

Breach notification standards

ISEC 3050 – LAW AND ETHICS IN DATA ANALYTICS



November 14, 2020

JAMIE LU

W0441213

Table of Contents

[Introduction 2](#_Toc56356442)

[Canada 3](#_Toc56356443)

[Health care 3](#_Toc56356444)

[ONTARIO 3](#_Toc56356445)

[ALBERTA 5](#_Toc56356446)

[Business 7](#_Toc56356447)

[Public Administration 9](#_Toc56356448)

[United States 12](#_Toc56356449)

[Business 12](#_Toc56356450)

[NEW YORK 13](#_Toc56356451)

[CALIFORNIA 15](#_Toc56356452)

[Health Care 17](#_Toc56356453)

[Public administration 20](#_Toc56356454)

[ANALYSIS 21](#_Toc56356455)

[References 33](#_Toc56356456)

# Introduction

A Data Breach is commonly described as the intentional or unintentional use or release of confidential or personal information by an unauthorized entity. The thing that usually varies, although not by a lot, with different Breach Notification Regulations is what the words personal information means. Sometimes personal information could mean the Personal Health Information of an individual, or intellectual property. (Wikipedia, n.d.) This usually depends on which organization or jurisdiction the regulations/legislation is under as it usually is molded to the needs of the organization or jurisdiction.

This assignment will explore the different breach notification regulations or practices in the different federal sectors as well as in the different provinces/states. It will explore the differences and similarities these regulations/practices have.

With data breaches happening frequently, with some major ones dating back to 2005 up to now [[1]](#footnote-1), it is good to explore these regulations and practices to be prepared in our future careers, and lives. It will help us discover what we can possibly do to avoid a breach and during a breach.

# Canada

## Health care

### ONTARIO

1. **What constitutes a breach**

A breach is defined as when there is unauthorized collection, usage, or disclosure of a person’s Personal Health Information or PHI. This includes any unauthorized duplication, theft, loss, alteration, or disposal of the PHI. This also includes any cyberattacks, loss or burglary of portable devices, misdirected faxes, and intentional unauthorized access to electronic medical records. (Office of the Privacy Commissioner of Canada, 2018)

1. **The information that must be contained in a breach notice**

The date of the breach must be contained in the breach notice. It should describe of the nature and scope of the breach, and what PHI was breached. It should include the methods done to contain the breach. It should also allow the affected individual/s contact the organization regarding inquiries they might have regarding the breach, so the notification must contain the name and contact information of the individual or group who can address these inquiries. If appropriate, the name of the individual responsible for the unauthorized access should be included as well. The notice should also let the affected individuals know that they have the right to file a complaint to the IPC. If the breach involves financial information or government issued documents, then the breach notice should contain suggested precautionary measures, such as contacting the bank or appropriate government office to let them know about the breach. (Information and Privacy Commissioner of Ontario, 2018)

1. **The target audience of the breach notice (who needs to be told)**

The affected individuals must be notified of the breach. The Privacy Commissioner must also be notified.

When the breach is done by a member of a College of a regulated health profession, and it results in termination, suspension, or any disciplinary action, then the College must be notified as well. (Johnson, 2016)

1. **Any timing stipulations affecting when the notice must be made**

Ideally, the affected individual/s must be notified at the first reasonable opportunity but timing on when the breach notice must be made depends on the situation. There might be a situation wherein a notation can be made in the affected individual’s file and the breach will be discussed during the next appointment. (Information and Privacy Commissioner of Ontario, 2018)

### ALBERTA

1. **What constitutes a breach**

A breach occurs when the health information, that can individually identify someone, is lost, or is accessed or disclosed by an unauthorized entity. The risk of harm to the affected individual must then be assessed and if there is any, then the breach notice is required. (Health Information Act, n.d.)

1. **The information that must be contained in a breach notice**

When notifying the individual/s that have been affected by the breach, it must describe the situation of the loss or unauthorized access or disclosure. It must include the date or period that the breach occurred. It must describe what personal information was breached/compromised. The notice must include the measures the organization has taken to reduce the risk of harm on the affected individual. It must include the contact information of someone in the organization or on behalf of the organization who can answer inquiries about the breach.

When notifying the Commissioner, the notice should include an assessment of the risk of harm to the affected individuals. It must describe the situation of the loss or unauthorized access or disclosure. It should state the estimated amount of individual/s that have a real risk of significant harm due to the breach. It must include the date or period that the breach occurred. It must describe what personal information was breached/compromised. The notice must include the measures the organization has taken to reduce the risk of harm on the affected individual. It must include the contact information of someone in the organization or on behalf of the organization who can answer the Commissioner’s inquiries about the breach. (Province of Alberta, 2018)

1. **The target audience of the breach notice (who needs to be told)**

The affected individual/s, the Information and Privacy Commissioner of Alberta, and the Minister of Health must be notified of the breach. (Health Information Act, n.d.)

1. **Any timing stipulations affecting when the notice must be made**

The notice must be made as soon as it is practicable, in accordance to the breach, if there is a risk of harm towards the affected individual/s. (Health Information Act, n.d.)

There are some exceptions that eliminates the need for the notification, one of which is when the information is encrypted in a way that would prevent access or make the information incomprehensible. Another exception is if the information is lost but it involves the destruction of the information which means the information is no longer comprehensive. Another is if the information was recovered and has yet to be accessed before it was recovered. A notification is also not needed if the information was accessed or disclosed (unauthorized) by another custodian. If the unauthorized access or disclosure was done accidentally or without an improper purpose, then the breach notification is not needed. Lastly, if the information was just used to determine if there had been an error or to address an authorized access or disclosure, then the notification is not needed. (Banks, 2018)

## Business

1. **What constitutes a breach**

Under PIPEDA, a breach happens in large/small businesses when there is loss, unauthorized access, or disclosure of personal information that resulted from a breach of the security safeguards of an organization or from failure to establish the safeguards. (Office of the Privacy Commissioner of Canada, 2018)

1. **The information that must be contained in a breach notice**

The breach notification to be sent to the affected individual/s should contain a description of the circumstances of the breach, the day or period of the breach or an approximate period, a description of the personal information that was breached and to what extent is known, a description of the steps that the organization has taken to lessen the risk of harm resulting from the breach, a description of the steps that affected individuals can take to mitigate or reduce the risk of harm resulting from the breach, and the contact information that can be used by the affected individuals to get more information regarding the breach. (Canadian Government, Legislative Branch, 2018)

The breach report to the OPC should contain breach description, the number of individuals affected, when the breach occurred, type of breach, description of the circumstances of the breach (such as how and why it occurred, when the breach was discovered, where it occurred, and who may have had access to it), description of the relevant security safeguards in place during the time of the breach to prevent the type of incident that happened, description of the personal information that was breached (such as the name, phone number, email address, account numbers, SINs, etc.), description of the steps the organization has taken or is taking to notify the affected individuals, description of the form of notification, and a copy of the notification sent out. This also includes some risk mitigation information as well. (Office of the Privacy Commissioner of Canada)

1. **The target audience of the breach notice (who needs to be told)**

Under PIPEDA, the breach notice must be sent out to the affected individuals. Also, under this law, the Office of the Privacy Commissioner or the OPC does not need to be notified of all breaches. It only requires the OPC to be notified when the breach creates a real risk of significant harm to the individual/s affected. This is regardless if there is 1 or 1,000 that is affected by the breach. Any other organization that can help mitigate harm to the affected individuals must be notified as well. (Office of the Privacy Commissioner of Canada, 2018)

1. **Any timing stipulations affecting when the notice must be made**

The affected individual/s, (and if needed the OPC), must be notified as soon as it is feasible. (Office of the Privacy Commissioner of Canada, 2018)

## Public Administration

1. **What constitutes a breach**

According to the Privacy Act, a breach is considered as the improper or unauthorized use, disclosure, retention, or disposal of personal information. The breach can happen within an institution or off-site. It may be caused by the unintended errors or malicious actions by the employees, third parties, intruders, or the partners in information-sharing agreements. (Government of Canada, 2014)

It can potentially be caused by theft or the loss of device that contains personal information, or the sale or removal of devices that contains personal information that has not been cleared before it was sold/removed. It can also be caused by the transfer of devices without using the correct security measures. Transporting and storing devices outside the office for off-work activities without proper security measures can also be a potential cause of breach. When electronic devices are used incorrectly in transmitting personal information, it can cause a breach. Phishing, pharming, or any other deceptive tactics that trick individuals to providing their personal information, can also cause a breach. (Government of Canada, 2014)

1. **The information that must be contained in a breach notice**

The breach notice should include a general description, and date and time of the incident. It should state the source of the breach, whether it was an institution, a contracted party, or a party to a sharing agreement. It should list the compromised personal information and describe the methods used or to be used to recover the personal information, contain the breach, and prevent it from happening again. The breach should contain suggestions on what the affected individual/s can do to alleviate the risks of identity theft or to handle compromised personal information. The affected individual/s should be able to talk about the breach or get assistance, thus, the name and contact information of an official from the institution should be included in the breach notice. The affected individual/s should also be updated by the institution of any developments while the breach is being investigated further and the issues at hand are resolved. Lastly, the breach should contain a reference to the effect that under the Privacy Act, the Office of the Privacy Commissioner and the Treasury Board of Canada has been notified regarding the nature of the breach, and that the affected individual/s have a right to file a complaint to the OPC’s office, when applicable. (Government of Canada, 2014)

1. **The target audience of the breach notice (who needs to be told)**

The breach must notify the affected individual/s, the Office of the Privacy Commissioner, and the Treasury Board of Canada Secretariat. (Government of Canada, 2014)

1. **Any timing stipulations affecting when the notice must be made**

The individual/s affected by the breach must be notified as soon as it is reasonably possible after the assessment and evaluation of the breach. The Access to Information and Privacy (ATIP) is the single liaison for the institution experiencing the breach when notifying the Office of the Privacy Commissioner (OPC) and the Treasury Board of Canada Secretariat (TBS). The ATIP office can verbally notify the OPC and TBS of the privacy breach at any point during the breach management process, informally. The institutions, however, must still provide a formal written notification or breach report to the OPC and TBS. (Government of Canada, 2014)

# United States

## Business

The FTC or the Federal Trade Commission has a Health Breach Notification Rule that covers vendors of personal health records (PHR), a PHR-related entity, or third-party service provider for a vendor of PHR or a PHR-related entity. This is only for those not under the HIPAA. (FTC, 2010)

The requirement for notification is triggered when there has been unauthorized acquisition of a PHR. When this happens, each person affected by the breach who is a resident or citizen of the United States, the Federal Trade Commission, and in some instances, the media, must be notified. The affected persons must be notified without unreasonable delay, within 60 calendar days from when the breach occurred. If the breach involves 500 or more people, the FTC must be notified as soon as possible, within 10 business days from the discovery of the breach. If it involves less than 500 people, you can send the breach along with any other breach that occurred that same year, as long as it is within 60 calendar days following the end of the calendar year. When there are at least 500 residents of a particular state, the District of Columbia, or a U.S. Territory are affected by the breach, the media has to be notified without any reasonable delay, within 60 calendar days after the discovery of the breach. (FTC, 2010)

The breach notification must include a summarized description of what had occurred, along with the date of the breach and its discovery (if possible), and the kind of PHR that was compromised. If the breach presents a possible risk or harm for the affected individual/s, the notification must include some suggested methods the individual/s can do to protect themselves. The breach notification must also describe the measures taken by the business to investigate the breach, to secure from future breaches, and to mitigate harm caused by the current breach. (FTC, 2010)

### NEW YORK[[2]](#footnote-2)

1. **What constitutes a breach**

A breach is when the integrity, protection, or privacy of the business’ personal information is compromised through unauthorized acquisition of computerized data.

Personal information here could be any information that can be used to identify a natural person. Private information is considered personal information once combined with either the SSN, driver’s license number, non-driver’s ID number, or account number, credit/debit card number (with the security code or anything that can allow access to the person’s financial account)

1. **The information that must be contained in a breach notice**

The breach notice must contain the contact information of the business making the notification. It must also contain a description of what information was compromised in the breach, which involves the specific data elements that were compromised. There are no flexibilities in the requirements for breach notification.

1. **The target audience of the breach notice (who needs to be told)**

The target audience of the breach notice are any resident of New York that is affected by the breach, the Attorney General of New York, the New York State Police, and the New York Department of State.

If the breach affects a lot of people, and more than 5,000 New York residents need to be notified, then the consumer reporting agencies must be notified.

1. **Any timing stipulations affecting when the notice must be made**

Once the security breach is discovered, the obligation for breach notification is triggered. The data owner or licensee should be notified immediately and without unreasonable delay.

If the reporting entity is regulated by the DFS or the Department of Financial Services, then the breach must be reported (or basically any cybersecurity incident) to the DFS within 72 hours from when it occurred.

There are no exceptions to the obligation for the breach notification, even if the entity is complying with other laws such as the HIPPA, GLB, etc.

### CALIFORNIA[[3]](#footnote-3)

1. **What constitutes a breach**

A breach is when a person, agency, or business’ personal information, specifically its security, privacy, or integrity is compromised due to an unauthorized acquisition of computerized data. Personal information here is defined as a person’s first and last name or initial combined with either the person’s SSN, driver’s license number, account number, debit/credit number (with the access code), medical information, health insurance information, or the data collected from an automated system that recognizes license plates. Personal information could also mean the email address or username of the individual combined with the password or security answer or basically a way to get into the individual’s account.

1. **The information that must be contained in a breach notice**

The breach notice must contain the name and contact information of the person/business/organization making the notification/report. It must list the types of personal information that is subject to the breach, and if it is possible to determine, it must include the date/estimated date/date range of the breach. If possible, it should also state if the notification was delayed or not because of police investigation. If possible, it must contain a description of the incident. If an SSN or driver’s license or California ID number was exposed, then the toll-free telephone numbers and addresses of major credit reporting agencies must be added as well. If the source of the breach was the person/business/organization, then they are to provide the proper identity theft protection and mitigation services for not less than 12 months, at no cost, to the affected person. They should also include the information that the affected person needs to accept the offer. If the entity is covered under HIPAA and has complied with HIPAA, then they are considered to have complied with the requirements for notice.

1. **The target audience of the breach notice (who needs to be told)**

The target audience of the breach notice are any resident of California that is affected by the breach and if the notifier is not the owner of the data, then data owner.

If under a single breach, there is a need to notify more than 500 people, the Attorney General must be notified through a single sample copy of the security breach notification. The insurance commissioner must receive the same notice or information sent to the Attorney General’s office, to be given by all the insurers, insurance producers, and insurance support organizations.

1. **Any timing stipulations affecting when the notice must be made**

The notice to the data owner must be made right away and without unreasonable delay. As soon as the breach is found, or after reasonable investigation of it. An additional exception on the timing of the notification depends on the measures needed to check the scope of the breach and restoration of the integrity of the system.

## Health Care

1. **What constitutes a breach**

Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, a breach happens when there is unauthorized use and disclosure of protected health information (PHI) that is unsecured or unencrypted. (American Speech-Language-Hearing Association, n.d.)

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a breach occurs when there is unauthorized use or disclosed of the unsecured protected health information (PHI), in a way that compromises the security and confidentiality of the PHI. The unauthorized use or disclosure of PHI is presumed to be a breach unless the covered entity can demonstrate that there is low probability of the PHI being compromised. This can be demonstrated by checking the nature and extent of the PHI involved, the unauthorized person/people who used the PHI and to whom this was disclosed to, whether or not the PHI was actually acquired or viewed, and to what extent the risk of the PHI has been mitigated. If deemed low probability, then the breach notification is not required. (American Medical Association (AMA), n.d.)

1. **The information that must be contained in a breach notice**

The breach notice must contain a brief description of the breach and it must describe the types of information that were breached. It must include the measures the affected individual/s can take to protect themselves from any potential harm. It must describe what the covered entity is doing to examine the breach, mitigate harm, and avoid more breaches. Lastly, it should include the contact information for the covered entity. The breach notice for the media, if required, must contain the same information as the notice sent to the individuals. (As stated above) (Office for Civil Rights, 2013)

1. **The target audience of the breach notice (who needs to be told)**

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Secretary must be notified of the breach. (Office of Civil Rights, 2015)

Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, covered entities by the HIPAA act must notify the affected individuals, government, and in some cases, the media must be notified. (Thomas Reuters Practical Law, n.d.)

1. **Any timing stipulations affecting when the notice must be made**

Under the HIPAA, if the breach affects 500 or more individuals, the Secretary must be informed without any unreasonable delay, and no later than 60 calendar days from the discovery of the breach. If the breach affects less than 500 individuals, the Secretary must be notified within 60 days towards the end of the calendar year in which the breach was discovered. In this case, however, it is not necessary to wait until the end of the calendar year, the breach may still be reported when it is discovered. (Office of Civil Rights, 2015)

Also under this law, once a covered entity discovers or by reasonable diligence should have discovered a breach, the covered entity has to notify the affected individuals, the HHS, and/or the media without unreasonable delay or up to 60 calendar days following the date of when the breach was discovered, even if when it was discovered the entity was still not sure whether or not the PHI had be compromised. (Office of Civil Rights, 2015)

The prominent media outlets, most likely through a press release, must be informed of the breach affecting more than 500 residents of a state or jurisdiction. This must be done without any unreasonable delay and no later than 60 days from the discovery of the breach. (Office for Civil Rights, 2013)

## Public administration

There are no laws or legislation regarding breach notification governing the federal public sector within the United States.

# ANALYSIS[[4]](#footnote-4)

| COUNTRY | STATE  /PROVINCE | SECTOR | UNDER WHAT CONDITIONS IS A BREACH NOTICE REQUIRED | WHAT INFORMATION IS REQUIRED IN THE BREACH NOTICE | WHO NEEDS TO RECEIVE THE NOTICE IN THE EVEN OF A BREACH | WHAT IS THE TIMING GOVERNING A BREACH NOTICE (WHEN DOES IT HAVE TO BE SENT) |
| --- | --- | --- | --- | --- | --- | --- |
| CANADA |  |  |  |  |  |  |
|  | ONTARIO | HEALTH CARE | * Unauthorized collection, usage, or disclosure of a person’s Personal Health Information * Unauthorized duplication, theft, loss, alteration, or disposal of the PHI * Cyberattacks * Loss or burglary of portable devices * Misdirected faxes * Intentional unauthorized access to electronic medical records | * Date of the breach * Nature and scope of breach * What PHI was breached * Methods used to contain the breach * Where appropriate, name of agent responsible for unauthorized access * Name and contact information of the individual that can address inquiries of affected person/s * Statement letting the affected individual/s know they have the right to file a complaint to the IPC * Suggested precautionary measures – if financial information or government issued documents are breached | * Affected individuals * Privacy Commissioner * When the breach is done by a member of a College of a regulated health profession, and it results in termination, suspension, or any disciplinary action, then the College must be notified as well | * At the first reasonable opportunity * Timing on breach notice depends on the situation, it is possible that a notation can be made in the affected individual’s file and the breach will be discussed during the next appointment. |
|  | ALBERTA | HEALTH CARE | * When the health information, that can individually identify someone, is lost, or is accessed or disclosed by an unauthorized entity * The risk of harm to the affected individual must be assessed and if there is any, then the breach notice is required. | NOTIFYING THE AFFECTED INDIVIDUAL/S:   * Description of the situation of the breach * Date or period of when the breach occurred * Description of what personal information was breached or compromised * Any measures the organization has taken to reduce the risk of harm * Contact information of a person from the organization or on behalf of the organization that can answer inquiries about the breach   NOTIFYING THE COMMISSIONER:   * All the information required when notifying the individual * Assessment of the risk of harm to the affected individual/s * Estimated number of individual/s that have a real risk of harm   Contact information of a person from the organization or on behalf of the organization that can answer the Commissioner’s inquiries about the breach | * Affected individual/s * The Information and Privacy Commissioner of Alberta * Minister of Health | * As soon as practicable * As soon as it is determined that there is a risk of harm for the affected individual. |
|  | FEDERAL | PRIVATE | * When there is loss, unauthorized access, or disclosure of personal information that resulted from a breach of the security safeguards of an organization or from failure to establish the safeguards | * Description of the circumstances of the breach * The day or period of the breach or an approximate period * Description of the personal information that was breached and to what extent is known * Description of the steps that the organization has taken to lessen the risk of harm * Description of the steps that affected individuals can take to mitigate or reduce the risk of harm * Contact information that can be used to get more information about the breach | * The affected individual/s * Office of the Privacy Commissioner – when breach creates real risk of significant harm on affected individual/s * Any organizations that can help mitigate the harm to the affected individual/s. | * As soon as it is feasible. |
|  | FEDERAL | PUBLIC | * When there is improper or unauthorized use, disclosure, retention, or disposal of personal information, whether within an institution or off-site. * Unintended errors or malicious actions by the employees, third parties, intruders, or the partners in information-sharing agreements. * Theft or the loss of device that contains personal information * Sale or removal of devices that contains personal information that has not been cleared before it was sold/removed. * Transfer of devices without using the correct security measures * Transporting and storing devices outside the office for off-work activities without proper security measures * When electronic devices are used incorrectly in transmitting personal information * Phishing pharming, or any other deceptive tactics that trick individuals to providing their personal information | * General description of incident * Date and time of the incident. * Source of the breach (institution, contracted party, or party to a sharing agreement) * List of the compromised personal information * Description of the methods used or to be used to recover the personal information, contain the breach, and prevent it from happening again. * Suggestions on what the affected individual/s can do to alleviate the risks of identity theft or to handle compromised personal information. * Name and contact information of an official from the institution who can answer the affected individual/s inquiries * Updates from institution of any developments while the breach is being investigated further and the issues at hand are resolved. * Reference to the effect that under the Privacy Act, the Office of the Privacy Commissioner and the Treasury Board of Canada has been notified regarding the nature of the breach, and that the affected individual/s have a right to file a complaint to the OPC’s office, when applicable. | * Affected Individual/s * The Office of the Privacy Commissioner (OPC) * The Treasury Board of Canada Secretariat (TBS) | * Individual/s affected by the breach - as soon as it is reasonably possible after the assessment and evaluation of the breach. * The Access to Information and Privacy (ATIP) office can verbally notify the OPC and TBS of the privacy breach at any point during the breach management process, informally. The institutions must still provide a formal written notification or breach report to the OPC and TBS. |
| U.S.A. |  |  |  |  |  |  |
|  | NEW YORK | PRIVATE | * When a breach is discovered * When the integrity, protection, or privacy of the business’ personal information is compromised through unauthorized acquisition of computerized data. | * Contact information for the business that is making the notification * Description of the compromised information * Specific data elements that were compromised * No flexibilities in the requirements for breach notification. | * Any affected resident of New York * NY Attorney General * NY State Police * NY Department of State * Consumer Reporting Agencies (if more than 5,000 NY residents affected) | * Once the security breach is discovered. * The data owner or licensee should be notified immediately, without unreasonable delay. * If the reporting entity is regulated by the DFS, then the breach must be reported (or basically any cybersecurity incident) to the DFS within 72 hours from when it occurred. * No exceptions even if entity is complying with other laws (HIPPA, GLB, etc.) |
|  | CALIFORNIA | PRIVATE | * When a breach is discovered * When the personal information of a person, business, or agency has be acquired by an unauthorized entity. | * Name and contact information of reporting person/business * Types of personal info that were breached * *If possible****,*** Date (exact, estimate or date range) of the breach * Date of the notice * Was the notification delayed due to police investigation? * General description of incident * *If SSN, driver’s license, or CA ID No. was breached,* toll-free numbers and addresses of major credit reporting agencies * *If person/business caused breach,* offer for free (minimum 12 months) identity theft prevention and mitigation services to affected persons * If entity is covered and complied with HIPAA, then they are considered to have complied with the requirements for notice. | * Any affected resident of California * Data owner * Attorney General, if more than 500 NY residents need to be notified. * Insurance commissioners by all the insurers, insurance producers, and insurance support organizations. | * As soon as the breach is found, or after reasonable investigation * Depending on the measures needed to check the scope of the breach and restoration of the integrity of the system. |
|  | FEDERAL | HEALTH CARE | * Unauthorized use or disclosed of the unsecured protected health information (PHI), in a way that compromises the security and confidentiality of the PHI * Unauthorized use or disclosure of PHI is presumed to be a breach unless the covered entity can demonstrate that there is low probability of the PHI being compromised * Low probability can be demonstrated by checking:  1. nature and extent of the PHI involved 2. the unauthorized person/people who used the PHI and to whom this was disclosed to 3. if the PHI was acquired or viewed 4. to what extent the risk of the PHI has been mitigated.  * If deemed low probability, then the breach notification is not required. | * Brief description of the breach * Description the types of information that were breached * Measures the affected individual/s can take to protect themselves from any potential harm * Description of what the covered entity is doing to examine the breach, mitigate harm, and avoid more breaches. * Contact information for the covered entity | * affected individuals * government * Secretary * in some cases, the media | * If the breach affects 500 or more individuals, the Secretary must be informed without any unreasonable delay, and no later than 60 calendar days from the discovery of the breach. * If the breach affects less than 500 individuals, the Secretary must be notified within 60 days towards the end of the calendar year in which the breach was discovered but it is not necessary to wait until the end of the calendar year, breach may still be reported when it is discovered. * the affected individuals, the HHS, and/or the media - once a covered entity discovers or by reasonable diligence should have discovered a breach, should be without unreasonable delay or up to 60 calendar days following the date of when the breach was discovered, even if when it was discovered the entity was still not sure whether or not the PHI had be compromised. * media outlets - must be done without any unreasonable delay and no later than 60 days from the discovery of the breach. |
|  | FEDERAL | PUBLIC | N/A | N/A | N/A | N/A |

# References

American Medical Association (AMA). (n.d.). *HIPAA Breach Notification Rule*. Retrieved November 13, 2020, from American Medical Association (AMA): https://www.ama-assn.org/practice-management/hipaa/hipaa-breach-notification-rule

American Speech-Language-Hearing Association. (n.d.). *Health Information Technology for Economics and Clinical Health (HITECH) Act*. Retrieved November 13, 2020, from American Speech-Language-Hearing Association: https://www.asha.org/Practice/reimbursement/hipaa/HITECH-Act/

Banks, T. (2018, August 08). *New mandatory breach notification for health information in Alberta*. Retrieved November 11, 2020, from iapp: https://iapp.org/news/a/new-mandatory-breach-notification-for-health-information-in-alberta/#:~:text=New%20mandatory%20breach%20notification%20for%20health%20information%20in%20Alberta,-schedule%20Aug%208&text=On%20Aug.,personal%20health%20information%20d

Canada Gazette. (2018, March 27). *Breach of Security Safeguards Regulations: SOR/2018-64*. Retrieved November 11, 2020, from Government of Canada: http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html

Canadian Government, Legislative Branch. (2018, March 27). *Breach of Security Safeguards Regulations*. Retrieved from Justice Laws Website: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2018-64/page-1.html

Canadian Government, Legislative Branch. (n.d.). *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)*. Retrieved November 11, 2020, from Justice Laws Website: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/nifnev.html

FTC. (2010, April). *Complying with the FTC's health breach notification rule*. Retrieved November 13, 2020, from FTC: https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

Government of Canada. (2014, May 20). *Guidelines for Privacy Breaches*. Retrieved November 13, 2020, from Government of Canada: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154

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

Government of Canada. (2016, March 04). *For Discussion — Data Breach Notification and Reporting Regulations*. Retrieved November 12, 2020, from Government of Canada: https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html#s2.3

Gowling WLG. (2020, October 01). *Guide to doing business in Canada: Privacy Law*. Retrieved from Gowling WLG: https://gowlingwlg.com/en/insights-resources/guides/2020/doing-business-in-canada-privacy-law/#pt3

*Health Information Act*. (n.d.). Retrieved November 12, 2020, from Alberta: https://www.alberta.ca/health-information-act.aspx

Information and Privacy Commissioner of Ontario. (2018, October). *Responding to a Health Privacy Breach: Guidelines for the Health Sector.* Retrieved November 12, 2020, from IPC - Information and Privacy Commissioner of Ontario: https://www.ipc.on.ca/wp-content/uploads/2018/10/health-privacy-breach-guidelines.pdf

Johnson, J. (2016, June 01). *Changes to Ontario’s Health Information Privacy Law Include Breach Notification, Increased Penalties*. Retrieved November 12, 2020, from Mccarthy Tetrault: https://www.mccarthy.ca/en/insights/blogs/snipits/changes-ontarios-health-information-privacy-law-include-breach-notification-increased-penalties

Office for Civil Rights. (2013, July 26). *Health Information Privacy, Breach Notification Rule*. Retrieved November 13, 2020, from U.S. Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Office of Civil Rights. (2015, January 5). *Health Information Privacy, Submitting Notice of a Breach to the Secretary*. Retrieved November 13, 2020, from U.S. Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Office of the Privacy Commissioner of Canada. (2018, October). *What you need to know about mandatory reporting of breaches of security safeguards*. Retrieved November 12, 2020, from Office of the Privacy Commissioner of Canada: 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/

Office of the Privacy Commissioner of Canada. (n.d.). *PIPEDA breach report form.* Retrieved November 12, 2020, from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/media/4844/pipeda\_pb\_form\_e.pdf

Privacy Rights Clearinghouse. (2018). *Data Breach Notification in the United States and Territories.* Retrieved November 14, 2020, from IAPP-International Association of Privacy Professionals: https://iapp.org/media/pdf/resource\_center/Data\_Breach\_Notification\_United\_States\_Territories.pdf

Province of Alberta. (2018, December 12). *Personal Information Protection Act.* Retrieved November 11, 2020, from Province of Alberta: https://www.qp.alberta.ca/documents/Regs/2003\_366.pdf

Thomas Reuters Practical Law. (n.d.). *Health Information Technology for Economic and Clinical Health (HITECH) Act*. Retrieved November 13, 2020, from Thomas Reuters Practical Law: https://ca.practicallaw.thomsonreuters.com/3-501-7466?transitionType=Default&contextData=(sc.Default)&firstPage=true

Wikipedia. (n.d.). *Data breach*. Retrieved November 11, 2020, from Wikipedia: https://en.wikipedia.org/wiki/Data\_breach

1. Referenced from (Wikipedia, n.d.) [↑](#footnote-ref-1)
2. All information under this section if retrieved from (Privacy Rights Clearinghouse, 2018) [↑](#footnote-ref-2)
3. All information in this section is retrieved from (Privacy Rights Clearinghouse, 2018) [↑](#footnote-ref-3)
4. All information referenced in the paragraph sections above. [↑](#footnote-ref-4)