UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK | NB-IRDT New Brunswick Institute for Research, Data and Training

Data Privacy- When Linking to Administrative Data, is Consent Necessary?

Lunch and Learn Session
May 12, 2021

Presented by Donna Curtis Maillet, PhD
Contact: NB-IRDTData@unb.ca

Video
(en anglais seulement)

Réseau de recherche sur les données de santé du Canada
Health Data Research Network Canada

I want to start by respectfully recognizing that UNB stands on the unsurrendered and unceded traditional Wolastoquey land and we are in the Peace and Friendship treatise territory and the land we are situated on is the traditional territory of the Wolastoqiyik, Mi'kmaq and Wabanaki Confederacy peoples. I also want to take a moment to recognize that what I'm going to be talking about today is a topic that I am quite passionate about, and someone here that I work with stated that I cannot package my passion for privacy. It's a lot of 'P's in one sentence but it's true. I'm quite excited about it. And part of our role as NB-IRDT contributing as a partner to the Health Data Research Network (HDRN), I'm able to work with privacy officers or privacy professionals across the country who are all interested in working on making administrative data available for research work but doing it in a way that is still mindful and respectful of individuals' privacy. And one of the issues that has come up for us, is a bit of a misunderstanding about when and how consent is necessary when using administrative data. The work that I'm presenting today really comes from initiatives through the HDRN and I want to give them full recognition for that, and the package that was sent out today should be available on the HDRN website soon, if it's not already. I was a little concerned that it might not be up there just yet, and this is a work that has been put together with my colleagues across the country over the last year. So full recognition to it was a big team effort. No talk on privacy can start without defining what we mean by personal information and personal health information, so let's just get that out of the way. So, we want to remember that personal information - we're talking about those really unique things about an individual that makes them "them": Name, age, identifying number, opinions, race, beliefs, blood types… all of this is personal information. And then, coinciding with that, we also have personal health information and that's a little just… focusing in on the health aspects. So physical or mental health, health history, genetic information, provider information, payments - who's paying for their health care, care eligibility… all of these are considered personal health information. And what we need to recognize is

often we use the term "personal information", but it is inclusive of personal health information as well. And why we have two separate definitions is because we have separate legislation for the two types of personal information. But if we are referencing or if I'm seeing today personal information, please know that it's inclusive of the health aspect as well.

So why are we collecting personal health information? Why are we giving it out? You know, what are we doing with personal information? So, let's just start with we know we give it out for to private businesses and for commercial purposes. We do our business, we do our banking, you know, service provision, anything like that. Purchasing, we're giving out our personal information along for those reasons. I mean, let's think about it, every time we want to go and purchase something on Amazon, it's getting our personal information. We're willing to share it for that reason. Another reason we give out our personal information, it might be for research work, questionnaires, interviews, focus groups, clinical trials… these are all reasons that we might be giving out our personal information. And we also give out our personal information to have access to services; so municipal, provincial or federal services - they all require information about us to provide those services. And I want to focus in on that because, oh yes… I've done a little bit of this (you'll get my teaching style here, I want you to just hold as a thought, research and public and administrative, just hold those thoughts just put them somewhere) and then what I wanted to focus on was administrative data because this is… Eva is actually the person that I first heard it explained this way, and I really like this expression that administrative data - all that information that we're giving to, whether it's the provincial government for services or to the federal government for services, it's creating a story of our lives and it's collecting all those bits and pieces from our birth. Taking us through our education, collecting information that way through health care, all of our information that's, as you know, from our provider's information (is there is there a question or anything there maybe just a late join-up) and then social services

anything that we might have along the way. Maybe we have interactions for in-family services, maybe we've reached out, maybe unfortunately we've had some situations with the criminal justice system, you know, different things like that. Anywhere that data about us is being collected and that carries right on through until death. And so, anything like that is all considered our administrative data. And I emphasize that because often, I know I'm not 100% sure of who our audience is today joining us for lunch, but I do know that a lot of us are aware of administrative data with respect to health but it includes everything around that might be gathered or collected through a government. And the other thing I wanted to highlight is personal information formats. And what I mean by that is to recognize we're saying that, you know, people are collecting our information… well they're collecting it and they're holding it in a certain way. And the first type is "Identifying Information". This is when we have those unique identifiers about us. This is the pieces of information that belong only to us. Snd so it might be our name: our name is uniquely ours; it could be our street address: you know, we're the ones that live at that address so it's going to clearly identify who we are. And then it goes into the things like our numbers, you know, our student numbers when we're students and our driver's license number and things like that - our SIN numbers, our Medicare numbers, those are all uniquely identifying to us but also uniquely identifying to us could be a bunch of information that's had, you know, sort of those unique identifiers removed, but if you put it together you could kind of figure things out. And what I mean by that is like, reasonably figure it out. And I call this the phenomenon of the maritime kitchen party and this is where you're standing around, you're all kind of …this is what we used to do before COVID remember you know, Saul's mask you know… we were able to chat around a kitchen and we would start talking and you'd say "oh my goodness, yes, my partner's brother knows somebody who knows somebody…" and then the next thing you know you know exactly who you're talking about. You've never exchanged a name, you've never exchanged any unique identifiers but because you've been foreseeably able to

re-identify someone, you're sharing personal information. There's a risk of re-identification there. And then finally there's also "de-identified information" that is truly, you know, the effort has gone into de-identifying. Now, the problem with this lovely definition is, and I always say nothing gets privacy professionals knickers more in a knot than talking about defining what we mean by "de-identified" and, unfortunately, there's no one shared definition, so we all have our own perspectives. But what is important to remember is de-identified means that those unique identifiers have been removed. We've taken out the names, we've taken out those unique numbers and what's left behind is not necessarily unique to one person, but it still presents a picture. So, if we take away, you know, my name you and still have my age, my health conditions, my education, that's all still my personal information, it's just been presented in a de-identified format and really it can be along a spectrum. And what I mean by that is that when we de-identify, we can truly de-identify, although it's getting harder and harder these days with tech-savvy folks out there, the naughty ones, what… the ability to completely strip, you know, like there's nothing left that would be able to trace back to an individual. That is anonymous, okay. And like I was sort of trying to joke there, it's really hard to have that situation and the world that we operate in when we're talking about administrative data and accessing administrative data for research, is often more of a pseudo-anonymous, you know, pseudonymous way of having the information. And that means that there's enough identifiable information there that allows us to do some meaningful work with that information. Because if it was truly anonymous, we wouldn't be able to join data sets together or we wouldn't be able to make some of the inferences and do the research work we can. So just to draw attention to that. Now, I've talked about this and I'm talking about this, you know, de-identified and personal information and stuff, so of course I have to speak to what are we going to do about protecting… oh yes, here's another piece for thought here: de-identified information, hold that one.

I have to speak to privacy because we have to recognize what we're talking about here and that is that privacy is a human right, okay. It is something that has to be protected across the board. And we have ways of doing it, we're very fortunate we're very resourceful as privacy folks, we have privacy programs and these are comprehensive and systematic programs of privacy protection, they include governance around information data management plans, policies and procedures, best practices and even having specific staff who are trained in certain ways. This is, for anybody who's interested, one of the C11… which is the new proposed federal privacy legislation, one of the new requirements that anyone handling personal information will require a program in place. We also have mechanisms of privacy by design, which is from a former Canadian privacy commissioner, Ann Cavoukian, and this is the concept of embedding privacy right into everything we do in our institutions and our handling of personal information or personal health information so that we, by default, are compliant with legislation and best practices. It's been a really popular way of practicing privacy around the world and it's been picked up, and it's even embedded in legislation in Europe, and then finally we have the privacy principles and these are our founding principles around privacy and there's a set of internationally accepted principles that even show up in like ISO standards and even the Canadian Standards Association and I know folks, if you've ever heard me talk before, I always emphasize these and I always ask people to stop checking their email when I run through these and I'm going to say it again here just, you know, pause for a moment and just visit these with me because these are really important principles, because they apply to the work we're talking about today, they apply to yourselves with your own personal information and how your information is accessed and used and disclosed to other people.

So first, accountability - if you're accessing personal information or personal health information, you are accountable for your actions. Straightforward. Identifying purpose - you cannot access personal information or personal health

information without having a purpose, there has to be a reason, it can't be just because you're curious, okay? That's why people are always getting caught and you hear these stories in the news. Limited collection - that means that when you are accessing that personal information or personal health information, it's limited to what you need for the purpose that you've given. So, you're not getting all the extra stuff, you see what you need to see, you have access to what you need to have. We limit use, retention and destruction… and so that means that we have a plan for that purpose that we've given, we're going to use it the way we said we would, we're going to retain it for the length of time we said we would and we're going to destroy it. So, here's some food for thought all those …like if folks here in New Brunswick, if you've been going out to dinner and you've given over your personal information, there is a plan in place for that information when they take your tracing information. They're using it for a purpose, they're supposed to retain it (I believe I'm going to get this wrong) I believe it's 28 days and then they're supposed to destroy it. Okay, so there's a plan. There's also safeguards and safeguards are perhaps a more familiar concept for folks and these are administrative practices, technical practices or physical practice that ensure the safety of personal information or personal health information and these are things like your administrative would be like confidentiality agreements and your physical is actually, you know, how you physically store personal information: where is it locked, in a locked room in a locked cabinet, and then of course your technical safeguards are the ones that we often hear about because this is the password protection and the way that we have our VPN clients or how data might be stored electronically we have consent okay. So consent is that ability to say what is happening and to your information how is it being used, who's using it, what are they using it for, that ability to say yes to that extremely important …this is the one that I always give the retailers a hard time about, why do you need to know my postal code? So, accuracy, if we are going to hold personal information and personal health information for a purpose, it has to be accurate. What is that purpose? Are we

going to be holding information to make policy decisions? Are we going to be holding personal information to provide health care? It needs to be accurate and true about that individual. We have to respect that. There's also openness: we can't be secretive what we're doing with personal information, you know, we have to be forthcoming. Why are we holding the data, what are we going to… how are we going to disclose the data? There we have to be very forthcoming with that information. And then we have to recognize that individuals always have the right to access their own information. If, you know, a retailer (picking on retailers here today) if retailer is holding personal information why like, you know, I want to know what it is, what do you have on me, that kind of information. This is the debates about Facebook and all those interesting things if you follow that in the news that's going on now, all the information collection that's going on. We have a right to know what it is and then finally challenging compliance - if you are uncomfortable with the way your information is being held, used, accessed, disclosed, you have a right to challenge that and we have mechanisms in our legislation and practices within our institutions that hold personal information and personal health information or government bodies that allow for us to challenge. So those are all the principles that we are always coming back to as privacy professionals and as we practice privacy just as individuals. And the one I wanted you to draw… the point that I want to draw here is of course consent, because that's what we're talking about today. Now these principles, they go on to inform for us legislation and policy that we follow very closely and so and what I mean by that is, I mean it literally, that the legislation in Canada is actually built on those principles even the current privacy legislation that would be applied to the federal government bodies actually even lists the privacy principles in it. It's a kind of an unusual way to approach legislation but they're listed right out so, and what I'm talking about here, because we're talking about NB-IRDT and the resources here in New Brunswick. So the legislation that we follow is, first of all, is the Right to Information and Protection of Privacy Act and that speaks to personal information the wider

personal information and then we have Personal Health and Information Privacy and Access Act and that act speaks very directly to personal health information and it also is where we are provided the authority to act as a holder or custodian of administrative data sets for research purposes, so it very much guides our work as an institution. And then we also have the Act Respecting Research which is a piece of legislation that I'm very proud that NB-IRDT was the leader in that, and we had a champion in the government who just really made it happen, but what this act did is it allowed us to have the capacity to hold data across different government bodies and be able to link data and that's, let's be honest, that's one of the big things that's what makes administrative data so interesting, so robust. So is that ability to link data sets and I'm going to touch on that a little bit more in a moment. And then, of course, we have policy and the guiding policy as researchers that we're following in Canada is the Tri-Council Policy Statement and that's the ethical conduct for research involving humans and the TCPS that came out 2018, this is where we are often turning for guidance on even on secondary use for accessing administrative data, that is included in this document as well. So very important guidance is provided to us from both of these two types of sources. Now and of course, I want you to remember those thoughts as well. So now, just for a moment, I've been talking about administrative data a little bit on the fringes but just to focus in so what we are talking about here today is, we are talking about administrative data, when we need to use it, when we want to use it we're going to be accessing it through a research data center like NB-IRDT as an example, there's other research data centers and research data administrative data places across Canada, I want to be mindful of that. Everybody's jurisdiction might be slightly different, we have other organizations that are all part of the HDRN we have ICES in Ontario we have the Health Data Nova Scotia we have SIDR in PEI which is Secure Island Data Repository, so we're there, we exist across the country so it's not just NB-IRDT, I want to emphasize that. But we have a role under legislation that allows us to provide that access for research work and it also gives us

specific directions and it says what we have to do and what we cannot do and when we can and cannot do things during the entire data life cycle. And that means, when I talk about the daily life cycle, it means from collection, so as we receive the data as a research center, as we access it for research purposes, our whole application process, if you want to use the data, how it's used, the actual research work that gets conducted, the disclosure, how are we sharing it, are we sharing it in research reports you know, how is it coming out and then finally how do we retain and securely dispose of that data at the end of its life cycle? So those are all obligations that we need to follow and we turn to legislation, we turn to privacy principles we turn to TCPS2 as well and then we have our safeguards as an institution, like as a research data center, we have safeguards in place we have policies we follow we have a physical site where you go in two-factor authentication and nobody wanders down our halls and just pops in for a visit, you know, those kind of things. And then finally the capacity for data linking and like I alluded to before this is this is the cool stuff right, this is that ability to take de-identified data and be able to join it, so we can take that picture of someone's life to bring it all together and say okay this is their education and if I pair it up with this particular you know with their health care or the health condition this is what I'm going to learn. So, this point here that I just want to be clear about, this linking or the joining of data is at the individual level and it can be across two or more data sets okay, just to emphasize that. And as well, we can link all de-identified data or we can also be linking de-identified data to identifiable data and this is why we're talking today, is because that is such an interesting thought. So, I want you to think for just a minute, all those things that we circled (oh data linking of course) we circled, let's put them together. We're talking about de-identified data, we're talking about the principle of consent, we are adding into it legislative practices we know we have to follow, we're following the Tri-Council Policy very important, really the guidance on consent comes from the Tri-Council, and then finally that data linking piece we want to link to something you know, we want that de-

identified data to be linked to something else and this is where the idea about consent comes in. Because we're very familiar I find, and I and I'm sorry if I'm pigeon-holing you into this group, we're quite familiar about the consent waiver possibility and what I mean by that as researchers, we're often told about administrative data and that capacity to link across multiple data sets and we know that under certain conditions we don't have to go back and consent and get consent or have consent to do that linking and that makes sense, I mean my goodness. We're talking about, that's one of the beauty of these data sets they're huge, they're massive but in reality there's a set of questions that actually need to be addressed before you even have that possibility of waiver and that is to ask has a research plan been reviewed by an REV, what do they think about waiving, you know, consent. Do you really need this data, you know, is this the data that you need to do the research work? Has that question been asked? Is it the the minimum amount needed to actually answer your research questions that you have? So, you know, you don't have to have a lot of information or, you know, are making sure that you don't have all this extra superfluous information. Are the data in the most de-identified form? So is it in a format that is nice and straightforward, you know, that you have removed all those identifiers that are not necessary. And then finally we have the word that everyone remembers is impractical - is it impractical to obtain consent and I mean thank goodness for that, really, because when you're dealing with hundreds and hundreds of records and, you've met all the other requirements, that's great. I mean, we don't want to have to go around and introduce bias to our research by asking folks for consent to look at de-identified data, but another set of questions we have to ask is what are the REB requirements? Maybe there is a consent requirement. Maybe it's that simple, because of the data that you're working with for the REB feels that it's appropriate and if that's the case, then that has to be respected.

Do you have contact with your participants? So let's say that you've only got a couple hundred people and there's an actual relationship there, a research relationship, that's another consideration where consent could be required. Because you have that contact, there's an ability there for you to ask for their consent for their information to be used. Are you thinking to link identifiable data to administrative data? And even though the unique identifiers might be removed, if you are linking… so let's say, we talked about earlier, primary collected research data… so if you are linking a questionnaire and maybe you want to make your study a little bit more robust. So you're going to add in some administrative data on that cohort, then you need to seek that consent. When you're getting consent for them to even participate in your study, you need to do it then.

Are you seeking to access, use or disclose data in a manner that requires consent? I think that is a wrong point, but are you thinking to access, use or disclose data in a manner that requires consent and legislation? That's right, I'm just getting ahead of myself. And so the point is there sometimes. In legislation it will spell out that if you want…. under certain conditions, so sharing. And if you're a researcher here in Canada and you've been working with administrative data and you've been involved in multi-jurisdictional research, you will know that data does not flow across borders. It just doesn't. And so maybe you're seeking consent to have the authority to do that; maybe you are doing a project, maybe you're involved in a clinical trial and all the data is going to be housed in one central location and so you need to spell out that information in your consent form. So, there's something there that has to be addressed. So this is another set of questions that I want you to ask yourself when you're preparing your research protocols and you're putting together your consent forms. Something to think about if there is going to be any kind any answers to these questions where you're saying "oh yeah, we are contacting all our participants", then this is what you need to ask.

Now, I want to build on this. Of course, this is kind of why we're here today and I want to start with a few guidelines. Consent is not a barrier and I think what happens is, we hear that and we think 'oh my goodness', but we just have to pivot, I love that coveted term "pivot", our thinking. Really, consent is going to facilitate ethical research. It says to people that you respect them and you want them to be part of their study, that you're building that trust with that participant. And you're going to find that people want to participate, they don't mind if they know what's going on and that's where those principles are so important. The consent, however must be explicit or informed consent, okay? So none of this implied business, none of this "well, you know, you tick the little box in the corner" you know, that kind of thing. That is not acceptable. Consent needs to be free and voluntary. It has to be able to be withdrawn at any time. We have to revisit consent and you have to revisit it often throughout your project, throughout relationships if you have interactions with your participants. They need to have that ability to withdraw and they need to know how they can withdraw informed consent. That's kind of a bit of a redundant there. We're talking about informed consent but it needs to be ongoing, so anything that changes in your protocol, any amendments that are made, that information has to be conveyed to the participants and they need an opportunity to withdraw or to reconsent. It needs to be clear and it needs to be documented, so very important. And I want to, just for fun, just for a moment, here's sort of a reality check to yourselves when I'm talking about that informed consent, how many times have you… and let's just say in the last week… given away your personal information without being informed? And I can tell you, I'm guilty. I'm absolutely guilty. I was giving this example yesterday. I signed up for my COVID vaccine and I just clicked on everything. I just wanted my vaccine. But when we go on the web and we choose those cookies and we say "oh yeah, cookie, whatever" you know, they do those nice little disclaimers and sometimes they put little happy faces and sad faces but we don't read it, so are we really

informed? No, not really. So it has to be meaningful and I'm going to talk about that. That's how we're really going to wrap up today's session is talking about that information.

I also want to point out that data sharing agreements must be in place between data business owners and data custodians or stewards. And my point about that for this guideline is: if you are sharing your primary data collection, if you're sharing identifiable information, even though you might have removed the unique identifiers and only have a study ID, if you're sharing it with another party to do that linking you must enter into a data sharing agreement. To do that you can't just hand it over, kind of thing, there has to be a proper agreement in place. There's also REB approval that has to be sought prior to the data linking. So what you have to do, is when you're putting in your application for the REB to approve, is that's when you need to say this is what we want to do, this is our intention, we're going to take this information and we want to link it to administrative data even if it's down the road in a couple years you know. Even if that's the intent, you need to be upfront about it and the REB needs to see that you're going to seek that consent when you're getting your consent. And speaking of that, consent for data linking is only one piece of the consent process and we recognize that consent forms, they're not easy because it's one of those things, you know, it's like trying to write poetry. You're trying to say in a concise, really meaningful way what you want to say but how do you get all that content in there? Do you really want people to read it so that they understand what they're consenting to? It's not easy and using clear and plain language is really the best advice that we can give, but also stay focused because, if anyone has participated in a clinical trial or just research in that area, you'll know the consent form obligations for the entire trial …it's ginormous. There's pages and pages and so it's a big ask to add one more layer. Oh and, by the way, we're also consenting to, you know, this portion as well, so we recognize that, but it doesn't mean we can skip over it.

So now what I want to just focus on are some of the things that I promised and that is: so what is that consent? So you want to link to administrative data, so what is that consent? What is it the content going to be? Well it has to include the types and the linking activity. So what are you talking about? We're going to be linking your test results. So yes, I have it right here in my hot little hands, the COVID vaccine consent form, you know, what are they going to do with it, kind of thing? They have to be clear about that, the data types and the linking activity that's going to take place. What are they linking it to, your administrative data and then what are the linkage options? So, how long, you know? So if the person, if they want to participate in a study but they're really not comfortable about this whole linking to their administrative data, can they opt out of that part and still be part of the study? So what are their options for the linking, is that the requirement to be in the study, kind of thing? There's use of personal and unique identifiers. So if you're using the Medicare, even if it's going to be observed it's going to be coded into another, which is what happens here at NB-IRDT, we have it masked. It's done for us by a third party, by the Department of Health and that becomes a unique identifier. We don't know who it belongs to, but we know we can use it. If that is what's being used, you need to state that, what personal identifiers being used, the linkage process. You need to explain that we are going to send your de-identified data to NB-IRDT and that's actually the next point, the steward that's going to be doing the linkage.

So what's going on there? Your unique identifiers are going to be sent to the Department of Health to be masked and then maybe your administrative data will be linked at the NB-IRDT, you know being clear about it. There's also linking from multiple stewards and this is to recognize that maybe we're in a situation where the possibility does exist in Canada. It's not so seamless here or possible in New Brunswick just yet, but it is possible elsewhere that you might have multiple stewards. So maybe you're in a research environment where multiple hospitals

are all participating and they're all going to bring the data into one place so you need to say that. You say it's going to be housed at this hospital and then it's going to be stored here over time kind of thing. And then linking to genomic data, this is really important. There's a whole suite of unique risks that come up around genomic data and it's a whole talk for another day, but the point is we don't know what the capacity of genomic data is. So in the absence of that, we privacy officers, we're all risk adverse. We like to think we're wild and crazy but really we're very cautious on some things when it comes to personal information. And so, genomic data, we want to be careful around that. Be upfront, what you're going to do. Are you building a genomic database? What are you doing with that individual's genomic information, and then we also have future contact with the participants. Are you going to be following up in 10 years? You're going to be following five years? Maybe two months? Maybe they are okay with a one-time interaction but they don't want to follow up with you, make sure that's included …linked data, years of inclusion. So let's say you're looking at Donna's life history here - are you going to be looking at from grade school all the way on up, kind of thing, or are you looking for just the last five years? Be inclusive, people have things you know that they might feel like sharing and not sharing, so that's important to be included.

Intended future use of linked data. So what do you want to do with this data? If you think there's something you're going to do down the road, I want to be very cautious about this. This is not an open thing: "…and we might want to use your data down the road…" know kind of thing. It's not like that. It's "we will be using it for this down the road". Because if you we say that "oh we might be using it down the road" or "it could be used" or whatever, that's not informed. People don't know what they're consenting to. So just important there. Or even "yeah we'll just leave it there"… data storage, disclosure, access outside of Canada, very important. Is this data going to be shared? Is it going to be going off for another study? Do they want to participate in that? Is that even an option?

Withdrawing linked data again… if there's a point at which people cannot withdraw their data, you need to say so. You're collecting all this primary data, that you're going to have linked to administrative data, that's going to go on for about a year but, after that point, it's going to be shared in a secure manner and it's going to be linked …well, then we're not going to know who belongs to what data at that point, so we wouldn't be able to withdraw it. So, you need to say, "at this point in time you will no longer be able to withdraw". You have to be clear about that. And a lot of these practices are the same through all our… all consent with research, with respecting individuals and then data retention reuse and destruction. And again, the where and the how: who's retaining it, is it going to be used/reused in any way? I want to know how long… at least for two studies or for one study? You know, all that has to be disclosed.

And then destruction, how is it going to be securely destroyed? You know, it's going to be held on for seven years kind of thing or for 10 years kind of thing. I'm still holding on to my data collection work that I've had, you know, waiting so I can throw out that box because I promised I'd hold on to it for 10 years, kind of thing. We're getting there. So those kind of things. That's really coming to the end here and I hope that I've been able to present for you that, while there's lots of possibilities around accessing administrative data and linking to it and particularly linking with some really interesting like maybe for other data sets around like questionnaires and clinical trials and surveys and there's so much we can do with administrative data. And that the first step is getting consent and then, once that consents in place, then you're good to go.

Other reports

autres rapports

Website

site web

Other videos

autres vidéos

If you have questions, or would like to know more about NB-IRDT visit us online or contact us:
506-447-3363 | nb-irdt@unb.ca | unb.ca/nb-irdt