

WDGPH Annual Privacy Program Update

TO: Chair and Members of the Board of Health

MEETING DATE: March 6, 2019

REPORT NO: **BH.01.MAR0619.R08** Pages: 7

PREPARED BY: Charles Wright, Privacy and Health Information Analyst

APPROVED BY: Dr. Kyle Wilson, Director, Information Systems & Chief Privacy Officer

SUBMITTED BY & SIGNATURE: *Original signed document on file*

Dr. Nicola J. Mercer, MD, MBA, MPH, FRCPC
Medical Officer of Health & CEO

Recommendations

It is recommended that the Board of Health:

1. Receive this report for information.

Key Points

- In 2018, Wellington-Dufferin-Guelph Public Health (WDGPH) experienced a lower than normal number of data breaches and a return to normal levels of access to information requests after a spike of requests in 2017.
- Information Systems uses a Privacy and Health Information Analyst to complete freedom of information requests, respond to data breaches and conduct privacy impact assessments.
- Towards the goal of continuous quality improvement, there was a continuation of ongoing privacy training with successful privacy training sessions held for WDGPH staff.
- Calendar year 2018 is the first year WDGPH will be required to report annual statistics on health data breaches to the Information and Privacy Commissioner of Ontario.

Discussion

Privacy breaches

Between 2014 and 2017 the number of documented privacy breaches in a year has averaged approximately nine per year. In 2018, WDGPH had four (4) documented data breaches. Privacy breaches in 2018 included incidents where clients were given incorrect records, mail and email were sent to the incorrect address and a stack of letters delivered to a school mistakenly included pages from a personal health record. The overall downward trend in breaches is thought to be attributed to increased privacy training creating awareness within the agency and changes to some processes which decreased the probability of privacy breaches.

Year	Number of Privacy Breaches
2014	9
2015	12
2016	9
2017	7
2018	4

Figure 1: Number of documented privacy breaches experienced by WDGPH in each year over the period of 2014 to 2018.

Access to information data requests

Under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), WDGPH is required to provide access to information at the request of clients and members of the public. In 2018, WDGPH received five (5) formal MFIPPA requests. Information requests received in 2018 included requests for rabies exposure reports, health inspection reports, an environmental health report and a request related to a law enforcement matter. Between 2014 and 2017 the annual number of MFIPPA requests has ranged between two (2) and twelve (12) with an average of approximately five (5) requests in each year. The peak in the number of information requests in 2017 is attributable to a spike in requests as the result of WDGPH Public Health Inspector enforcement actions. In 2018, the number of requests returned to a normal levels and were in line with the five (5) year average.

Year	Number of MFIPPA Requests
2014	2
2015	2
2016	3
2017	12
2018	5

Figure 2: Number of formal MFIPPA requests received by WDGPH in each year over the period of 2014 to 2018

Privacy Resources

In June, in line with agency priorities regarding privacy, a part-time Privacy and Health Information Analyst was hired. The Privacy Analyst is responsible for completing Privacy Impact Assessments, coordinating Access to Information Requests, complying with reporting requirements and responding to privacy concerns from across the agency. This position has helped with privacy awareness activities to ensure a ‘privacy first’ mindset for staff.

Ongoing Staff Training

In October 2018, an outside speaker was organized to conduct a three (3) hour seminar focused on privacy and access to information. These are both increasing concerns for WDGPH and ensuring that employees are well versed in both are essential to an efficient and effective privacy program.

Before and after the seminar, a survey was conducted of the participants. The survey found that participants significantly increased their knowledge of MFIPPA and PHIPA. It was encouraging to see that even prior to the training, WDGPH staff had a good understanding of key concepts, including the circle of care, protecting patient privacy and privacy breaches. Please see Appendix “A” for more information on the survey results.

Mandatory Reporting

Bill 119, an amendment to PHIPA which was passed in 2016, introduced mandatory reporting of health information breaches. Starting with calendar year 2018, all health information custodians (HICs) will need to provide statistical reporting to the Information and Privacy Commissioner of Ontario (IPC) on any PHIPA privacy breaches that have

occurred. In 2018, WDGPH experienced three (3) data breaches which are reportable under this mandatory reporting.

Annual statistical reporting published by the IPC generally publishes reports with the number of reported privacy breaches for each reporting institution. Given the large number of HICs, in Ontario, it is not yet known whether the IPC will be publishing these results as aggregated numbers or whether there will be a public report detailing the number of breaches for each HIC. At a webinar, in June 2018, the IPC declined to provide details on the format of the report. This is the first time such reporting by HICs has been done in Ontario and the form of the report could vastly change the potential reputational risks for HICs.¹

Privacy Impact Assessments

Any new projects, or substantial changes to projects which involve personal information or personal health information are subjected to the Privacy Impact Assessment (PIA) process. PIAs are a tool used to analyze projects and assure their compliance with applicable legislation and privacy standards.

In 2018, twelve PIAs were initiated. Projects that are currently under a PIA review include: Office 365 deployment, cellphone security & privacy, cloud-based Electronic Medical Records system evaluation, dental medical record software, pre-natal health education and a telemedicine system.

Privacy Trends

Laws such as Europe's General Data Protection Regulation (GDPR) and the new California Consumer Privacy Act along with prominent breaches such as Cambridge Analytica and Google+ have thrust privacy into the general public consciousness.

With the increased awareness of privacy and consumer rights among the general public, combined with the explosion of social media, there can be serious consequences for any organization or public institution that is involved in a privacy scandal. For Cambridge Analytica, it led to the end of the company, for Google it hastened the end of Google+.

In the age of social media, every organization that deals with personal information or personal health information should be cognizant of properly protecting privacy. A failure to do so can result in reputational harm, financial harm and a loss of trust from the public. Without the trust of the public, it is difficult for any organization to deliver on its mandate.

Conclusion

Privacy is an important concern for WDGPH and properly safeguarding privacy is an essential factor in maintaining the trust of the community WDGPH serves. Privacy breaches can be one of the most visible symptoms of a poor privacy program within an organization. There are grave reputational and financial risks posed by privacy breaches. Privacy breaches can also negatively impact public trust and result in significant fines for organizations. WDGPH has made great progress in its privacy program and privacy breaches are at a five (5) year low.

Ongoing staff training and education helps to keep staff up-to-date on emerging privacy issues and concerns such as mandatory statistical reporting of health privacy breaches or increased penalties for privacy infractions.

Dedicated privacy resources allow WDGPH to continue responding efficiently to information requests, to strengthen privacy protections through the privacy impact assessment process and to build and strengthen relationships across the agency.

Into the future, the impact of privacy breaches will only become more of a concern for organizations. The potential impact of privacy breaches grows with the amount of information that an organization holds. Organizations will need to apply a privacy lens in all that is done to minimize the probability of a privacy breach and minimize the associated financial, reputational, legal and operational risks.

WDGPH Strategic Direction(s)

- Health Equity:** We will provide programs and services that integrate health equity principles to reduce or eliminate health differences between population groups.
- Organizational Capacity:** We will improve our capacity to effectively deliver public health programs and services.
- Service Centred Approach:** We are committed to providing excellent service to anyone interacting with WDG Public Health.
- Building Healthy Communities:** We will work with communities to support the health and well-being of everyone.

Health Equity

Marginalized and vulnerable populations can be disproportionately affected by privacy harms. A privacy breach can lead to reputational damage, job loss and could significantly erode an individual's trust in public services. To see the effect of a privacy breach on a marginalized population, examine the fallout of a recent breach involving the identities of HIV positive individuals in Singapore leaked by a disgruntled former employee. These harms have an outsized impact on the lives of individuals with tenuous work, health, or living arrangements; the loss of trust could decrease the chance they will seek out health services. Additionally, these same populations may be less familiar with their rights in regards to their personal information. The combination of these two (2) factors make it essential for an organization like WDGPH to maintain a responsible and transparent privacy program in order to best serve those among us who are most vulnerable.²

References

1. Annual Reporting of Privacy Breach Statistics to the Commissioner.
<https://www.ipc.on.ca/health/report-a-privacy-breach/annual-reporting-breach-statistics/> ed.
2. Griffiths J. HIV status of over 14,000 people leaked online, Singapore authorities say [Online Article].; 2019 [cited 2019 February 21. Available from:
<https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html>.

Appendices

Appendix "A" – Information on survey results.

APPENDIX “A”

Question: In your opinion, how would you rate your knowledge of the Personal Health Information Protection Act (PHIPA)?

	Before Training	After Training
Expert	-	-
Exceptional	-	15%
Competent	70%	85%
Weak	30%	-

Figure 3: Question from employee survey rating employee knowledge of the Personal Health Information Protection Act (PHIPA), after training there is a marked decrease in employees rating their knowledge of PHIPA as weak and a marked increase in employees rating their knowledge or competent or exceptional.

Question: In your opinion, how would you rate your knowledge of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)?

	Before Training	After Training
Expert	-	-
Exceptional	-	5%
Competent	55%	85%
Weak	45%	10%

Figure 4: Question from employee survey rating employee knowledge of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), after training there is a marked decrease in employees rating their knowledge of MFIPPA as weak and a marked increase in employees rating their knowledge or competent or exceptional.