Meeting #4 Summary

Date held: July 22, 2015	**Time held: 8:30 AM – 2:15 PM**	**Location held: IESO Adelaide Offices Toronto, ON**
Working Group Members and Observers	**Company Name**	**Attendance Status** (A)ttended; (R)egrets; (S)ubstitute; (P) Phone Participant
Adam White	Aitia Analytics	R
Jeff Evenson	Canadian Urban Institute	R
Rob Kerr	City of Guelph	R
Sarah Griffiths	EnerNOC, Inc.	A
Jennifer Gordon	Halton Hills Hydro	A
Christine Dade	Horizon Utilities	A
Sally Barakat	Hydro Ottawa	A
Janet Gore (Observer)	Information & Privacy Commissioner	A
Renee Barrette (Observer)	Information & Privacy Commissioner	R
Stuart Smith	London Hydro	R
Karen Carter	Ministry of Education	A
Brian Byrnes (Observer)	Ministry of Energy	R
Guy Newsham	National Research Council	A
Jessica Webster	National Resources Canada	A
Marisa Uchin	Opower	P
Adriana Gliga-Belavic	PricewaterhouseCoopers LLP	A
David Craig	PricewaterhouseCoopers LLP	A
Gord Ellis	Soft Grid Analytics Corporation	P
Kevin Myers	Veridian	A

Foundation Project Team	Company Name	Attendance Status (A)ttended; (R)egrets; (S)ubstitute; (P) Phone Participant
Lisa Barnet	IESO	A
David Barrett	IESO	A
Simon Geraghty	IESO	A
Bob Guberman	IESO	A
Ryan King	IESO	A
Julia McNally	IESO	A
Przemek Tomczak	IESO	A
Chris Tuff	IESO	A
Doug Thomas	IESO	R
External Attendees	**Company Name**	**Attendance Status** (A)ttended; (R)egrets; (S)ubstitute; (P) Phone Participant
Gary Michor	Screaming Solutions	A
Samira Viswanathan	Bruce Power	A
Afreen Khan	Electricity Distributors Association	A
Please report any corrections, additions or deletions to: stakeholder.engagement@ieso.ca		

Please note that the views represented in the summary below reflect the diverse views of members of the FWG and not necessarily those of the IESO. Links to the presentation materials are provided with each item.

Item 1 Introduction/Opening Remarks for FWG Meeting #4

The IESO provided opening remarks for FWG Meeting #4.

Item 2 Review Proposed Recommendations on Data Enhancement
http://www.ieso.ca/Documents/consult/Foundation/Foundation-20150722-FWG_Geolocation_and_Occupant_Change_Recommendation.pdf

The FWG reviewed and adopted the above recommendation. Subsequent to its adoption, a working group member suggested that in addition to street name, street direction be included in the street address information. The Working Group members and the IESO agreed that this is important and it would be incorporated in the final recommendation.

Item 3 Framework for De-identification of Data
http://www.ieso.ca/Documents/consult/Foundation/Foundation-20150722-De-identification.pdf

The IESO presented the Framework on De-Identification. The objective of this session was to seek input on the proposed de-identification principles and process elements. The following discussions and input ensued.

- From the last working group meeting, the IESO incorporated feedback from the expert panel and reference material. It was noted that the healthcare sector has significantly more experience and practice with de-identification issues.
- The IESO clarified that identifiable information will be used as an input to any de-identification process and that controls would be put in place to keep the identifiable input data secure. This is captured in the principles section of the presentation materials.
- A working group member suggested that identifiable data not only be held securely with access restricted to authorized organizations and users, but also only be accessible for authorized purposes.
- The IESO clarified it would establish a risk threshold to re-identification. The data custodian would assess each request against the threshold and make a determination whether to fulfill the request. A working group member noted the health care sector has bodies that assess re-identification risk to determine if requests are fulfilled.
- Several meeting attendees requested clarification of the governance and accountability of the de-identification process. The IESO clarified that it is developing a framework to inform whatever entity will define the process but that defining the process is not within the scope of the Foundation project.
- A working group member raised the issue that data de-identification needs to be done in a standardized way. It was noted that different de-identification techniques could be necessary for different requests, and that a standard process could be developed, the execution of which would determine the specific data de-identification technique to be applied to service each request. It is expected that standards and techniques would evolve over time.
- A question was raised about who will be the data custodian and would be doing the data de-identification. It was clarified that for the Foundation project the IESO would be the data custodian and would handle MDM/R data requests. If a request was made for a single LDC's data, then the LDC could handle that data request.
- A working group member suggested adding the following language to one of the data de-identification principles (*italicized)*: "Enable appropriate *collection*, use, *storage, and disclosure* of data while maintaining public trust, privacy, *integrity, availability, and confidentiality*."
- It was noted that the IESO would have to be transparent about the process used to de-identify data without providing a roadmap on how to re-identify the data.
- A question was raised whether data collection should be included in the de-identification principles. It was noted that in the healthcare sector they did not specifically reference data collection.
- A working group member suggested adding the wording to the principle (*italicized)*: "Manage risk of providing data access and minimize those risks where possible, while acknowledging that risks cannot be entirely eliminated *according to the framework*."

- The IESO clarified that the data being discussed only includes data currently being collected and stored in the MDM/R and that the transformed and de-identified data could be stored outside the MDM/R. A working group member suggested noting that not only identifiable data, but also de-identified data, be held securely with access restricted to authorized organizations and users."
- It was clarified that adding address and occupancy change information to the existing MDM/R electricity consumption data makes it more useful, even if not combined with other data sets. The potential to combine MDM/R data with other data is outside the scope of Foundation and is part of MDAP. The discussions on Foundation scope are about a framework to de-identify data that is already in, or would be added to, the MDM/R and to establish general principles and processes. A working group member suggested clarifying this assumption in the presentation to help frame the discussion.
- The IESO clarified that, under Foundation, address and occupancy change information are the only additional data being added to the MDM/R and that the addition of other data sources to the MDM/R would not fall under Foundation. A working group member suggested adding language describing "these principles only apply to data in the MDM/R and if other data sets are considered the principles need to be revised."
- The IESO clarified that address information may be considered personal information according to the *Freedom of Information and Protection of Privacy Act*.
- The IESO clarified that data requesters could make requests for themselves and on behalf of other recipients, which would also receive the resultant information. The framework for third party access would require the requester to identify all other recipients of the data.
- The IESO clarified that the process requirement "Define the activities for managing and fulfilling data access requests." would have to be undertaken each time the dataset changes.
- A working group member suggested adding a definition for "data utility." The IESO clarified that data utility refers to the purpose for which the data will be used for and the minimum dataset that's useful for analysis. A working group member suggested using different language when referring to data "utility," so that this the word "utility" is not confused with "LDC." It was agreed that "usefulness" or "usability" or something along similar lines would be used instead.
- The IESO clarified that the process requirement "Require the identification and classification of data fields that are direct identifiers and quasi-identifiers." refers to the data; the process requirement "Determine the acceptable data utility for each data access request." refers to what the data requester wants to use the data for.
- The IESO clarified that the word "disclose" in the process requirement: "Document and disclose the de-identification methodology without exposing specifics that could lead to re-identification." would mean disclosed to the data requester. For better clarity, future uses in this context will substitute an equivalent descriptor for "disclose".

- A working group member suggested that the following language be added to the process requirement (*italicized*): "Periodically review the process and methodology against current and foreseeable threats *and known vulnerabilities as they evolve*." It was suggested that an independent audit be used to review the process and methodology.
- Working group members raised questions regarding the de-identification process requirements about inherent risk assessment. It was suggested that this requirement include language that describes both internal and external inherent risks. The IESO clarified that risk is to be assessed for each data request, including considering requestor risks and the risk that de-identified data could be re-identified by matching with other data sets. Further, the IESO noted that for each request, the end-users, the conditions and the cost to fulfill the request will all be considered.
- A working group member suggested there was a need to plain-language some of the terminology used throughout the framework for de-identifying information. The individual also suggested that a front-end "context and assumptions" slide in the presentation would help frame the conversation around some of the process requirements.
- A working group member suggested including examples of data transformation to help clarify the process requirement "Define a set of data transformations for de-identification to reduce the risk to an acceptable level."
- The IESO noted and clarified that it is acceptable that a risk threshold should be established and that it is acceptable to decline a data request if the risk to re-identification exceeds the threshold. A FWG member noted that the risk threshold could vary, depending on who was requesting the data and its intended use. Residual risk should be reviewed and re-evaluated on a periodic basis. This should be called out as a separate step in the process requirements.
- A working group member asked a question on the cost to fulfill a data request. The IESO noted that the risk to re-identification would factor into the de-identification techniques applied, which would in turn influence the cost of the process. The IESO suggested that issues related to: the evaluation the costs, the tradeoff between processes that could be used to minimize costs but could affect the quality of the results, how the service is funded, and whether to fulfill the request based on the cost, would all have to be determined. These are outside the scope of Foundation, but these details would have to be undertaken as part of any implementation of a data de-identification service.

Item 4 Framework for Rules for Third Party Access to Data
http://www.ieso.ca/Documents/consult/Foundation/Foundation-20150722-Third_Party_Access_Framework.pdf

The following discussions took place for each third party access scenario presented.

Scenario 1 – Downloadable Standard Reports from a Public Website

The FWG discussed the importance of machine-readable and standard formats for sharing data. Attendees noted that releasing standard reports with a consistent periodicity is important to improving their usefulness. Meeting attendees also noted that statistically relevant sample data for regular reports would work in most cases. One example mentioned, containing only MDM/R data, was a standard report providing hourly or daily energy consumption by location (i.e. at a municipal or regional level). Other examples of reports were given that included elements not part of the MDM/R (i.e. building type and industry sector). While the IESO recognized the value of reports segmented using these elements, they are not part of the Foundation scope.

Scenario 2 - De-Identified Data Requests That Are Fulfilled By The Data Custodian

The FWG discussed:

- Whether all third parties could request data in this way;
- The Data Custodian should consider risk of nefarious use of de-identified data to make a determination whether to fulfill the request;
- Examples of appropriate and inappropriate use of the data.

Scenario 3 - Personal Information Requests that are Fulfilled by the Data Custodian

General consensus from the FWG was that most use cases would not require personal information from the MDMR to be disclosed. However, some use cases would and in such scenarios, those requests would be better served through the LDCs who already have allowances in their licenses to use personal information for certain purposes, such as Conservation and Demand Management (CDM). Furthermore, all the LDCs present indicated that if any problems arose from the provision of their customers' personal information, regardless of the circumstances, they would be held responsible and accountable by their customers. Therefore, they needed to be involved when any of their customers' personal information was being disclosed to third parties.

The FWG discussed who owns the data in the MDMR, (the customer, the LDC or both), how requiring consent for each disclosure would increase cost dramatically, and what party would be vetting the third party requesters (the IESO as the Data Custodian). Some FWG members also noted that the core guiding principle for decisions on whether to disclose personal information should be whether it is in the greater public interest and benefit. A suggestion was made that any use of personal information be communicated to the LDCs involved so they can answer questions and keep track of initiatives to respond to public concerns.

Scenario 4 - Data Access Requests fulfilled using a Portal or Interface for use by Authorized 3rd Parties

The FWG identified that this scenario is similar to scenarios 2 and 3, but would be self-served by an authorized third party. A meeting attendee noted that having automated request and delivery of any data shared would be a huge benefit.

A Working Group member identified a fifth Scenario that would be de-identifying and making available the entire MDM/R energy consumption data set, but it was also noted that the degree to which it might have to be de-identified might render it of little use. Furthermore, the size of the data set would require significant resources dedicated to making it available on a continuous basis.

Other comments included:

- Applicable to all scenarios:
  - As data becomes more valuable, risk of theft increases.
  - Increased adoption of standards increases the value of the data and the benefit to the public.
  - Availability of the IESO's wholesale energy market and power system data (already available from the IESO), along with the MDMR data, could be very useful.
- (Scenario 3) If third parties can access personal information, even with adequate controls, and terms and conditions in place, still have to consider the cost to rate payers. Increased security measures mean greater operations costs.
- (Scenario 4) Any implementation of this should be done in phases, starting with a pilot.

Item 5 Wrap-up and Next Steps

To keep to the schedule of the Foundation Project an additional meeting of the FWG was agreed for August 18, 2015. This meeting was subsequently cancelled with the expectation that the necessary progress on the Foundation Project recommendations could be accomplished through e-mail communication without having to impose an additional meeting on the members of the FWG.

Action Item Summary					
#	Date	Action	Owner	Status	Comments