OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

March 23, 2017

Dr. David Morgan
PHIA Review Committee
P.O. Box 8700
1st Floor, West Block, Conf. Bldg.
St. John's, NL A1B 4J6

Dear Dr. Morgan:

I note that the other Third Round Submissions in the *PHIA* Review process were all from Regional Health Authorities (RHAs), and furthermore a large proportion of their comments were in relation to recommendations which were made by the OIPC in its initial submission. Upon review and consideration of the comments offered by the RHAs, some clarification of the OIPC's position on these topics may be of assistance to the *PHIA* Review Committee.

One of the topics which attracted commentary from the RHAs was the recommendation by the OIPC that certain large custodians, including the RHAs, complete privacy impact assessments (under conditions explained in our submission) and provide those to the OIPC for review and comment. In our initial submission, we failed to note that there will be times when a preliminary privacy impact assessment (PPIA) would be sufficient. Section 2(w) of *ATIPPA, 2015* defines a PIA as "an assessment" but it does not specify a particular form or depth of analysis. Our conception of this process would be that this assessment can take the form of either a PPIA or a PIA as the circumstances warrant. As noted by the RHAs, PIAs are already a standard operational procedure, whether these be produced in cooperation with other RHAs or produced individually by one RHA. The word that is used by the RHAs in some of their responses is a "formal" PIA. The interest of the OIPC is in being able to provide input on the assessment which has been conducted by an RHA of the privacy considerations of an undertaking, whether that be a PPIA or a PIA. Our interest is in the content of the assessment, rather than the length or format.

Another point which we failed to address was brought to light in the concerns expressed about how our review process might result in slowing down the implementation of a new program or process. Of course, it is inherent in any PIA process that privacy risks may be identified and mitigation measures implemented to address those risks. That process may result in a delay whether or not the OIPC is involved. It is possible that through review by the OIPC that questions which had not been previously considered about a new program or process may be raised. The intention of raising such questions would be to ensure that the program or process is compliant with PHIA, and we do not expect that any of the RHAs would want to proceed with a program or process with unmitigated, unacceptable risks attached. In terms of the time required by the OIPC to review a PIA or PPIA and provide feedback, we can commit, and we would support this being incorporated into legislation, that our review, including any written feedback or commentary, will be provided within 30 days, with an extension of 30 days allowable only in extraordinary circumstances.

Another issue that was raised by the RHAs was in relation to our recommendation that the response time for an access request be decreased from 60 days to 30 days. Given the challenges currently faced by the RHAs in light of the added responsibility represented by our recommendation of PIA/PPIA review by the OIPC, we withdraw that recommendation.

P. O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 • Facsimile: (709) 729-6500
E-mail: commissioner@oipc.nl.ca • www.oipc.nl.ca

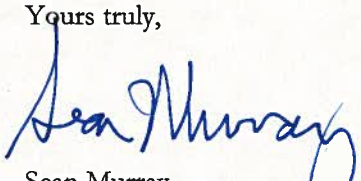
Central Health refers in its submission to "the current provincial fee schedule". It should be noted that there is no provincial fee schedule that applies to all custodians. There is a fee schedule that has been agreed upon by the RHAs, and in our Supplementary Submission on page 3 we support it. However, there is currently no guidance to all custodians as to what is considered to be a "reasonable" fee in accordance with section 57 of *PHIA*. There is some commentary by a couple of RHAs to the effect that there should be some element of cost recovery involved. In our Supplementary Submission we reference our Report AH-2012-001, which considers differing approaches to fees based on differing legislative language used in various jurisdictions. We stand by the principle that the most important factor is that the information being requested is in fact the personal health information of the applicant and assessing the reasonableness of the fee is an exercise that is primarily intended to be oriented towards the right of the applicant to obtain access.

Another comment offered in the recent submission of Central Health on pages 2 and 3 is in relation to a suggested revision to section 14(2)(b) where it is proposed that "in accordance with accepted professional practice" be added. This could be problematic. For one thing, the rationale assumes that accepted professional practice is potentially in conflict with *PHIA*, whereas our view is that *PHIA* was designed to be largely complementary to professional practice standards. The difficulty is that those standards are not spelled out in *PHIA*, but are included in other statutes and/or guidelines. Including such a provision may have the effect of undermining *PHIA* if there are differing views as to what may constitute accepted professional practice. Furthermore, in the case of serious breaches leading to prosecution, it may significantly hinder a prosecution if witnesses are brought in to testify that "professional practice" justifies the breach and/or are unable to agree on what it means in a given case. In the first prosecution undertaken in this Province under *PHIA*, the accused, who was a nurse, offered the defense that her inappropriate access was actually within the scope of accepted professional practice. She was found guilty of the offence, but if such a provision was added to *PHIA*, the line will become so blurred as to potentially preclude *PHIA* prosecutions involving registered health professionals.

Central Health also addressed our recommendation that all privacy breaches reaching the threshold requiring notification to affected individuals also be reported to the Commissioner. The point that perhaps could have been more fully addressed in our original recommendation was that the rationale for this is related to the ability of the OIPC to monitor compliance with *PHIA*. The value of breach reporting is represented not only in the details of a particular breach, but in being able to monitor and evaluate trends, and allowing this to inform training and education with the goal of preventing or avoiding similar breaches. This was also addressed by the *ATIPPA* Review Committee in the section entitled "Conclusion" on page 177: http://www.oipc.nl.ca/pdfs/ATIPPA_Report_Vol2.pdf. The Review Committee recommended that all breaches be reported to the Commissioner, and this recommendation was accepted and is part of the law. With regard to *PHIA*, our recommendation was that the OIPC only be informed of those breaches which meet the threshold of requiring notification to affected individuals.

I trust this additional input will be of some value. As always, if you have any further questions please do not hesitate to contact me.

Yours truly,



Sean Murray
Director of Special Projects