NSCC

Large Assignment

Breach Notification Standards

Jeong Eun Jang (W0451032)

ISEC 3050

Ronald McLeod

November 8, 2021

Table of Contents

1. INTRODUCTION

With the global rise of data collection from internet usage, data breach is raising crucial issue in the society. A data breach is taking information without the knowledge or permission from the information owner (Trend Micro, n.d.). Data breach is mainly caused by hacking or malicious code attacks, and it can occur regardless of the size of the company. Furthermore, data leakage by insiders, theft of payment information, loss and theft of electronic devices, and unintended disclosure due to mistakes or carelessness are also the causes of data leakage (Trend Micro, n.d.).

This document contains analyzing various breach notification regulations in the United States and Canada on data breach in several different sectors, by country, states, or provinces. It will be a good practice to learn the right process and mindset about data security as Database Administrators who manage and use data.

2. CANADA

2.1. Public Administration

2.1.1. What constitutes a breach

Under the Privacy act, personal information is information of a recognizable individual and is stored in various forms. A privacy breach includes unauthorized use, collection, or disclosure of personal information. The breach can occur by intended or unintended actions by employees, third parties or intruders (Government of Canada, 2014).

There are many potential causes that lead to privacy breaches. It can be occurred by theft or loss of electronic devices containing personal information. The use of equipment without proper security measures causes unauthorized access. If employees or contractors have a low level of privacy awareness, it can be a risk factor. Furthermore, stealing personal information through phishing or fraudulent activity and theft of personal information disguised as the official website of the Canadian government can be an issue (Government of Canada, 2014).

2.1.2. The information that must be contained in a breach notice

The content of notifications will become different depending on the type of breach and the method of notice, but it should include a brief description of the breach and date and time it occurred. It should describe the source of the breach, whether it is an organization or a contracted party or a third party making a contract. The notification should include a list of accessed disclosed personal information and the measures to prevent potential risk of the breach, as well as the mitigation steps in case the action has not been taken yet. There must be contained advice to the individual to reduce risks of identity theft or cope with compromised personal information and instructions to handle these activities. Lastly, the name and contact information of an

official at the entity should be provide help and a reference to the effect that the Office of the Privacy Commissioner (OPC) and the Treasury Board of Canada have been informed about the type of the breach and the individual's right of complaint to the OPC under the Privacy Act (Government of Canada, 2014).

2.1.3. The target audience of the breach notice

At first, the affected individuals should be notified of the breach. In privacy breach management process, Offices of Primary Interest (OPIs) have a role of stopping the breach, protecting affected data, and document situations. The Department Security Officers (DSO) investigate security incidents, make recommendations, and reports them to law enforcement if necessary (Government of Canada, 2014).

2.1.4. Any timing stipulations affecting when the notice must be made

The breach of individuals affected must be notified as soon as reasonably possible after assessment and evaluation of the breach. Once the senior official of the office discovers a privacy breach, he or she should notify the Chief Privacy Officer (CPO) or Access to Information and Privacy (ATIP) Coordinator as soon as possible. When a suspected breach situation occurred, the Office of Primary Interest containment (OPI) should immediately perform action to secure the affected data, systems, or websites (Government of Canada, 2014).

2.2. Business

2.2.1. What constitutes a breach

In Canada, large and small business must report and notify breaches of security safeguards and maintain records of breaches if there is unauthorized access, disclosure or loss of personal information. Under Personal Information Protection and Electronic Documents Act (PIPEDA), the intentional offences of reports, notices, or records relating to breaches of security safeguards is considered a crime and is subject to fines (Office of the Privacy Commissioner of Canada, 2018).

2.2.2. The information that must be contained in a breach notice

PIPEDA Breach Report contains that information of the organization a breach occurred, the number of individuals affected by the incident, start and end date of breach occurrence, type of breach, and a description of the circumstances. It must provide contact information of a person on behalf of the organization, and this person must answer OPC's question about the breach. This report also includes a description of affected individual's information and measures the company attempts to mitigate risk of the incident (Office of the Privacy Commissioner of Canada, n.d.). The breach notification for affected individuals should indicate the situation of breach, the date and time of the incident, a description of the breached information. The organization must

describe the steps has taken to reduce the risk of harm and mitigation method to prevent potential risk of harm, and the contact information that the individual can get advice (Canadian Government, 2018).

2.2.3. The target audience of the breach notice

Under PIPEDA, an organization shall report to the Office of the Privacy Commissioner if the situation is judged that there is a reasonable risk of serious harm to an individual. The notice must report to the affected individuals. (Office of the Privacy Commissioner of Canada, 2018).

2.2.4. Any timing stipulations affecting when the notice must be made

If a breach of security safeguards happens, organizations must report it to the OPC as soon as possible, even if all information is not investigated or confirmed. The affected individual(s) must notify the breach as soon as feasible (Office of the Privacy Commissioner of Canada, n.d.).

2.3. Health Care

2.3.1. Ontario

2.3.1.1. What constitutes a breach

When the personal health information is collected, used, or disclosed by someone who is not authorized, it is defined as a privacy breach. Any theft, loss, or unauthorized copying, modification or disposal of personal health information are included in a breach. In Ontario, health information custodians have an obligation to protect personal health information under the Personal Health Information Protection Act (PHIPA) (Information and Privacy Commissioner of Ontario, 2018).

2.3.1.2. The information that must be contained in a breach notice

Under the PHIPA, custodians require notifying affected individuals. The notice should provide the date of the breach and the name of the agent responsible for the unauthorized access. It also should describe the nature and scope of the breach and the personal health information breached. Last, it should include the steps took to control the breach and the contact information for the person who can assist.

Under the PHIPA, custodians must report privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) following 'Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector'. The report to the IPC must describe the situation of the breach, the nature of the breach, the measures implemented to contain, and information notified of the affected individuals. It must also provide the measures implemented to contain, investigate, and correct the breach and reduce the potential harm (Information and Privacy Commissioner of Ontario, 2021).

2.3.1.3. The target audience of the breach notice

The affected individuals and the Privacy Commissioner of Ontario must be notified of the breach. In addition, the custodian can notify to the chief privacy officer or other staff member responsible for privacy, if needed (Information and Privacy Commissioner of Ontario, 2018).

2.3.1.4. Any timing stipulations affecting when the notice must be made

Once a custodian realizes know a privacy breach happened, he or she must act immediately. Under the PHIPA, custodians must report privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) and affected individuals at the first reasonable opportunity (Information and Privacy Commissioner of Ontario, 2018).

2.3.2. Alberta

2.3.2.1. What constitutes a breach

Under the Health Information Act (HIA), a breach includes loss of personal health information, unauthorized access, or unagreed disclosure. A custodian, which is an organization or entity designated in the HIA, must think about whether the breach has any risk of damage to any individual carefully (Health Information Act, n.d.).

2.3.2.2. The information that must be contained in a breach notice

Under section 37.1 of the Personal Information Protection Act Regulation, the notification for an individual who in a risk of harm because of personal information breach must describe the situation of the loss or unauthorized access or disclosure, the date or time that the breach happened, and the personal information involved in. It must also describe the measures the entity has taken to reduce the risk of damage and contact information of a person who can deal with questions about the breach (Province of Alberta, 2018).

A custodian should provide a notice to the Commissioner, and it must include a description of the circumstances of a breach, the date and time the incident occurred, the personal information involved in, and the number of individuals exposed to the breach. A description of measures the organization has taken to individuals who have affected and contact information of a person who is responsible must include in the notice (Province of Alberta, 2018).

2.3.2.3. The target audience of the breach notice

When the custodian recognizes a breach, it must notify the breach to affected individuals, the Information and Privacy Commissioner of Alberta, and the Minister of Health (Health Information Act, n.d.).

2.3.2.4. Any timing stipulations affecting when the notice must be made

Under the Health Information Act (HIA), custodians have a duty to notify the Commissioner of breaches as soon as practicable (Office of the Information and Privacy Commissioner of Alberta, n.d.).

3. UNITED STATES

3.1. Public Administration

The Data Breach Notification Act has been enacted in all 50 States in the United States; however, the Federal Data Violation Notification Act has not yet passed Congress (Garrison & Hamilton, 2019).

3.2. Business

3.2.1. Texas

3.2.1.1. What constitutes a breach

Under the Texas Business and Commerce Code 521.053, businesses must notify affected individuals and the Texas Attorney General after discovering or receiving notification of any breach. Unauthorized acquisition of data considers as a breach for violating the security, confidentiality, or integrity of sensitive personal information (Casale et al., 2021).

3.2.1.2. The information that must be contained in a breach notice

The data security breach report must contain information of entity that causes the breach, detailed description of the nature and situation of the breach. The entity also must provide measures taken by the person or company concerning the breach. In addition, the notice must indicate the number of persons affected by the breach, whether it notified another law enforcement agency of this breach and contact information of a person who submits the form (Ken Paxton Attorney General of Texas, n.d.).

3.2.1.3. The target audience of the breach notice

Any individual whose personal information has been breached, or is reasonably believed to have been, must be notified. The Texas Attorney General must be notified if at least 250 Texas residents are involved in the breach. The notice must report to National Consumer Reporting Agencies if more than 10, 000 persons affected at once (Privacy Rights Clearinghouse, 2018).

3.2.1.4. Any timing stipulations affecting when the notice must be made

Under Texas Business and Commerce Code 521.053, the notice must be made and reported to individuals whose personal information has been breached within 60 days. The Texas Attorney General must be notified of the breach within 60 days if at least 250 Texas residents are involved (Casale et al., 2021).

3.2.2. California

3.2.2.1. What constitutes a breach

Under the California Civil Code s. 1798.82, the company that runs a business in California and possesses computerized data that includes personal information has an obligation to report and disclose a breach. If personal information is obtained by an unauthorized person, or unauthorized acquisition of encrypted data is happened when the encryption key has been accessed by an unauthorized person, these cases are defined as a breach (California Legislative Information, n.d.).

3.2.2.2. The information that must be contained in a breach notice

Under the California Civil Code s. 1798.29(e) and California Civil Code s. 1798.82(f), businesses are required to send a sample notice If a breach of personal information, including over 500 Californian residents, is violated. This security breach notification sample contains information about the breach occurred organization for law enforcement purposes. It also shows the date of breach, the date of discovery of breach, and the date of individual notice provided to consumers. The document includes the type of personal information entailed for the breach, a brief description of the breach, and contact information for the connection with the Attorney General (State of California Department of Justice Office of the Attorney General, n.d.).

3.2.2.3. The target audience of the breach notice

Following the California law, a business or state agency must report any affected California resident of a breach of personal information. If there are more than 500 California residents involve in this incident, a list of sample breach notices must be provided to the California Attorney General (State of California Department of Justice Office of the Attorney General, n.d.).

3.2.2.4. Any timing stipulations affecting when the notice must be made

The announcement of a breach must be proceeded in the most expedient time possible without unreasonable delay (State of California Department of Justice Office of the Attorney General, n.d.).

3.3. Health Care

3.3.1. What constitutes a breach

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is a federal law that grants everyone the right to his or her medical information and prescribes rules for those who can view or receive personal medical information (Office for Civil Rights, 2021). Under the HIPAA, a breach in health sector indicates violation and impermissible use of protected health information. The scope of use or disclosure of medical information corresponding to the data bridge occurs when the following requirements are met. The nature and content of protected health information, whether the protected health information has been obtained or inquired by someone who does not have the authority to use or disclose the protected health information, and the degree of risk mitigation for protected health information. The relevant corporation and business associates may provide violation notifications without any risk assessment, if applicable to them (Office for Civil Rights , 2013).

3.3.2. The information that must be contained in a breach notice

If violation is found, breach notice must be provided to the individual within 60 days. This notification should describe the breach and the information infringed. These include actions that individuals affected by the violations can take to protect themselves from potential damage, how to mitigate and prevent the damage, and contact information for the covered agency or business associate under investigation (Office for Civil Rights, 2013).

3.3.3. The target audience of the breach notice

Under the HIPAA Breach Notification Rule, the breach notification should be provided to affected individuals. Covered entities should send a press release form to prominent media serving in the State or Jurisdiction. The Secretary should be noticed the breach by a breach report form (Office for Civil Rights, 2013).

3.3.4. Any timing stipulations affecting when the notice must be made

Under the HIPAA Breach Notification Rule, relevant entities must provide breach notice to individual within 60 days without unreasonable delay. It may be delivered in written form or email according to the individual's existing consent. Media notification for the breach should be provided to major media within 60 days unless there is a specific reason, and the same information required for individual notifications should be provided. In case of notice to the Secretary, covered entities must report the breach within 60 days if 500 or more people are affected by the breach. If the breach affects fewer than 500 people, the notice may be reported annually (Office for Civil Rights, 2013).

4. ANALISYS

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
Canada						
	Federal	Public	▪ unauthorized use, collection, or disclosure of personal information.	▪ A general description of the breach and date and time it occurred. ▪ The source of the breach ▪ A list of accessed of disclosed personal information	▪ The affected individual(s) ▪ The Office of the Privacy Commissioner ▪ The Departmental Security Officer	▪ The breach should be notified of individuals affected as soon as reasonably possible.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				▪ The measures to prevent potential risk of the breach and mitigation steps ▪ Advice to the individual to reduce risks of identity theft ▪ The name and contact information of an official at the entity to provide		

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				help		
	Federal	Private	▪ Unauthorized access ▪ Disclosure of personal information ▪ Loss of information	▪ The breach report for the OPC: information about the organization a breach occurs, a description such as number of individuals affected, type of breach, date of breach	▪ Affected individuals ▪ Office of the Privacy Commissioner if significant harm occurs by a breach.	▪ Affected individual(s) and organizations must report a breach to the Office of the Privacy Commissioner as soon as possible.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				occurrence, a description of the circumstances, contact information of a person on behalf of the organization, affected individual's information and measures to mitigate risk of the		

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				incident		
	Ontario	Health	▪ Defined as when personal health information is collected, used, or disclosed without authorization. ▪ Include theft, loss, unauthorized copying, modification, or	▪ The report to the IPC: the situation of the breach, the nature of the breach, the measure implemented to reduce harm and prevent future breaches ▪ The report to	▪ The affected individuals and the Privacy Commissioner of Ontario must be notified of the breach. ▪ The chief privacy officer or other staff member	▪ Under the PHIPA, custodians must report privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) and affected individuals at the

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
			disposal of personal information.	affected individuals: The date of the breach, the nature and scope of the breach, a description of the PHI related to the breach, contact information of the person who can assist	responsible for privacy, if it may need	first reasonable opportunity.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
	Alberta	Health	▪ Loss of personal health information ▪ Unauthorized access ▪ Unagreed disclosure	▪ For the notice to individuals: A description of the situation of the breach, the date that the breach happened, the personal information involved in the breach. ▪ For the notice to the	▪ Affected individuals ▪ The Information and Privacy Commissioner of Alberta ▪ The Minister of Health	▪ Under the Health Information Act (HIA), custodians must notify the Commissioner of breaches as soon as practicable.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				Commissioner: A description of the circumstances of a breach, the date the breach occurred, the personal information involved in, the number of individuals exposed to the breach, the measures the		

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				organization has taken to and contact information of a person who can answer questions.		
U.S.A	Federal	Public				
	Texas	Private	▪ Unauthorized acquisition of data	▪ Information of entity that occurs during the breach	▪ Any individual whose personal information	▪ For individuals whose personal information

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				▪ Detailed description of the nature and situation of the breach. ▪ Measures taken by the person or company concerning the breach. ▪ The number of persons affected by the breach	breached or is reasonably believed to have been breached. ▪ The Texas Attorney General must be notified the breach if at least 250 Texas residents are involved in.	breached within 60 days. ▪ The Texas Attorney General must be notified the breach within 60 days if at least 250 Texas residents are involved.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				▪ Whether it notified another law enforcement agency of this breach ▪ Contact information of a person who submits the form	▪ National Consumer Reporting Agencies if more than 10, 000 persons affected the breach at once.	
	California	Private	▪ The personal information is obtained by an	▪ The information about the organization that	▪ Any affected California resident ▪ The California	▪ The disclosure of a breach must be reported in the

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
			unauthorized person. ▪ Unauthorized acquisition of encrypted data when the encryption key has been accessed by an unauthorized person.	the breach occurred. ▪ The date of breach ▪ The date of discovery of breach ▪ The date of individual notice provided to consumers. ▪ The type of breach ▪ A brief description of the breach	Attorney General (if more than 500 California residents involved in the breach)	most expedient time possible without unreasonable delay.

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
				▪ Contact information of the organization		
	Federal	Health	▪ The nature and content of protected health information ▪ Whether the protected health information has been obtained or inquired by	▪ A brief report of the breach and the type of information that is related to breach. ▪ Measures individuals can protect themselves from potential damage.	▪ Affected individuals by the breach ▪ Appropriate media within the State or jurisdiction ▪ Notice to The Secretary by	▪ Individual notice within 60 days in written form or email ▪ Media notice within 60 days ▪ Notice to the Secretary within 60 days if the

Country	State / Province	Sector	Under what conditions Is a Breach Notice required	What information is required to be in the Breach Notice	Who needs to receive notice in the event of a Breach	What is the timing governing a Breach Notice (When does it have to be sent)
			someone who does not have the authority to use or disclose the protected health information ▪ The degree of risk mitigation for protected health information.	▪ Measures to mitigate damage caused by violations. ▪ Contact information with the agency being investigated for the violation.	submitting a breach report form	breach affects over 500 individuals. If fewer than 500 individuals, the notice may be reported annually.

References

California Legislative Information. (n.d.). *Civil Code -CIV.* https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

Casale, E., Harris, R. (August 16, 2021). Texas amends data breach notification law creates public listing of data breaches. *Thomson Coburn LLP.* https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2021-08-16/texas-amends-data-breach- notification-law-creates-public-listing-of-data-breaches

Garrison, C., Hamilton, C. (2019). A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law.* 28:1, 99-114. https://doi.org/10.1080/13600834.2019.1571473

Government of Canada (May 20, 2014). *Guidelines for Privacy Breaches.* https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154

Government of Canada (May 20, 2014). *Privacy Breach Management.* https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/breach-management.html

Government of Canada (October 28, 2021). *Protection of Personal Information in the Private Sector.* laws-lois.justice.gc.ca/eng/acts/P-8.6/page-4.htmal#h-417174

Health Information Act. (n.d.). *Health Information Act.* Alberta. https://www.alberta.ca/health-information-act.aspx

Information and Privacy Commissioner of Ontario. (October 2018). *Responding to a Health Privacy Breach: Guidelines for the health sector.* https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf

Information and Privacy Commissioner of Ontario. (March 2021). *Reporting a Privacy Breach to the IPC.* https://www.ipc.on.ca/wp-content/uploads/2019/09/2019-health-privacy-breach-notification-guidelines.pdf

Ken Paxton Attorney General of Texas. (n.d.). *Data Breach Reporting.* https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting

Office for Civil Rights (July 26, 2013). *Breach Notification Rule.* U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Office for Civil Rights. (2021). *HIPAA for professionals.* U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/index.html

Office of the Information and Privacy Commissioner of Alberta. (n.d.). *How to Report a Privacy Breach.* https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx

Office of the Privacy Commissioner of Canada. (n.d.). *PIPEDA breach report form.*

priv.gc.ca/media/4844/pipeda_pb_form_e.pdf

Office of the Privacy Commissioner of Canada. (October 2018). *What you need to know about mandatory reporting of breaches of security safeguards.* https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Privacy Rights Clearinghouse. (2018). *Data Breach Notification United States Territories*. https://iapp.org/media/pdf/resource_center/Data_Breach_Notification_United_States_Territories.pdf

Province Of Alberta. (December 12, 2018). *Personal Information Protection Act Regulation.* https://www.qp.alberta.ca/documents/Regs/2003_366.pdf

State of California Department of Justice Office of the Attorney General. (n.d.). *Submit Data Security Breach.* https://oag.ca.gov/privacy/databreach/report-a-breach

Trend Micro. (n.d.). Data Breach. https://www.trendmicro.com/vinfo/us/security/definition/data-breach