April 7, 2023

Financial Services Regulatory Authority of Ontario
25 Sheppard Avenue West, Suite 100
Toronto, ON M2N 6S6

Re: Comments on draft Proposed Information Technology (IT) Risk Management Guidance

Dear Sir or Madam:

TELUS Health (formerly LifeWorks) is pleased to provide the following comments to the Financial Services Regulatory Authority of Ontario ("FSRA") in response to the consultation on the Proposed Information Technology (IT) Risk Management Guidance (the "Proposed IT Guidance"). We specifically would like to provide comments with respect to how the Proposed IT Guidance impacts pension plans.

1. Implementation

The Proposed IT Guidance calls for a very short implementation period, with an effective date of June 2023. While we recognize that many pension plan administrators should already have practices and policies in place, almost all will need some level of change to be made to their governance policies. In addition to needing to complete a gap analysis and make applicable changes, pension plans will need approval of the changes from their primary stakeholder (i.e. board of trustees, plan sponsor, unions, etc.). Such a short period in which to comply would force them to hold emergency meetings to align with the Proposed IT Guidance. This may place an undue burden on plan administrators, additional costs and many may not be able to make the changes in time.

Further, we believe that many pension plan administrators in Ontario have been delaying making information or cyber security related changes to their governance policies as they await the Canadian Association of Pension Supervisory Authorities ("CAPSA") Guideline on yber Risk for Pension Plans ("Cyber Risk Guideline"). Consultations on the Cyber Risk Guideline were completed last year and a final version has not yet been released. As a result, many plans have not turned their mind to cyber and information security best practices while they await the final release of the Cyber Risk Guideline. Introducing changes within a very short timeline may take many pension plan administrators by surprise, leading them to rush to comply and creating unintended consequences, such as the adoption of inadequate practices and policies.

Looking to the implementation timeline of the British Columbia Financial Services Authority (BCFSA) Information Security Guideline, which was released in October 2021, regulated entities and individuals were given one year to implement and comply from the time the final version was released. Based on our experience, we found that most plans were able to meet

this one-year deadline and all the plans we advised required some degree of update to their governance policies. Moreover, the updates were prepared weeks prior to board or other stakeholder meetings, giving them enough time to understand and implement the changes as needed.

TELUS Health recommends a longer and more reasonable implementation period of one year, similar to what was provided for by the BCFSA.

2. Reporting Material IT Risk Incidents

The Proposed IT Guidance requires that FSRA be notified of an IT risk incident that is material as soon as it is discovered. We would like to make the following comments regarding this requirement:

a) Reporting Requirement

We believe more information should be provided regarding the need to report a material IT risk incident to FSRA. For example, we understand that the Protocol for IT Risk Incidents would be activated; however, it is unclear as to what additional recommendations over and above those provided in the Proposed IT Guidance could potentially apply to a pension plan administrator as part of the Protocol for IT Risk Incidents.

In addition, should a pension plan administrator be found to have not complied with the Proposed IT Guidance or met the standards expected under section 30.1(2) of the *Pension Benefits Act*, would FSRA impose penalties?

TELUS Health requests that more details be provided regarding the Protocol for IT Risk Incidents so that pension plan administrators can ensure they are compliant.

b) Timing Requirement

The Proposed IT Guidance requires breaches to be reported potentially before enough information is available to properly complete a review. We appreciate that the timeline provided is "as soon as possible" instead of outlining specific time periods. However, we are concerned that valuable time that should be spent on controlling and minimizing the breach may be impacted. The immediate response should be to quickly address the IT risk incident by placing all efforts and necessary personnel into controlling, stopping and mitigating the breach.

In addition, without enough information early into an IT risk incident there may be an initial determination that an incident is material, and later found that it is not, resulting in resources being wasted. On the other hand, it is also not clear what the repercussions may be for initially determining that an IT risk incident is not material and having to report it to FSRA at a much later time once it is determined that the breach was in fact material.

We also note that the Proposed IT Guidance is more onerous than the breach reporting requirement under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), which requires breach notification "as soon as feasible after the organization determines a breach has occurred, even if not all information (e.g. the cause, or planned mitigation measures) is known or confirmed."[1]

[1] *PIPEDA breach report form*, https://www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf

TELUS Health recommends allowing the organization enough time to control and understand the breach in order to complete an informed analysis of whether the breach is material by adopting the same requirement as the Privacy Commissioner of Canada (the "Privacy Commissioner"), that is, reporting a material breach "as soon as feasible after the organization determines a breach has occurred, even if not all information (e.g. the cause, or planned mitigation measures) is known or confirmed."[2]

c) Co-ordination with federal Privacy Commissioner reporting requirements

It is unclear whether an IT risk that requires reporting to FSRA as well as to the Privacy Commissioner would be coordinated or communicated between the two parties. It is important that the pension plan administrator not be tied up in communicating to two separate bodies in addition to trying to contain, stop and mitigate the breach.

TELUS Health requests that there be an attempt to work with the Privacy Commissioner where appropriate in order to ensure a streamlined response is provided and less burden is placed on attempting to comply with two different regulatory bodies.

3. Proportionality

The Proposed IT Guidance provides that a principle-based approach would allow flexibility to better achieve the outcomes in a matter that is suitable for the size and nature of the business. While we believe that this is critically important given that there are different plan sizes and circumstances, there needs to be a minimum standard that is adhered to. For example, no matter the size and circumstances of the plan, when an employee changes jobs there should be control measures in place to ensure that their access to information is reviewed and adjusted.

TELUS Health recommends releasing a guide with best practices to be followed as a minimum standard.

4. Harmonization

As mentioned, many Ontario plans are currently awaiting the release of the CAPSA Cyber Risk Guideline. While the Proposed IT Guidance addresses the need for pension plan administrators to determine familiarity with the CAPSA plan governance and other applicable guidelines, we would like to ensure that there is harmonization in order to reduce the burden of complying with multiple guidelines.

Conclusion

TELUS Health appreciates the opportunity to provide comments on the consultation and we hope that these comments are helpful in furthering the review of the Proposed IT Guidance. If you have any questions regarding our comments, please do not hesitate to contact us.

Sincerely,

Barbara Walancik
Principal
barbara.walancik@lifeworks.com

Teri Truong
Legal Consultant
teri.truong@lifeworks.com

[2] *Ibid*.