Zoom Chat for "Legislative Roundtable: Draft Regulation on the anonymization of personal information in Quebec", held on 30 January 2024.

00:38:08 Attendee 1: Can't hear the speaker, there's an echo.

00:38:55 Attendee 2: coming through clear for me.

00:39:04 Attendee 3: Reacted to "coming through clear..." with 👍

00:39:07 Attendee 4: Reacted to "coming through clear..." with 👍

00:39:09 Attendee 5: Reacted to "coming through clear..." with 👍

00:39:17 Attendee 6: Reacted to "coming through clear..." with 👍

00:39:17 Attendee 7: Reacted to "coming through clear..." with 👍

00:39:25 Attendee 8: Reacted to "coming through clear..." with 👍

00:41:55 Attendee 9: It is unique, we do not have that in the FOIP Act in Alberta

00:42:13 Attendee 10: does it have a slightly different meaning in French? Legitimate seems more common and easier to interpret than "serious"

00:42:28 Attendee 9: Reacted to "does it have a sligh..." with 👍

00:43:38 Attendee 10: perhaps "serious" just means considered or deliberate

00:45:23 Attendee 11: Reacted to "coming through clear..." with 👍

00:45:37 Attendee 12: The Act uses the term in other contexts as well, so may appear to apply to any real business purpose? ss. 1.1 "1.1. For the purposes of this Act, any person who collects personal information relating to another person for a serious and legitimate reason is deemed to be establishing a file within the meaning of the Civil Code and the rights concerning such a file conferred by articles 35 to 40 of that Code apply to the personal information collected."

00:47:53 Attendee 13: As this session is being recorded, will it be made available for access later?

00:48:05 Attendee 14: Replying to "It is unique, we do ..."

Not yet! It is being updated at the moment. Lots of custodians/public bodies already have policies for non-identifying standards which causes havoc in ISAs.

00:48:27 Attendee 10: Reacted to "The Act uses the t..." with 👍

00:51:31 Attendee 15: Surely data can be rendered as 'statistics only' (including small cell controls etc) without reasonable potential for reidentification?

00:53:42 Attendee 15: Please confirm no consent required to deidentify under PHIPA?

00:55:35 Attendee 6: Will this draft document be available for us to look through, or just shown through Zoom here?

00:56:14 Attendee 15: PHIPA 11.2(2) permits custodians to use deidentified data to reidentify...

00:57:28 Attendee 11: Hi - nice to see you on! PHIPA Decision 175 goes into this matter in a lot of detail. HICs using PHI to de-identify is a "permitted use" under PHIPA but you do need to ensure 1. that the data is de-identified according to the standards/complies with PHIPA 2. Notice/Transparency as set out in PHIPA Decision 175 is implemented

00:58:32 Attendee 15: Replying to "Hi - nice to se..."

Hi - right, but its still not an absolute prohibition as we see here, correct?

01:00:54 Attendee 16: can you repeat what decision was recommended to review?

01:01:30 Attendee 11: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2022-23/pa_20230529_phac/

01:01:45 Attendee 17: Reacted to "https://www.priv.gc...." with 👆

01:01:52 Attendee 18: Reacted to "https://www.priv.gc...." with 👆

01:01:53 Attendee 16: Reacted to "https://www.priv.gc...." with 👆

01:02:20 Attendee 19: Thank you

01:03:14 Attendee 15: Please confirm that the regulator here intends that anonymized means 'not possibly re-identifiable', whereas deidentified means' positively potentially re-identifiable...

01:04:16 Attendee 20: "Best Practice" - By whose definition and standard?

01:04:25 Attendee 21: Reacted to ""Best Practice" - By..." with 👆

01:04:30 Attendee 22: Reacted to ""Best Practice" - By..." with 👆

01:04:41 Attendee 19: Reacted to "https://www.priv.gc...." with 👆

01:04:41 Attendee 23: Seems odd to not want regulation but at the same time wanting clarity. Why wouldn’t clarity come from regulation

01:04:47 Attendee 19: Reacted to ""Best Practice" - By..." with 👆

01:04:49 Attendee 23: Reacted to ""Best Practice" - By…" with 👆

01:04:58 Attendee 24: Reacted to ""Best Practice" - By..." with 👆

01:05:28 Attendee 20: Zero Risk is definitive, "Very Low Risk" is subjective. What is the criteria to confirm the risk is "Very Low" ... and not any greater?

01:12:09 Khaled El Emam: Replying to "Zero Risk is definit..."

There are specific thresholds for "very low" specified in the ISO standard and the Ontario guidance (they are consistent with each other).

01:12:34 Attendee 20: Replying to "Zero Risk is defin..."

Thank you!

01:13:33 Khaled El Emam: Replying to ""Best Practice" - By..."

One can argue that an international standard and guidance from other regulators would meet that definition, but there are also anonymization guidance documents from expert groups

01:14:23 Attendee 11: Reacted to "One can argue that a..." with 👆

01:16:15 Khaled El Emam: Replying to "Please confirm no co..."

PHIPA Permitted use
37 (1) A health information custodian may use personal health information about an individual,

01:16:41 Khaled El Emam: Replying to "Please confirm no co..."

(f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual;

01:16:51 Attendee 25: If I anonymise a production data set for use in a non-production. Since i still have the original data, is it legitimate to say that the data is not anonymise since there’s a way you can reidentify?

01:19:07 Attendee 26: HIPAA uses de-identification and it is data that isn’t re-identifiable, so it is anonymized.

01:20:13 Attendee 20: Where do we find specific cases to help determine whether we're in compliance with the "serious and legitimate" requirement?

01:21:05 Attendee 27: Reacted to "Where do we find spe..." with 👍

01:21:09 Attendee 20: If it is anonymized ... that doesn't help for purposes such as countering criminal activity for an identified individual?

01:25:06 Attendee 20: Replying to "If I anonymise a p..."

If you are retaining data (production or non-production data) beyond the period permitted by the Act ... it must be destroyed or anonymized (if you have a valid reason). Remember this also applies to not being able to infer the original data value of anonymized data.

01:25:44 Suzanne Morin: Replying to "Where do we find spe..."

there is no doubt that what is "serious and legitimate" will be interpreted by the CAI and the courts over time

01:26:01 Attendee 6: If the anonymisation assessment must take into account the "reasonably foreseeable circumstances", then wouldn't that be invalidated if the data controller changes the purpose and thus the "circumstances"?

01:29:05 Attendee 15: But surely a release to public would imply a possibly greater level of 'anonymization' than private release? If so, and those releases exist, what is the difference in the anonymization itself?

01:30:05 Attendee 28: Can you please share the document which is being shown here in the chat

01:31:43 Attendee 28: https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2023A/106606.pdf

01:32:02 Attendee 27: Reacted to "https://www.publicat..." with 👍

01:32:27 Attendee 28: Thank you

01:32:54 Attendee 19: Reacted to "https://www.publicat..." with 👍

01:34:05 Attendee 29: and what "problem/issue" are they trying to solve; what is the value-add?

01:35:29 Attendee 30: Reacted to "and what "problem/is..." with 👆

01:35:40 Attendee 15: If I counted the number of cases of COVID today (from some public or private source), without collecting any identifiers, why would that be any different than an anonymized data set derived from PI?

01:35:50 Attendee 12: If we take a step back and take a look at what appears to be an underlying concern - that in X years, there would be a new technological advance that would permit someone a higher probability of being able to link between data sets to re-identify someone, would that mean that the data set that had been anonymized in the past may no longer meet the "very low risk" threshold, and therefore would be reconsidered as personal information? Or, if the circumstances changes such that information that had a very low risk of re-identification when kept internally with safeguards, would now be made public where there are fewer safeguards? In those cases, wouldn't it make more sense to monitor the environment/circumstances for material changes to re-identification risk, instead of requiring organizations to regularly assess the information?

01:37:28 Attendee 20: Pam - Is Section 9 referring to an instance of a specific individual's personal information, as opposed to a grouping derived from multiple individuals? The latter does not carry risk of the individual's data being de-identified.

01:39:04 Attendee 19: The difficulties drafting regulations continue arise as we recognize the individual's ownership of their data and their right to be compensated and control the use of their data. Private use verses the use for the common public betterment become necessary to discern.

01:39:46 Pam Snively: Section 9 doesn't distinguish between those 2 things. Data "derived" from personal information is anonymized data under this legislation.

01:40:10 Pam Snively: That's my view.

01:41:54 Attendee 19: Totally agree with Khaled's comment.

01:42:08 Attendee 20: Replying to "That's my view."

Sure. Thank you for the reply. I guess it's open to interpretation. If we take the approach of 'anonymization' by grouping ... we could have case for remaining 'on-side' with the Act.

01:42:44 Attendee 26: HIPAA has two options: one is to have an expert with appropriate statistical knowledge do it and the other is to give a list of identifiers which, if all are removed, results in de-identification.

01:43:18 Attendee 26: Having a safe harbour option plus a statistical expert option would make for a better regulation.

01:44:02 Attendee 6: Replying to "HIPAA has two option..."

Note Safe Harbor (second option) also has the important clause that "The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information" - i.e. just redacting the listed variables is not necessarily sufficient

01:44:52 Attendee 26: Replying to "HIPAA has two option..."

Yes, but I've yet to see a case where that's been a problem.

01:45:14 Khaled El Emam: Replying to "HIPAA has two option..."

the safe harbor option does not ensure that the risk is actually very small and has not passed the test of time, but changing HIPAA would be very hard to do at this point to adjust SH

01:45:26 Attendee 6: Reacted to "HIPAA has two option..." with 👆

01:45:31 Attendee 6: Reacted to "the safe harbor opti..." with 👆

01:45:44 Attendee 24: Reacted to "the safe harbor opti..." with 👆

01:46:41 Attendee 22: Re Khaled's comment: When it comes to talent, anyone may hold themselves out as a privacy/access/data protection practitioner. The only formalized definition of competency is the Canadian National Standard of Qualification and Proficiency of Access-to-Information, Privacy, and Data Protection Professionals. The standard articulates the combined education, experience, knowledge, skills, proficiency, attitudes and judgment by which a practitioner's competency can be gauged.

01:47:01 Attendee 26: Replying to "HIPAA has two option..."

This part, at the end of the list of identifiers, is key:

Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

01:47:18 Attendee 20: Reacted to "Re Khaled's comme..." with 👆

01:47:21 Attendee 19: Reacted to "Re Khaled’s comment:..." with 👆

01:49:34 Attendee 28: Could Section 9 be seen as similar in part to GDPR Art.30 ROPA?

01:49:53 Attendee 26: Replying to "HIPAA has two option..."

The real weakness of the Safe Harbour option is that the resultant data pool may not be useful for use (e.g., where people’s ages are clinically important), so the statistical route is often used to get more robust data.

01:50:16 Attendee 11: Agree that Section 9 would be nearly impossible to implement when statistical data is used regularly in all types of evidence-based decision-making. For example, in healthcare when data is reported at all levels for a variety of different purposes

01:50:20 Khaled El Emam: Replying to "HIPAA has two option..."

that too

01:58:34 Attendee 20: I may be the outlier ... but section 9 makes sense to me. But I can't find a way to 'put my hand up' to speak

01:59:11 Attendee 29: and what value does it bring??

01:59:26 Attendee 31: Question for the panel: What is the relationship between consent withdrawal (if consent is the only basis for processing) and the scope of Art 23 and these regs? It seems Art 23 only permits anonymization where purposes are ‘achieved’.

02:00:55 Khaled El Emam: Replying to "I may be the outlie..."

the "hands up" is in the reactions at the bottom of the screen

02:01:20 Attendee 20: PI data should only be anonymized for "serious and legitimate' reasons. How do you track that the business is complying with this? What data is being anonymized? For what purpose? How is it being anonymized ... are the methods good enough? etc ...

02:01:36 Attendee 6: Question/case-study:

Someone does a section (7) assessment under certain "circumstances", which is e.g. a controlled environment where access is restricted. The data is then considered "anonymized", and so some data controller then decides that, as the data is outside of the legislation, it can be released to the public, beyond where the data was assessed to be anonymized, increasing the risk of re-identification beyond "very low". Without something like sections (8) and (9) (perhaps a modified version of it), is there anything explicit in this legislation to prevent that sort of thing?

02:02:22 Attendee 20: Replying to "PI data should onl..."

Where and how would that visibility to auditors ... without a formal means of recording and tracking such action

02:02:38 Attendee 32: Replying to "PI data should only ..."

IMO, that's where your Privacy Impact Assessment or similar process and supporting policies would come into play.

02:03:19 Attendee 33: so important to stress test section 9 with real life scenarios ..and to understand what a hurdle it risks constituting to essential decision-making/information dissemination

02:04:08 Attendee 20: Replying to "PI data should onl..."

Does the PIA process cover ALL requirements of section 9, sub-sections 1-5

02:05:42 Attendee 20: Replying to "I may the the outl..."

Thank you!

02:06:02 Attendee 34: Agree with PIA being that documentation

02:06:20 Attendee 32: Replying to "PI data should only ..."

You would need to determine what is in and out of scope of your PIA.

02:07:32 Attendee 35: In my opinion, Section 9 is in order. Privacy legislations are big on transparency. I understand that a PIA would likely have been completed before the latter anonymization, however, the anonymization increases the uses of this information (which by the way, is no longer personal information, but was derived from personal information). In my opinion, it provides individuals the ability to provide an informed consent when initially providing their personal information.

02:07:54 Attendee 11: Agree with Pam re scope and Adam re documentation. Documents are already retained in connection with the de-identification...

02:08:26 Attendee 20: Reacted to "In my opinion, Sec..." with 👍

02:08:41 Attendee 19: Reacted to "In my opinion, Secti..." with 👍

02:08:53 Attendee 36: Reacted to "In my opinion, Secti…" with 👍

02:11:27 Attendee 20: I don't agree with the view that Section 9 is superfluous. It has merit.

02:11:36 Attendee 35: Reacted to "I don't agree with t..." with 👍

02:11:38 Attendee 37: Anonymized information is never entirely outside the scope of the law - if the regulations are not complied with then the information again becomes subject to oversight.

02:11:42 Attendee 19: Reacted to "I don't agree with t..." with 👍

02:12:46 Attendee 6: Reacted to "Anonymized informati..." with 👍

02:13:02 Attendee 20: #2 addresses the question WHY you are anonymizing the data. That is a legitimate expectation to comply with the Act

02:13:25 Attendee 20: I would like to speak please

02:13:38 Attendee 27: To Keren's point on the use of the word "register", to what depth and degree is sufficient or acceptable with respect to penalties being applied should a description of how a data set has been anonymized along with what techniques were used?

02:16:43 Attendee 27: Replying to "To Keren's point on ..."

Noticed that my previous question was cut off:
To Keren's point on the use of the word "register", to what depth and degree is sufficient or acceptable with respect to penalties being applied should a description of how a data set has been anonymized along with what techniques were used is not deemed acceptable?

02:17:46 Attendee 38: How do biometrics fit into this? For example, facial recognition, utilizing the data to continue to enhance the algorithms for accuracy?

02:21:25 Pam Snively: documentation versus a register

02:21:33 Suzanne Morin: Reacted to "documentation versus..." with 👍

02:21:36 Katelyn Smith: Reacted to "documentation versus..." with 👍

02:21:42 Attendee 39: Reacted to "documentation versus..." with 👍

02:23:00 Attendee 35: Doesn't section 9 serve as a central and wholistic go-to location to view a body's anonymized data practices?

02:24:34 Attendee 40: Reacted to "If we take a step ba..." with 👍

02:27:35 Attendee 41: Will this recording be made available to participants?

02:27:38 Attendee 42: Excellent discussion. Thank you!

02:27:42 Attendee 43: Great discussion. Thank you to Adam and all the panelists!

02:27:51 Attendee 33: fantastic session - thank you very much

02:27:53 Attendee 41: Thank you.

02:27:56 Attendee 44: Thank you for the excellent discussion.

02:27:58 Attendee 45: Great discussion!

02:28:06 Attendee 30: Great Discussion, thank you!!

02:28:08 Attendee 20: Reacted to "Agree with Pam re ..." with 👍

02:28:12 Attendee 9: Interesting discussions! A lot of knowledge in this group!