threat to one of the fundamental facets of our Canadian identity.

It happened in Newfoundland and Labrador, but the issues it brought to the fore are relevant countrywide.

Here in BC, for example, my office's 2022 investigation report into the Provincial Health Services Authority's public health database found glaring security flaws.

We released a subsequent report on the PHSA's work to address those flaws.

But in both cases, there was an urgent need to take action because of the stakes that were involved.

We know the stakes are high because we're not just working in the field or in the regulatory space, we're also active participants in the system.

Our human experience with the system informs our participation in it.

We know how important and sensitive personal health information is.

It's information that is often collected when we're at our most vulnerable and it can reveal the most intimidate details about us, about our physical and mental wellbeing, even our genetic makeup.

A breach of that information could have devastating results: compromising care; harming people's physical and mental health; identity theft; reputational damage; discrimination and financial loss.

A fundamental principle of our privacy laws is that the safeguards around personal information should be commensurate to the sensitivity of that information.

By that standard, personal health information must have the highest level of protection we can provide.

Health information professionals such as yourselves are on the front lines providing that protection.

I would like to take a moment to acknowledge and express my appreciation for the work you do every day in countless very difficult situations.

My talk today will focus on some of the big picture questions that I think everybody working in this field needs to consider.

These are areas where we need to shift our thinking to reflect the reality of modern healthcare provision, including on how, along with safeguarding personal information, we need to improve how that information is shared and accessed in people's best interests.

I said earlier that there were four principles I wanted to discuss today. Let's start in with the first one:

1. **There is no privacy without access.**

We need to think differently about privacy in the age of virtual care.

Privacy, in the analog world, was primarily about keeping information secure and in a box and constraining its accessibility.

In hospitals, there were registries where all the files were kept.

If a medical professional wanted a chart, then they would have to go and check it out.

Health information regimes were built around that process.

Some of that system is still around because the transition to digital has not been all encompassing.

But we are transitioning away from that.

We're transitioning away from the notion that the most important privacy consideration is keeping everything safe behind those walls and in those filing cabinets - locked down.

Today, the most important privacy consideration, in my view, is about access. Whose access?

The access of the individual and their clinicians. Right?

Now you hear frustration from individuals and from their clinicians about not being able to get the health information they need. So, in this sense, privacy is about more than security.

It's really about control. Our ability as individuals to control our own personal health information.

Having control of our own information is not about whether or not we have something to hide. It is about whether we can have autonomy.

It is not about just being able to say who should NOT use our information, but also about who CAN use it.

It is about how we are defined as individuals vis a vis one another and each other's organizations and the state.

It is how we are distinct, how we are more than just undifferentiated cogs in the broader social machine….

In this sense, privacy is the precondition to our individuality – it is how we have autonomy and dignity as individuals in a society. This has always been true, but in today's Information Society, it is a much more tenuous truth.

There is more information about us flowing about than ever before, and it can be obtained and used in countless ways. It can be used for our benefit and the benefit of others, but it can also be used to manipulate us.

But the important thing to realize is that it is our essence – what makes us distinct is what matters about us – and the ability to control that **is** everything….

And….

The key privacy point that I'm trying to make here...to encourage you to conceive privacy differently – is not just a question of how to keep our vital information secure. It's about how our personal information is inherently connected to our autonomy as individuals in a world in which information exchange is the central feature of society and the economy. And to that end, these systems must be accessible to clinicians and to patients.

Yes, protecting information is, of course, vitally important.

BC's FIPPA and PIPA mandate it and require a high level of security safeguards to be in place

But we need to think of privacy in this more modern health information context where access – with all that entails – plays a vital role in privacy.

It's a modern concept but it's where we really need to get to.

We need interoperability between systems to facilitate this.

Interoperability is, I think, particularly important for rural areas in British Columbia.

If I'm a patient in Prince George who needs access to tertiary care, where am I getting that tertiary care? Vancouver, a lot of the time. Right? And that means that I'm moving from one health authority to another.

We need to have systems in place with the right controls that recognize and respond to that reality.

2. **Moving onto my second point…There is no such thing as the health information system – it's just the health system.**

I'd like to challenge the notion of a "health information system" – something separate from the healthcare system, more of a support function operating in the background.

Really, there is no such thing as a health information system.

Today's healthcare is less about the laying on of hands and administering medicines than it used to be.

It's about collecting information.

It's about sharing information.

It's about analyzing information.

Modern health care is an information science. And increasingly, it's a digital information science.

In that context, it's outdated to think of a health information system as separate from the wider system.

We don't have a health information system – we have a health system that needs information to function.

3. **Now, to point three: Virtual care is care, and it is integral to mainstream health care.**

We also need to shift our thinking when it comes to virtual health care.

We used to think of it as an alternative – a substitute for the preferred type of health care, which is in person. Ten years ago, when we talked about virtual care, it was about bridging geographic barriers to keep health services and ERs open, primarily in rural and remote areas.

Today, virtual healthcare care has been integrated into mainstream healthcare, in different ways, whether you live in a large city or in a rural setting. What we once called 'virtual care', is now just regular 'care' with a virtual element.

And the new frontier, wherever you call home, has moved towards wearables and a constant stream of patient-provided data as part of routine care.

For example, I have a device in my chest that syncs up with a device that sits on my bedside table and provides a continuous stream of data to my clinician.

Every step of patient care is becoming digitalized.

The role health information staff play within a health authority is becoming more and more critical - so much valuable information is passing through your hands and being managed by you.

Take AI Scribes, for example. Our office is receiving an increasing number of questions about these tools, which use generative AI to listen to, transcribe, and summarize real-time conversations between patients and clinicians.

AI Scribes have exploded onto the scene in the last couple of years, particularly in family practice settings, where of course there is a high and growing administrative burden on physicians.

A 2023 survey of family physicians in Ontario found that the administrative burden was the #1 challenge impacting physicians' day-to-day work life. 94% felt overwhelmed with administrative tasks, which took up 40% of their work week.

So, it's no wonder clinicians and even patients are singing the praise of these tools.

They take care of chart notes and other documentation, while the clinician delivers more attentive and holistic patient care – an improved experience for both parties.

And cutting down on the administrative burden for overworked family doctors on the verge of burnout could become a valuable part of the solution to the healthcare crisis.

Here in BC, the AI Scribe Burdens Pilot is underway with 50 doctors to explore the potential for AI scribes to reduce physician burdens, with a focus on saving time and reducing stress for providers. A formal evaluation of the pilot expected to be available soon (February 2025).

Sounds great, right? A real win-win?

I am a techno-optimist, but there are some factors you should consider before using an AI Scribe.

First, with about 30 vendors vying for a piece of the market in Canada, know that AI Scribes are not created equal. The onus is on the practitioner or public body to ensure that AI scribes meet requirements under the applicable privacy Acts.

What questions should be asked before diving in?

Transparency with your patients is paramount. Many of the vendors themselves recommend obtaining express consent before using an AI Scribe in a consult. And I agree, express consent would be a best practice.

Is the AI Scribe you're considering an "open" AI system, where your patients' very private information is put into the tool to train the model, or is it a "closed" AI system, where the product arrives fully trained?

While closed systems are more privacy centric, there's still concern about bias and discrimination being built into the algorithm, and misinterpretations.

And of course, there are also concerns about data security – of the platform itself, but also how and where the information is transmitted.

What are the secondary uses of the data? Is the information being commodified - sold to third parties? Is it being sent across borders?

What about the retention of patient data - both by the platform, and within the medical practice?

Do you have a privacy management plan in place? Have you invested in adequate cybersecurity measures?

And finally, is there a human in the loop? These tools should augment professional judgement, not replace it.

This is particularly important to note. AI Scribes began as stand-alone applications, but now, some of these programs can also integrate seamlessly into electronic medical record systems.

They enable real-time data entry into the EMR and, potentially, provide suggestions for diagnosis, treatment, and prescribing…all of which raises a whole raft of new privacy, ethical, and legal questions.

So, in our digitalized healthcare system, I would say, just beware of function creep - the bar keeps moving at a rapid pace with these tools– they are evolving as I speak, and these shifts could fundamentally change both features and risks.

As I alluded to earlier, health information is different – it's important, it's precious to people, and they need to know it's protected.

In fact, it's critical for the provision of health care that people feel they can trust their health system to protect their privacy.

Which leads me to my fourth point…the necessity of social licence.

**4. The important of trust/social licence**

It's my view that we are still in the early days of the Information Society and our society's views on how our personal information should be handled are unclear.

In my line of work, people talk to me about personal information all the time, and it is not unusual for me to hear people express views like "privacy is dead"; "all of our information is out

there anyway"; and even "well today's generation wants all their personal information out there because they are dying to be noticed."

I believe people are now suffering from privacy fatigue.

They are close to giving up on the idea that their privacy can be protected.

At the same time, we are seeing optimistic signs that legislation is coming:

For example, Bill 25 in Quebec; the recent bipartisan attempt at privacy legislation in the US; the state level legislation on AI in the states (e.g. California); the number of state level child harm enforcement activities; the EU AI Act and, finally, hope for a new version of Bill C-27.

I am regularly confronted with people who feel extremely sensitive about their information and feel deeply betrayed and violated when they think it is breached. Not only can privacy breaches cause tangible harms – such as identify theft or embarrassment or discrimination – but they can cause people to feel a major harm to their sense of identity and autonomy and thus their membership in this society.

As I mentioned, I had the privilege to sit on the Expert Advisory Group on a pan-Canadian Health Data Strategy. One of the big takeaways from our report was that we need our health system to be person-centric.

We need to move from a provider-centric model to one that is centered on the needs of the people.

That is the focal point – the data is organized around the patient and follows the patient.

We must find a way to maximize the use of data for good, and we need to talk through the privacy issues.

This is something that is so personal – to the individual, to their families, and to their communities – that we cannot get ahead of where people are on these issues.

If we do, we risk repeating the mistakes of the past – and trust will become a casualty in the race ahead.

Our laws in Canada and internationally aren't there yet. They don't adequately deal with information from a perspective of privacy or ethics.

BC, in fact, is in the only province in Canada with no standalone health information privacy legislation – so this point is particularly salient to me.

…

The innovation is being rolled out at a very rapid pace.

We are in dire need of a regime that can grapple with these important questions.

What guardrails are there currently around the access to and use of that data by private companies for health research?

For instance, I wonder to what extent are people in BC comfortable with a for-profit company using their personal health information to train an AI Scribe model or other innovative technologies.

The research to date has shown that the public cares about how their health data are used.

When it comes to secondary uses of personal health data, most Canadians support use for research aimed at improving health and the healthcare system for public benefit, but reactions turn more negative when use is for private sector commercialization.

The boundaries of social licence for AI Scribes could get interesting. For example - what would the public think about a for-profit AI Scribe company using their personal health information to train the AI model and improve their commercial product, which will then circle back to improving services for patients and healthcare providers?

Public involvement and ensuring social licence are essential to building and maintaining trust as these game-changing technologies are adopted

These matters need to be debated in the public arena – people's trust is precious, and we cannot afford to break it, especially given the life and death stakes we're dealing with here.

Trust is important for all of us to talk about. It's a concept that resonates with everyone because we all know the feelings of trusting in something, not trusting in something or, even more pointedly, having our trust betrayed.

But I sometimes worry because trust can be an overly static and passive idea. Yes, when we use the word "trust," it is typically associated with assurances – for example, when financial assets are held in trust, there are rules and regulations about that. But oftentimes, the word trust is used without the idea that assurances are required – we have all trusted someone solely on the basis of their authority or position.

But "Just trust me" won't work here.

The concept that I like more is one that I think emerged from the natural resource sector. It is the concept of social licence – the notion that to utilize a resource you need to achieve and maintain the legitimacy of the project by the affected community.

I've been talking about the concept of social licence as applied to this sector for many years and increasingly I've seen others doing it too. I like that social licence adds a few things to the broader concept of trust:

- a notion of action – it is something that needs to be actively achieved;

- it involves *who* needs to be engaged – the affected community;
- and the licence needs to be actively maintained and monitored.

So how do we get this social licence? In three ways, I would argue

First, we need meaningful public engagement. I acknowledge that this isn't as self evident as it sounds but it is a familiar concept and there are many resources out there on it, so I won't dwell on it.

Second, we need independent, transparent and inclusive governance at multiple levels. Cumbersome? Maybe. Necessary? Definitely. If you believe in the potential of this new wave of care, then you must believe that it's worth it.

In December 2024, I joined other Federal, Provincial, Territorial Information and Privacy Commissioners and Ombudsperson to call for a new standard in government service. Together we urged our respective governments to take transparency by default into account in the early stages of designing any new systems, administrative processes, procedures, and governance models and to embed it in their day-to-day operations. Our resolution underscored the importance of access to information for the effective functioning of Canadian society and its democracy. Together, we called on Canada's governments to show leadership by making the modernization of legislative and governance regimes around freedom of information and protection of privacy a priority.

I think that we need this at the provincial level, provided for by statute; we need it at the institutional level – I mean universities, health authorities, and companies; and we need it at the individual project level.

Governance can be proportional, but it needs to exist. In my view it is essential to the role of stewardship.

I also believe that we need independent, transparent and inclusive governance of the secondary uses of health information at the provincial level – and for that to be grounded in legislation.

What do I mean by these adjectives:

- **transparent** as in according to established and accessible terms of reference;
- **independent** means ensuring that decision making is insulated from undue influence by those with a material interest in the outcomes of those decisions – and that might mean health care executives, governments, and companies;
- And **inclusive** means involving patients, caregivers, Indigenous peoples, independent experts.

Governance was often understood as “control of your information by us” but instead it needs to be conceived as “use of the data for all the things considered good….”

If our young people or anyone else feels that the right answer is a complete lack of governance then they are kidding themselves. The idea that absence of governance equals freedom is naïve. The absence of governance means that someone you CAN’T see is the one controlling the information, and that definitely NOT in your interests.

**And third, we need effective oversight**. OK, forgive me if that sounds a bit self-serving, but it’s not just OIPC privacy oversight I’m talking about. I am also talking about a strong and effective and efficient health ethics regulatory regime that is streamlined with privacy oversight. I’m talking about strong Indigenous oversight of Indigenous data.

There are lots of pieces to this puzzle, but with all of us working together, I believe we can devise effective solutions to meet the rapidly changing healthcare landscape.

Thank you again for inviting me here today, and to all of you for your attention.

Now I believe we have some time for questions…