Appendix B – Preliminary Analysis Questionnaire

Instructions:

- Save the Preliminary Analysis Questionnaire as a separate document before completing.
- Enter your answers in the shaded areas.
- Reference the relevant note at the end of the questionnaire for explanatory information related to the headings and questions.
- Attach supporting material, as necessary.

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
PART I		
GENERAL		
1.		Project Title[1]
2.		*Google Apps for Education for McMaster Undergrad Students*
3.		Program Name (if relevant)[2]
4.		N/A
5.		Institution (include ministry, branch, division, as applicable)
6.		*McMaster University*
7.		Business Owner Contact Name[3]
8.		*Julia Kraveca*
9.		Business Owner Contact Job Title
10.		*Manager, Client Services*
11.		Business Owner Contact Business Email
12.		*Kraveca@mcmaster.ca*
13.		Business Owner Contact Business Telephone Number
14.		*905-525-9140, ext. 23678*
15.		Cluster Contact Name (if relevant)
16.		N/A
17.		Cluster Contact Business Email (if relevant)
18.		N/A
19.		Cluster Contact Business Telephone Number (if relevant)
20.		N/A
21.		Project following Cluster or Corporate Architecture Review Process (Please identify the relevant checkpoint and date of review — scheduled or completed)
22.		N/A
23.		Project following I&IT Project Gateway Review Process (Please identify the relevant gate and date of review - scheduled or completed)
24.		N/A

25.	**Describe your PROJECT.**[4]	
26.		McMaster undergraduate email system is in urgent need of technological currency. It is currently offering 15MB of storage to each student and resides on Communigate Pro system. Adding more space and additional functionality to the email system are the key requests from students. McMaster's CIO has explored options to upgrade the current email system and it proved to be too cost prohibitive. Given that other Canadian Universities are thinking or going into a hosted solution and having an opportunity present itself, the CIO, in conjunction with McMaster Student Union (MSU) have decided to migrate the current student email accounts and content to Google Apps for Education. Google Apps provides not only the exponentially increased size of the Inbox (7GB) but also additional features that students did not have before, e.g. calendaring, document management. MSU has run a survey with undergraduate population at McMaster (approx. 30,000 students) resulting in students' overwhelming support to move to Google Apps for Education.

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
27.	**Which of the following describes your project's impact?** (Check all that apply)[5]	
28.	X	Substantive change in the amount of personal information (PI) collected, used or disclosed
29.		Substantive change in the type of PI collected, used or disclosed
30.	X	Substantive change in the business processes affecting the collection, use or disclosure of PI
31.		Creation or modification of a database(s) containing PI, or the creation or modification of associated applications(s)
32.	X	Processing or storage of PI that may be outsourced to an external or third party service provider[6]
33.		Acquisition of commercial software (e.g., application) and/or hardware that offer little or no opportunity for customization of PI processing functions[7]
34.		Acquisition of commercial software (e.g., application) and/or hardware for which PI processing functions can be customized[8]
35.		New development of one or more applications using tools and methods that provide flexibility in the design of PI processing functions
36.	X	Acquisition of IT services or consolidation of IT services[9]
37.		Acquisition of non-IT business services[10]
38.		All changes UNKNOWN at this time
39.		Other (Please specify)
40.		
COLLECTION OF PERSONAL INFORMATION (PI)		
41.	**What kinds of PI will be COLLECTED?** (Check all that apply)[11]	
42.		name[12]
43.		personal address
44.		personal email address[13]

45.		personal telephone number
46.		race
47.		national origin
48.		ethnic origin
49.		skin colour
50.		religion
51.		age
52.		date of birth
53.		sex
54.		sexual orientation
55.		marital status
56.		family status
57.		education

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
58.		medical history
59.		psychiatric history
60.		criminal history
61.		employment history
62.		financial transactions involving the individual
63.		identifying number[14]
64.		identifying symbol[15]
65.		photograph of the individual
66.		other identifying particular[16]
67.		fingerprints
68.		blood type
69.		the personal opinions or view of the individual, except where they relate to another individual
70.		correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence
71.		the views or opinions of another individual about the individual
72.		PI not listed above[17] (Please list)
73.		
74.		NO COLLECTION of PI
75.		COLLECTION of aggregate, anonymous or otherwise de-identified information[18] (Please explain)
76.	X	*Username and Password. Password is not read or stored.*
77.		COLLECTION of PI UNKNOWN at this time (Please explain)
78.		
USE OF PERSONAL INFORMATION		
79.	**What kinds of PI will be USED?** (Check all that will apply)[19]	
80.		name[20]
81.		personal address
82.		personal email address[21]
83.		personal telephone number
84.		race
85.		national origin

86.		ethnic origin
87.		skin colour
88.		religion
89.		age
90.		date of birth
91.		sex
92.		sexual orientation
93.		marital status

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
94.		family status
95.		education
96.		medical history
97.		psychiatric history
98.		criminal history
99.		employment history
100.		financial transactions involving the individual
101.		identifying number[22]
102.		identifying symbol[23]
103.		photograph of the individual
104.		other identifying particular[24]
105.		fingerprints
106.		blood type
107.		the personal opinions or view of the individual, except where they relate to another individual
108.		correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence
109.		the views or opinions of another individual about the individual
110.		PI not listed above[25] (Please list)
111.		
112.	X	NO USE of PI
113.		USE of aggregate, anonymous or otherwise de-identified information[26] (Please explain)
114.		
115.		USE of PI UNKNOWN at this time (Please explain)
116.		
DISCLOSURE OF PERSONAL INFORMATION		
117.	**What kinds of PI will be DISCLOSED?** (Check all that apply)[27]	
118.		name[28]
119.		personal address
120.		personal email address[29]
121.		personal telephone number
122.		race
123.		national origin
124.		ethnic origin
125.		skin colour
126.		religion
127.		age

128.		date of birth
129.		sex

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
130.		sexual orientation
131.		marital status
132.		family status
133.		education
134.		medical history
135.		psychiatric history
136.		criminal history
137.		employment history
138.		financial transactions involving the individual
139.		identifying number[30]
140.		identifying symbol[31]
141.		photograph of the individual
142.		other identifying particular[32]
143.		fingerprints
144.		blood type
145.		the personal opinions or view of the individual, except where they relate to another individual
146.		correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence
147.		the views or opinions of another individual about the individual
148.		PI not listed above[33] (Please list)
149.	X	*Usernames, electronic content.*
150.		NO DISCLOSURE of PI
151.		DISCLOSURE of aggregate, anonymous or otherwise de-identified information[34] (Please explain)
152.		
153.		DISCLOSURE of PI UNKNOWN at this time (Please explain)
154.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
		PART 2
		COMPLETE THE REST OF THIS QUESTIONNAIRE ONLY IF THE COLLECTION, USE OR DISCLOSURE OF PI HAS BEEN IDENTIFIED IN THE QUESTIONS ABOVE
155.	**Have you completed the PIA or do you plan to do so?**[35]	
156.		Yes, a past PIA document is being updated now
157.		Yes, the Privacy Risk Analysis part of the PIA is being undertaken now
158.	X	Yes, the Privacy Risk Analysis part of the PIA is planned but has not yet been started
159.		No, the Privacy Risk Analysis part of the PIA is not planned
160.		Yes, the Privacy Design Analysis part of the PIA is being undertaken now
161.		Yes, the Privacy Design Analysis part of the PIA is planned but has not yet been started
162.		No, the Privacy Design Analysis part of the PIA is not planned (Please explain why not)
163.		
164.		Unknown at this time
165.		Other (Please specify)
166.		
167.	**What is the estimated total cost of your project?**[36]	
168.	X	Less than $100,000
169.		$100,000 to $1,000,000
170.		$1,000,001 to $10,000,000
171.		More than $10,000,000
172.		Unknown at this time (Please explain)
173.		
174.	**Has the relevant program area(s) had a privacy breach within the last year?**[37]	
175.		Yes (Please explain)
176.		
177.	X	No
178.		Unknown at this time
179.		Other (Please specify)
180.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
181.	**Will ANY of the following types of information be collected, used or disclosed:**[38] ! **credit card number** ! **social insurance number** ! **bank account number** ! **ATM card number** ! **any other identifier (not including name or contact information) (e.g., client or licence number)?**	
182.		Yes (Indicate which identifiers will be collected, used or disclosed)
183.		
184.	X	No
185.		Unknown at this time
186.	**Will ANY of the following types of information be collected, used or disclosed:**[39] ! **health card number (e.g., OHIP number)** ! **medical history, in whole or in part** ! **psychiatric history, in whole or in part** ! **medication history, in whole or in part** ! **laboratory test results** ! **diagnostic images** ! **immunization records, in whole or in part** ! **any public health information related to identifiable individuals?**	
187.		Yes (Describe the personal health information that will be collected, used or disclosed)
188.		
189.	X	No
190.		Unknown at this time
191.	**Which institutions of the Government of Ontario will be involved in this project?** (Check all that will apply)[40]	
192.		Aboriginal Affairs
193.		Agriculture, Food and Rural Affairs
194.		Attorney General
195.		Cabinet Office
196.		Children and Youth Services
197.		Citizenship and Immigration
198.		Community and Social Services
199.		Community Safety and Correctional Services
200.		Consumer Services
201.		Culture
202.		Economic Development and Trade
203.	X	Education

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
204.		Energy and Infrastructure
205.		Environment
206.		Finance
207.		Francophone Affairs
208.		Government Services (including ServiceOntario)
209.		Health and Long-Term Care
210.		Health Promotion and Sport
211.		Labour
212.		Municipal Affairs and Housing
213.		Natural Resources
214.		Northern Development, Mines and Forestry
215.		Office of the Premier
216.		Research and Innovation
217.		Revenue
218.		Seniors' Secretariat
219.		Tourism
220.		Training, Colleges and Universities
221.		Transportation
222.		Women's Directorate
223.		Other Government of Ontario agencies or organizations[41] (Please list)
224.		
225.	**Which institutions of the Government of Ontario will have access to or use the PI or the information applications, systems or services related to this project?** (Check all that will apply)[42]	
226.		Aboriginal Affairs
227.		Agriculture, Food and Rural Affairs
228.		Attorney General
229.		Cabinet Office
230.		Children and Youth Services
231.		Citizenship and Immigration
232.		Community and Social Services
233.		Community Safety and Correctional Services
234.		Consumer Services
235.		Culture
236.		Economic Development and Trade
237.		Education
238.		Energy and Infrastructure
239.		Environment
240.		Finance
241.		Francophone Affairs
242.		Government Services (including ServiceOntario)

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
243.		Health and Long-Term Care
244.		Health Promotion and Sport
245.		Labour
246.		Municipal Affairs and Housing
247.		Natural Resources
248.		Northern Development, Mines and Forestry
249.		Office of the Premier
250.		Research and Innovation
251.		Revenue
252.		Seniors' Secretariat
253.		Tourism
254.		Training, Colleges and Universities
255.		Transportation
256.		Women's Directorate
257.		Other Government of Ontario agencies or organizations[43] (Please list)
258.		
259.	**Will any of the selected institutions disclose the PI? (i.e., not just use the project's PI for own internal purposes)?**	
260.		Yes
261.	X	No
262.		Unknown at this time
263.		Other (Please specify)
264.		
265.	**How many organizations outside of the Government of Ontario will have access to or use the PI or information applications, systems or services related to this project?[44]**	
266.		0
267.	X	1 – 3 (Please list)
268.		*Google Inc.*
269.		4 – 10 (Please list)
270.		
271.		More than 10 (Please list)
272.		
273.		Unknown at this time
274.	**How many private sector organizations will be involved in the development or delivery of the project?**	
275.		0
276.	X	1 – 3 (Please list)
277.		*Google Inc. (SADA systems – potentially)*
278.		4 – 10 (Please list)
279.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
280.		More than 10 (Please list)
281.		
282.		Unknown at this time
283.	**Which of the following private sector organizations will have access to or use the PI of the information applications, systems or services related to this project?** (Check all that will apply)[45]	
284.		Private sector organization subject to Personal Health Information Protection Act (PHIPA)
285.		Private sector organization subject to Personal Information Protection and Electronic Documents Act (PIPEDA)
286.		Private sector organization subject to other Canadian privacy or health information legislation
287.		Private sector organization bound to FIPPA privacy requirements by contract
288.	X	Foreign organization not subject to any Canadian privacy legislation[46]
289.		Not applicable
290.		Unknown at this time (Please explain)
291.		
292.	**Which of the following categories of organizations will be involved in the development or maintenance of information applications, systems or services related to this project?** (Check all that will apply)	
293.		Private sector organization subject to PHIPA
294.		Private sector organization subject to PIPEDA
295.		Private sector organization subject to other Canadian privacy or health information legislation
296.		Private sector organization bound to FIPPA privacy requirements by contract
297.	X	Foreign organization not subject to any Canadian privacy legislation[47]
298.		Not applicable
299.		Unknown at this time (Please explain)
300.		
301.	**Will an external or third party provide information management functions or services that will involve the collection, use, disclosure, retention or disposal of PI?**[48]	
302.		Yes, a public sector organization subject to FIPPA, Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or PHIPA
303.		Yes, a public sector organization subject to other Canadian privacy legislation
304.		Yes, a private sector organizations with offices in Ontario

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
305.		Yes, a private sector organizations with offices in Canada, but not in Ontario
306.	X	Yes, an organization that may be subject to the USA PATRIOT Act or other foreign legislation with possible extra-territorial application[49]
307.	X	Yes, a foreign organization with no office in Canada
308.		No
309.		Unknown at this time
310.		Other (Please specify)
311.		
312.	**If more than one institution or other organization may have access to PI through use of the information applications, systems or services, will an agreement or other means of control be in place to ensure that FIPPA requirements and obligations will be met by all parties with access to the PI involved?**	
313.		Yes
314.	X	Yes, being developed
315.		No
316.		Not applicable
317.		Unknown at this time
318.		Other (Please specify)
319.		
320.	**Has the project been discussed with your institution's FIPPA Coordinator to address privacy requirements and measures, or do you intend to do so?**[50]	
321.	X	Yes, we have already discussed the project
322.		Yes, we will discuss the project later
323.		No
324.		Unknown at this time
325.		Other (Please specify)
326.		
327.	**Has the project been discussed with your legal counsel to address privacy requirements, or do you intend to do so?**[51]	
328.		Yes, we have already discussed the project
329.		Yes, we will discuss the project later
330.	X	Contact Randal Bocock
331.		Unknown at this time
332.		Other (Please specify)
333.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
334.	**What privacy and other legislation will apply to the project?** (Check all that will apply)[52]	
335.	X	FIPPA
336.		MFIPPA
337.		PHIPA
338.		PIPEDA
339.		Unknown at this time
340.		Other legislation (Please specify acts and provisions)
341.		
342.	**Will the PI be excluded from the application of FIPPA? (section 65)**[53]	
343.		Yes (Please explain)
344.		
345.	X	No
346.		Unknown at this time
347.	**Will the PI be maintained for the purpose of creating a record that is available to the general public? (section 37)**[54]	
348.		Yes (Please explain)
349.		
350.	X	No
351.		Unknown at this time
352.	**What will be the purpose(s) of the collection, use or disclosure of PI for your project, including consistent purposes?** (Please describe)[55]	
353.	X	Usernames are required for authentication. Electronic content will be stored on Google Inc. systems for e-communication.
354.	**What will be the authority for the collection of personal information? (subsection 38(2))** [56]	
355.		Expressly authorized by statute (Please specify act and provisions)[57]
356.		
357.		Law enforcement (Please specify nature of the law enforcement)[58]
358.		
359.		Necessary to the proper administration of a lawfully authorized activity (Please specify the activity)[59]
360.		
361.		Unknown at this time
362.	X	Other (Please specify)
363.		McMaster University Act 1976
364.	**How will PI be collected or compiled by the project? (section 39)**	
365.		Directly from the data subject[60]
366.		Indirectly with the individual's authorization
367.		Indirectly from a specified third party

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
368.		From a reporting agency in accordance with the Consumer Reporting Act
369.		Unknown at this time
370.		Another manner of collection (Please specify)
371.		
372.	**If collection will be directly from the data subjects will they be informed of the following? (section 39)** (Check all that will apply)[61]	
373.	X	The legal authority of the collection
374.	X	The principal purpose(s) for which the PI is intended to be used
375.	X	The title, business address and business telephone number of a public official who can answer the individual's questions about the collection
376.		Notice not required (subsection 39(3))[62]
377.		Unknown at this time
378.		Other (Please specify)
379.		
380.	**How will notice be given to data subjects?** (Please explain)	
381.		
382.	**If collection will NOT be directly from the data subject, will an indirect collection be authorized by any or all of the following?** (Check all that will apply)[63]	
383.		FIPPA (If checked, please specify provision)
384.		
385.		MFIPPA (If checked, please specify provision)
386.		
387.		PHIPA for personal health information
388.		Another act or regulation (Please specify act, regulation and provisions)
389.		
390.		Not applicable
391.		Unknown at this time
392.		Other (Please specify)
393.		
394.	**Will PI be used ONLY for the identified purpose(s) of collection? (section 41)**	
395.		Yes
396.		No (Please explain)
397.		
398.		Unknown at this time
399.	X	Other (Please specify)
400.		No PI will be used.

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
401.	**If no, explain authority. (section 41)**	
402.		
403.	**Will PI be used for a consistent or other purpose? (section 43)**	
404.		Yes (Please identify and explain consistent and other purposes)
405.		
406.		No
407.		Unknown at this time
408.		Other (Please specify)
409.		
410.	**How will you make sure PI is only used for the identified or consistent purposes?** (Please explain)	
411.		
412.	**Will the disclosure of PI be ONLY for purposes explicitly identified in FIPPA? (section 42)**[64]	
413.	X	Yes (Please explain)
414.		Only usernames and electronic content of one's email will be handled by Google Inc. The information has already been limited by handling the authentication process at McMaster and disclosing only usernames and subsequently storage of emails.
415.		No
416.		Unknown at this time
417.		Other (Please specify)
418.		
419.	**If no, explain authority.**	
420.		
421.	**Will PI be disclosed for a consistent or other purpose? (section 43)**	
422.		Yes (Please identify and explain consistent and other purposes)
423.		
424.	X	No
425.		Unknown at this time
426.		Other (Please specify)
427.		
428.	**How will you make sure PI is only disclosed for the identified or consistent purposes?** (Please explain)	
429.		Handling authentication process "in-house" prevents Google Inc. from getting passwords. Contract will be signed with Google Inc. to set the boundaries of their potential access to email content.
430.	**Will processes and procedures be provided to keep PI accurate, complete and up-to-date as needed for its intended purposes? (section 40)**	
431.	X	Yes (Please identify and explain processes and procedures)
432.		Account provisioning and administration process and procedure will be in place.
433.		No (Explain why not)
434.		
435.		Unknown at this time

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
436.		Other (Please specify)
437.		
438.	**How long will PI be retained? (section 40, Ontario Regulation 460, section 5)**	
439.		Not retained or used, flow-through model[65]
440.		Retained for one-time use only, then deleted or destroyed
441.		Retained for more than one-time use, but less than one year
442.	X	Retained for one year or more
443.		Unknown at this time
444.		Other (Please specify)
445.		
446.	**Do you have retention schedules for the personal information?**	
447.	X	Yes, in place
448.		Yes, in development or planned
449.		No
450.		Unknown at this time
451.	**Will individuals be able to request correction of their personal information? (section 47)**	
452.	X	Yes
453.		No
454.		Unknown at this time
455.		Other (Please specify)
456.		
457.	**Have you applied security classification to the personal information?**	
458.		Yes, classification completed (Please explain)
459.		
460.		Yes, classification underway or planned
461.	X	No
462.		Unknown at this time
463.	**Will PI be protected against risks such as loss or unauthorized access, collection, use, disclosure, destruction or modification? (Ontario Regulation 460, section 4)[66]**	
464.	X	Yes (Please summarize the security measures planned to be applied)[67]
465.		Contract with Google Inc. will be in place to put measures in place.
466.		No
467.		Unknown at this time
468.		Other (Please specify)
469.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
470.	**Have you discussed this project with security resources to address information security measures, or do you intend to do so?**[68]	
471.	X	Yes (Please identify and explain relevant security measures)
472.		IT Security Officer of McMaster University has been consulted. "In house" authentication addresses most of our information security concerns.
473.		No (Please explain why security measures not needed)
474.		Unknown at this time
475.		Other (Please specify)
476.		
477.	**Will a security threat/risk assessment (TRA) be undertaken?**[69]	
478.		Yes, it is done
479.		Yes, it is being prepared now
480.		Yes, it is planned but has not yet been started
481.	X	No, a TRA is not planned
482.		Unknown at this time
483.		Other (Please specify)
484.		
485.	**Will PI be appropriately disposed of? (O/Reg. 459)**[70]	
486.	X	Yes (Please specify)
487.		Contract with Google Inc. will address this.
488.		No (Please specify)
489.		
490.		Unknown at this time
491.		Other (Please specify)
492.		
493.	**How will you securely dispose of personal information?** (Please explain)	
494.		The contract with Google Inc. will specify their practice.
495.	**Will approved privacy policies and/or procedures be in place to protect PI associated with this project?**	
496.	X	Yes, they are in place (Please specify)
497.		McMaster University has general policies in place to address information security, access to it and electronic communication.
498.		Yes, they will be developed
499.		No
500.		Unknown at this time
501.		Other (Please specify)
502.		

Row #	Check shaded area with an "X"	Enter explanatory text in shaded areas
503.	**Will training and awareness programs be in place to provide appropriate staff and contractors with the necessary knowledge to protect PI associated with this project?**	
504.		Yes, they are in place (Please specify)
505.		
506.		Yes, they will be developed
507.		No
508.		Unknown at this time
509.	X	Other (Please specify)
510.		General communication will be issued.
511.	**Please outline any additional privacy assumptions or considerations related to the project.**	
512.		

Preliminary Analysis Questionnaire Notes

[1] The Project Title should be informative. If your project is related to a larger, approved initiative, include the name of the initiative. See Appendix A for definition of "project."

[2] The Program Name should be informative and indicate relevant program(s). See Appendix A for definition of "program."

[3] The Contact Name should be the person responsible for coordinating or completing the PIA process for the project. This person should be able to respond to questions about the project and related privacy issues.

[4] The project description should provide a broad, "big picture" and reasons for key changes. This part of the Preliminary Analysis is based on the assumptions about the direction of your project. Use the information available at the time of completion. The description may be included as an attachment.

Include the following information:
- overall project aim and objectives;
- parties/partners involved;
- links to government programs;
- significant business process changes and why;
- significant technology changes and why; and
- some of the key privacy elements (e.g., legal, policy, and technology).

[5] This question is designed to identify typical policy, program, business, or systems changes that may apply to a project and impact privacy.

[6] There are potential privacy risks when a project involves retaining an external or third party to provide information management functions or services that involve the collection, use, and disclosure of PI. The Guidelines for the Protection of Information when Contracting for Services provides guidance on addressing privacy in contracts.

[7] There are potential privacy risks relating to the degree of customization that commercial software (e.g., applications) or hardware offers. It is important to know if a product has privacy protective features built-in, or if it can be modified to include such features in order to meet the project's needs. The degree of possible customization may limit the ability to address potential privacy risks. Assess potential privacy risks against other advantages and costs associated with commercial software and hardware.

[8] See explanation for line 33 and note 7.

[9] See explanation for line 32 and note 6.

---

[10] See explanation for line 32 and note 6.

[11] This question is designed to help identify what PI the project plans to collect, if any. If your project is developing an application or system that will enable others to collect PI, complete the Preliminary Analysis with that fact in mind.

Under FIPPA subsection 2(1), PI means information about an identifiable individual. (See Appendix A for definition.) The list in the questionnaire includes specific types of PI defined under FIPPA, as well as other information that may be considered personal. A data element, on its own, may not be considered personal, but when you assess the type of data collected, consider whether an individual may be identified by combining several elements or types of information. The project may collect PI directly from individuals or get it from another organization or person. This is still considered a collection. FIPPA states that PI does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

[12] A name, where it appears with other PI relating to an individual or where the disclosure of the name would reveal other PI about the individual, is considered PI. A name by itself is not PI by definition.

[13] The Corporate Operating Policy on Internet Tracking Technologies states: "Government organizations shall consider email addresses for private individuals to be the personal information of the individual."

[14] An identifying number is typically a unique number connected to an individual in a particular context. Examples include Health Card number, medical record numbers assigned by hospitals, Social Insurance Number (SIN), driver's licence number, student numbers, and address information. It may also include personal fax numbers or Internet Protocol (IP) addresses.

The Corporate Operating Policy on Internet Tracking Technologies states: "Government organizations shall protect and manage IP addresses of individuals according to the same criteria as apply to PI under section 38 of FIPPA (collection of PI), section 39 (manner of collection), section 40 (retention), section 41(use), section 42 (disclosure), and Ontario Regulation 460, sections 1,2, 3, and 4 (safeguards)."

[15] An identifying symbol is something that stands for, or suggests, something else

by reason of relationship, association, convention, or accidental resemblance. Examples include a signature, a degree or professional designation, a tattoo, an emblem, or a scar.

[16] Other identifying particulars may include biometrics such as a handprint, footprint, iris scan or DNA. Behavioural biometrics may include keystrokes and voiceprints.

[17] Specify any other identifying characteristic or code. Also, specify whether your project will be collecting, using or disclosing any traffic data, access log records or analytics.

[18] If your project will be collecting, using or disclosing de-identified information, outline the process by which the PI will be de-identified (by you or others), as well as the volume of data and size of the group of individuals (i.e., cell count). Explain why it will not be possible to identify the data subject from the data.

The Personal Health Information Protection Act (PHIPA) provides guidance on what constitutes de-identified information:

> **47.** (1) In this section,
>
> "de-identify", in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and "de-identification" has a corresponding meaning.

[19] This question is designed to help identify what PI the project plans to use, if any. If your project is developing an application or system that will enable others to use PI, complete the Preliminary Analysis with that fact in mind.

Under FIPPA, using PI implies managing, applying, analyzing or otherwise making use of information that is already available to the institution.

[20] See explanation for line 42 and note 12.

[21] See explanation for line 44 and note 13.

[22] See explanation for line 63 and note 14.

[23] See explanation for line 64 and note 15.

[24] See explanation for line 66 and note 16.

[25] See explanation for line 72 and note 17.

[26] See explanation for line 75 and note 18.

[27] This question is designed to identify what PI the project plans to disclose, if any. If your project is developing an application or system that will enable others to disclose PI, complete the Preliminary Analysis with that fact in mind.

Under FIPPA, a disclosure may be when PI is transferred outside of an area or institution to another area or entity (e.g., another individual or organization).

[28] See explanation for line 42 and note 12.

[29] See explanation for line 44 and note 13.

[30] See explanation for line 63 and note 14.

[31] See explanation for line 64 and note 15.

[32] See explanation for line 66 and note 16.

[33] See explanation for line 72 and note 17.

[34] See explanation for line 75 and note 18.

[35] This question is designed to identify the stage your privacy analysis is at. Your project may or may not have considered privacy requirements in its Integrated Project Plan, may have previous PIA documents to build on, or may be in the process of completing the PIA process. For more information about the PIA process, how the Preliminary Analysis fits in, and an explanation of the purpose of the Privacy Risk Analysis and Privacy Design Analysis, please see Privacy Impact Assessment Guide for the Ontario Public Service.

[36] This question is designed to identify the scope of the project based on cost. The values coincide with other project requirements and approval processes for large scale I&IT projects (e.g., Gating and Architecture review processes).

[37] This question is designed to identify whether a privacy breach has occurred in the last year. A privacy breach is defined as "an incident involving unauthorized disclosure of PI in the custody or control of an institution covered by FIPPA." A privacy breach may signify privacy and/or security problems that should be addressed in your privacy analysis. For more information, see Taking the Right Steps - A Guide to Managing Privacy and Privacy Breaches.

[38] This question is designed to identify highly sensitive PI with high privacy risks that must be addressed.

[39] This question is designed to identify highly sensitive personal health information with high privacy risks that must be addressed. Before answering this question, consider if the Personal Health Information Protection Act (PHIPA) applies to your project.

[40] This question is designed to identify Government of Ontario institutions involved in your project (i.e., are or will be an interested party, committee participant, stakeholder, or have an advisory role). End users are not considered to be "involved" in your project.

[41] Other Government of Ontario institutions not identified on the list include agencies, boards, and commissions with a reporting relationship to a minister.

[42] This question is designed to identify the Government of Ontario institutions that

will have access to and use the PI or the information applications, systems or services resulting from your project. (See also line 191 and note 40.)

[43] See explanation at line 223 and note 41.

[44] This question is designed to be all-inclusive and identify organizations outside of the Government of Ontario such as other governments, private companies, or not-for-profit organizations. Include organizations with any possible exposure or access to the PI (e.g., developing, designing, building, testing, maintaining, storing or securing the data or systems resulting from your project). Cross-jurisdictional initiatives or cross-border data flows may create potentially high privacy risks that must be addressed.

[45] This question is designed to identify whether private sector organizations involved in your project are subject to privacy legislation. If not, they create high privacy risks that must be addressed.

[46] The involvement of foreign organizations not subject to Canadian privacy laws may pose a significant privacy risk. When PI is stored outside of Canada or maintained in Ontario but managed by a foreign-owned service provider or its Canadian affiliate, it could be subject to other countries' laws. Also, when contracting with a foreign-owned company, PI about Ontarians or other sensitive information may be accessible to a foreign government.

[47] See explanation at line 288 and note 46.

[48] See explanation for line 32 and note 6. Information management functions include all operations related to the collection, storage, maintenance, use, disclosure and disposal of PI by any means.

[49] This section is designed to bring attention to the risks that may be posed by laws in foreign jurisdictions. The Guidelines for the Protection of Information When Contracting for Services provide guidance on how to address these potentially high privacy risks.

[50] This question is designed to identify a key resource for your project in the early stages of information-gathering, review and approvals. The FIPPA Coordinator can help with the analysis of legislative and ministry-specific privacy issues. Consult your FIPPA Coordinator as early in your project lifecycle as possible. Document your discussions with the FIPPA Coordinator.

[51] This question is designed to identify the importance of consulting with legal counsel and having legal counsel assist in providing and analyzing statutory authority for the project. The legal complexity of your project may require a legal opinion, especially if it is a large scale, multi-ministry, cross-jurisdictional, contracted-out, or alternative service delivery project. Document your discussions with legal counsel.

The Access and Privacy Law Group, Legal Services Branch, Ministry of Government Services, has expertise in privacy legislation and is available to provide advice on privacy issues. It is recommended that you liaise with this Group through your Legal Branch or FIPPA Coordinator.

[52] This question is designed to identify the legal framework of your project. "Other Legislation" refers to a specific ministry or program statutes.

[53] In very limited circumstances, PI is excluded from the application of FIPPA. This means that neither the access nor privacy provisions of FIPPA apply to this information.

Section 65 of FIPPA outlines the exclusions from FIPPA, which include:

- some court records;
- some labour relations and employment-related data;
- some research material; and
- some teaching material.

> **Note:** The OPS Human Resources Privacy and Security Guidelines apply to labour relations and employment-related records, even if they are not covered by FIPPA. Contact the OCIPO for further information about the guidelines.

The exclusion of PI from the scope of FIPPA has a number of exceptions. Consult with your FIPPA Coordinator and Legal Branch when determining whether section 65 applies to your project.

[54] The privacy provisions of FIPPA do not apply to PI that is maintained as a public record. In order for PI to be excluded from the application of the privacy provisions under section 37, certain requirements must be met:

- your institution must maintain the PI as the public records — using another organization's public record will not trigger the exclusion;

- the primary purpose of maintaining the record must be for it to be made available to the public;

- the PI must be available to all members of the public, not just to a select group or portion of the populace; and

- the PI must be available through a regularized system of access.

All four conditions must apply for PI to be excluded from the application of FIPPA's privacy rules.

> **Note:** The exclusion only applies to the data elements or clusters maintained as public records. Other PI involved in your project will need to be protected in accordance with FIPPA's privacy rules.

To show that a "regularized system of access" exists, you must demonstrate that: 1) a system exists; 2) the record is available to everyone; and 3) there is a pricing structure that is applied to all who wish to obtain the information. Examples of types of records found to have a "regularized system of access" include: unreported court decisions; statutes and regulations; property assessment rolls; property sale data; and police accident reconstruction records.

If you think your project will maintain public records, a legal opinion and/or input from your FIPPA Coordinator is recommended to help you determine whether the

outlined conditions will apply to your project.

[55] This question is designed to identify, in simple business terms, why your project will need PI (i.e., the purpose). For example, the purpose may be registration, authentication, providing information, issuing a certificate or licence, research, or case management. A consistent purpose is one for which the data subject might reasonably expect such use or disclosure. It only relates to personal information collected directly from the data subject (section 43).

[56] FIPPA authorizes the collection of PI only if it is expressly authorized by statute, used for the purposes of law enforcement, or necessary to the proper administration of a lawfully authorized activity.

[57] The phrase "expressly authorized by statute" has been interpreted by the IPC to mean that the specific types of PI to be collected are expressly described either in a statute or in a regulation made under the statute. Where a regulation provides the authority for the collection of PI, the statute should set out a general reference to the activity.

[58] Subsection 2(1) of FIPPA defines "law enforcement" as:

(a) policing,
(b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
(c) the conduct of proceedings referred to in clause (b).

To be considered for the purpose of "law enforcement," the PI must be used for policing, investigations or inspection, or the conduct of a law enforcement proceeding.

[59] To qualify as "necessary," you must show that each item of PI to be collected is necessary to properly administer a lawfully authorized activity. Where the PI would merely be helpful to the activity, it is not "necessary" within the meaning of FIPPA. Similarly, where the purpose can be accomplished in another way (i.e., without collecting the PI), you are obliged to follow the other route. The IPC's approach is to examine, in detail, the types of information being collected and to determine whether each type is necessary for the collecting institution's activity.

[60] See Appendix A for definition of "data subject."

[61] A notice of collection is required when collecting PI. It must inform the data subject of the legal authority to collect their PI (e.g., statute reference and relevant program). You also need to inform the individual how their PI will be used, and provide them with contact information for an official who can answer their questions about the collection and use of their PI.

[62] An institution does not have to provide a notice of collection where the PI to be collected would qualify under the law enforcement exemption (subsections 14(1), 14(2), 14.1, or 14.2).

[63] FIPPA subsection 39(1) and MFIPPA subsection 29(1) list how PI can be collected indirectly. The manner of collection is defined in FIPPA as follows:

39. (1) Personal information shall only be collected by an institution directly from the individual to whom the information relates unless,

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act;
(c) the Commissioner has authorized the manner of collection under clause 59(c);
(d) the information is in a report from a reporting agency in accordance with the Consumer Reporting Act;
(e) the information is collected for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service;
(f) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or tribunal;
(g) the information is collected for the purpose of law enforcement; or
(h) another manner of collection is authorized by or under a statute.

[64] Section 42 of FIPPA specifies the conditions under which an institution may disclose PI. No other disclosures of PI are permitted.

[65] The term "flow-through model" describes a situation where one organization collects PI on behalf of another organization (e.g., contact information). The collecting organization does not use or store the information but passes the information along to the organization that has authority for the use of PI. The flow-through model can apply to PI collected in hard copy or electronically.

[66] This question is designed to identify how security requirements under FIPPA will need to be considered and addressed. Key security tools and processes are the Information Security and Privacy Classification (ISPC) and Threat Risk Assessment (TRA).

[67] This line is designed to identify relevant security measures in place or planned. Typical security measures include user access control to computer applications and systems; physical locks on buildings, doors and cabinets; encryption of sensitive information in databases and hard drives; and employee records checks, bonding and related human resources security measures.

[68] This question is designed to identify key security resources corporately and within clusters. The Corporate Security Branch is responsible for the Information and Information Technology Security directives, policies and procedures, and operating guidelines. Cluster security officers can provide information and advice on security measures and processes within a cluster.

[69] This question is designed to identify what stage your project is at regarding the identification and assessment of security risks. You may or may not have identified security requirements in your Integrated Project Plan, may have a past or current TRA to build on, or may be in the process of conducting the security analysis.

[70] For information about secure shredding and disposal practices and the OPS

Vendor of Record, watch the "Think Inside the Box" video on the MyOPS home page or on the iNetwork.