InterPARES Trust Project Final Report

Title:		NA18 - Assessment of Privacy-Preserving and Security Techniques for Records Management in Cloud Computing
Status:		Final
Version:		1.0
Date submitted:		2017-12-29
Last reviewed:		2017-12-29
Author:		InterPARES Trust Project
Writer(s):		Eun G. Park and Victor Liang
Research domain:		Security
URL:		

Document Control

Version history			
Version	Date	By	Version notes
1.0	Dec 29, 2017	E. Park and V. Liang	Final report submitted

Table of Contents

Executive Summary

The emergence of cloud computing has significantly improved the potential for sharing data. However, the major obstacle to adopting this technology in the public sector is a lack of trust in sufficient security and privacy protection. This case study aims to explore the current privacy-related requirements that could be applicable to cloud environments, especially for institutions that host person-specific information, and to examine the readiness of health and government agencies in making a technological shift to the cloud for their records management practices. Based on the findings, we plan to make suggestions on how to manage security and privacy issues in records management practices at government and health agencies. The following methodology is being used in the study: (1) conduct a literature review on the current legal guidelines for privacy management in the United States and Canada; (2) examine the available security and privacy-preserving techniques and tools that could be applicable to the cloud and develop and choose one technique; (3) select one privacy-preserving technique to be tested at host sites with person-specific information; (4) conduct a case study to test how the technique can legally and technically protect the privacy of records and data at the sites (e.g. at government agencies and health care service providers); and (5) based on the findings of the case study, make suggestions on how to manage security and privacy risks in records and data management at government and health agencies.

A review of the current legal guidelines for privacy management in the United States and Canada has been done. The mandatory requirements of the three acts have been identified. A review of the available security and privacy-preserving techniques and tools that could be applicable to the cloud has been completed. Based on this review, one privacy-preserving technique has been selected to be tested at host sites that handle person-specific information.

With the chosen technique, a case study was conducted at the Société de transport de Montréal, the transportation agency for the city of Montreal, Quebec, Canada, to test how the technique can protect privacy in records and data that is kept at this Canadian site. The results of the case study show that the level of protection is theoretically guaranteed. Then, we checked the data with the mandatory privacy requirements that we identified. After anonymization, age and social status information from a passenger's transportation card was not revealed. Thus, legal requirements are also met. Nevertheless, there is still a risk in protecting privacy and security at privacy sensitive institutions.

1. Introduction

In the past couple of decades, many privacy-preserving records and data management techniques have been developed to address privacy issues in different data sharing institutions. The emergence of cloud computing has significantly improved the potential for sharing data. However, a major obstacle to adopting this technology in the public sector is a lack of trust in there being sufficient security and privacy protection. Thus, there is a need to assess privacy-preserving techniques and tools that are both readily available and frequently used in the field to test how well these techniques and tools could help legally and technically (e.g. both theoretically and practically) protect privacy and security at institutions that are held to high privacy and security requirements.

Our literature review revealed that there is a lack of control when outsourcing to third-party cloud computing providers, which is a problem that is further exacerbated by a lack of clarity and uniformity between laws, both nationally and internationally, leading to breaches and the misuse of data. The result is a buyer-beware situation in which due diligence and contracts between users and providers are key to protecting personal data and ensuring accountability.

Protecting privacy rights should never be largely left up to providers and consumers, but current laws are not adequate enough. The way in which many organizations and companies have mishandled private information is reflective of this, as well as reflective of the general underappreciation of risks associated with cloud computing; therefore, those using cloud computing services need to be vigilant and proactive. Despite the numerous risks involved, consumers do not have much choice now, as they face a situation in which they should decide between accessing important or essential services, such as healthcare and government services, or being left behind without any alternative resources that would enable them to fully participate in society.

2. Aims and Objectives

The objectives of this case study are (1) to examine the security and privacy challenges of hosting person-specific information in the cloud; (2) to study the readiness of health and government agencies in making a technological shift to the cloud; (3) to evaluate state-of-the-art privacy-preserving techniques, mechanisms and tools in the context of the cloud environment; and (4) make suggestions on how to manage security and privacy issues in records management practices within government and health agencies.

3. Methodology

1. Conduct a literature review on the current legal guidelines of privacy management in the United States and Canada. Researchers conducted a

literature review on privacy guidelines, such as the *Health Insurance Portability and Accountability Act* and the *Personal Information Protection and Electronic Documents Act* in North America. Develop criteria to evaluate privacy management;

2. Based on the criteria driven by the literature review, examine the available security and privacy-preserving techniques and tools that could be applicable to the cloud and develop and choose one technique;

3. Choose one privacy-preserving technique for implementation and testing at host sites with person-specific information;

4. Conduct a case study to test how the technique could legally and technically protect privacy preserving records and data at the sites (e.g. within government agencies or a health care service provider); and

4. Findings

4.1. Comparison of Laws

A review of the current legal guidelines of privacy management in the United States and Canada (Privacy Act of 1974 and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; and the Health Insurance Portability and Accountability Act (HIPAA) in the US) has been completed.

PIPEDA is the Canadian federal privacy protection law that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. PIPEDA applies to federal works, undertakings and businesses with regards to an employee's personal information. PIPEDA generally applies to organizations' commercial activities in all provinces, except where provinces have created their own privacy laws. In recent years, while there has been a strong push towards moving data to the cloud for financial and efficiency reasons, various stakeholders and players have urged caution. As Melodie Szeto and Ali Miri point out, PIPEDA is a consent-based Act, so companies must have consent "from individuals to collect, use, and disclose personal information. Under the Act, companies cannot refuse services to an individual that refuses to consent to collection of information beyond what is 'required to fulfill the explicitly specified, and legitimate purposes" (2007, pp. 2-3).

Like PIPEDA, HIPAA aims to strike a balance between providing better services and the protection of personal information. HIPAA focuses exclusively on the healthcare sector and identifiable health information of United States citizens. While cloud computing has created major innovations in health care research, it also presents a serious risk to patient privacy and confidentiality. Yang and Borg point out that "records of patients'

personal medical histories and others identifying data are at a high risk of being abused when stored in the cloud currently, because patient data is in an invisible place that is constantly threatened by hackers and internal breaches in security" (Yang & Borg, 2012, p. 145).

The Privacy Act 1974 is a U.S. federal law that establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. Parker sees that the current U.S. legislation does not adequately protect end-users' privacy because it does not recognize the nature of personal information (2014). It gets worse: the federal statute does not directly address the collection and use of data collected from the end-users of cloud computing providers under contract with the Federal Government (Parker, 2014).

Although several laws might provide the framework for future legislative action to address these issues, the development of technology has again outpaced the development of relevant legislation. Ryan also remarked that "despite the numerous technical benefits of cloud computing, consumers should consider what legal rights and responsibilities are with cloud computing technologies. As with the technologies, the applicability of existing laws and the possibility of new laws tailored specifically to the new technologies remain unclear" (Ryan, 2014, p. 498). Although the U.S. Federal Government has demonstrated some awareness and sensitivity to data privacy concerns in the cloud computing context, it seems that the security of the data is purposefully placed within the control of cloud computing service providers, while regrettably ignoring end-user privacy" (Parker, 2014, 400-1).

As a way to solve a problem, Ryan indicates that there should be one uniform set of standards and regulations and requirements acceptable for existing laws and applications (2014). The European Union is on the way toward decreasing uncertainty by publishing standards and clearing up regulatory framework. Ryan suggested that "there is more need for quick action or at least clear communication between legislators, the judiciary, prosecutors, and players in the cloud computing industry" (2014, 523-4).

The comparative Summary table of PIPEDA, HIPPA, and Privacy Act is attached in 6. Products, 6.1. Comparative Summary of PIPEDA, HIPPA, and Privacy Act.

4.2. The privacy requirements of the three acts

The mandatory and optional privacy requirements of the three acts have been identified. The full list is attached in 6. Products, 6.2. The mandatory and optional privacy requirements of the three acts.

4.3. Case Study

A review of available security and privacy-preserving techniques and tools that could be applicable to the cloud has been made. Based on this review, one privacy-preserving technique has been selected to be tested at host sites with person-specific information (e.g. within government agencies and a health care service provider). With the selected technique, a case study was conducted to test how the technique can protect privacy preserving records and data at the Canadian site.

The case study was conducted at the Société de transport de Montréal (STM, http://www.stm.info), the transportation agency in Montreal, Quebec, Canada. The STM is searching for a privacy-preserving data publishing method to share its information internally across different departments, as well as externally to other transportation companies. We intended to evaluate the potential privacy threats of releasing raw passenger transit data with the chosen technique and to study the feasibility of applying an existing state-of-the-art data anonymization method to the real-life transit data.

We obtained two real-life transit datasets for the metro and bus, which represent a 2-week transit history of passengers in the STM metro and bus networks. The Metro dataset contains 847,668 records of 68 metro stations. An anonymization method was adopted to convert the STM trajectory data by removing passengers' names and ages from the dataset in order to protect the privacy of every passenger. Thus, a high level of protection is theoretically guaranteed. Then, we checked the data according to the mandatory privacy requirements of PIPEDA, the Privacy Act of 1974 and HIPAA to identify whether legal requirements were met.

As the STM issues specific transportation cards to seniors and students only by confirming their ages and names, other information related to privacy is not collected. Information on social status may be revealed via their age because the transportation card application form indicates whether the person is a senior or a student according to their age. After anonymization, age and social stats information from a passenger's transportation card cannot be revealed. Thus, legal requirements are also met, although the STM's transportation card includes limited information about passengers.

The second case study was to be done with the Ministry of Health of British Columbia. The aim was to receive data access permission from the host institution. Due to the sensitivity of their data, which belongs to a government agency, permission request procedures were complicated and therefore would have prohibited the success of the case study.

4.4. Literature Review Summary

The literature review mainly looked at three privacy-related laws in the United States and Canada: Canada's Personal Information Protection and Electronic Documents Act

(PIPEDA), and the US Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Act 1974. The aim of the literature review was to examine the applicability of these laws to cloud computing, and whether the three laws sufficiently protect Personal Information stored in the cloud.

The literature review considered the legal and security risks of storing personal information on the cloud - including jurisdictional differences in privacy and cloud computing laws, the cross-border transfer of personal information, disclosure and misuse of personal information, hacking and privacy breaches, and loss of data control - as well as socio-technological challenges. The following is a summary of the main findings from the literature review.

One of the major legal obstacles of storing data in the cloud is the geo-jurisdictional location of information and the applicable law of the jurisdiction where data is purported to reside in, which may come in conflict with local laws and regulations protecting personal information. This is a significant issue, especially as organizations increasingly outsource cloud computing to service providers in a different jurisdiction and data may travel through multiple different jurisdictions as it is being processed. The Office of the Privacy Commissioner of Canada identified jurisdiction as one of the overarching problems with cloud computing (Office of the Privacy Commissioner of Canada, 2010). Waggott et al's study remarked, "by transferring data to the cloud, an organization relinquishes a degree of control and must manage the relationship between its privacy obligations in the jurisdiction where it collects personal information, and the governing privacy laws in the jurisdictions" (2013, p. 1).

One way in which the government has dealt with data crossing through different jurisdictions that have different laws has been by legislating the use of contracts, obligating cloud providers to adhere to the privacy laws of the jurisdiction in which the personal information originates from. For example, under HIPAA, service providers that handle Personal Health Information, such as cloud providers, are referred to as "business associates" and are also governed by HIPAA and therefore held liable for violations (Determann and Zee, 2013, pp. 16-17). Business associates located outside of the US are not exempt from HIPAA's scope. Subcontractors of business associates are also caught up in HIPAA (Determann and Zee, 2013).

Standards are also important in cloud computing for a variety of reasons, in order to assure customers that using the cloud is safe with the existing standards for cloud security and data protection in the cloud (Gleeson & Walden, 2014). However, the complexity and ambiguity of many of the standards is one of the key obstacles in the uptake of cloud computing (Gleeson & Walden, 2014).

One of the most significant barriers to adopting cloud computing solutions is security: According to Hashizume et al. (2013): "Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are

no longer enough for clouds in their current form" (p. xx). In their most recent report on the top cloud computing threats, the Cloud Security Alliance ("CSA") states that "[t]he risks of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers. A cloud environment is subject to the same threats as a traditional corporate network as well as new avenues of attack by way of shared resources, cloud provider personnel and their devices and third-party partners of the cloud provider. Cloud providers are highly accessible and the vast amount of data they host makes them an attractive target" for hackers (2016, p. 8). Recent examples of data breaches demonstrate that current security measures in the public sector are insufficient and that breaches may come from the inside as well as the outside.

Experts and users alike have identified the loss of control over data as one of the top cloud computing security concerns, mainly because maintaining identity and access control in the cloud becomes challenging when one is employing "multiple cloud providers, managing diverse standards and handling third-party access to your data and applications within the cloud context" (Wang, 2010, p 3). Losing control of one's data is as much a legal issue as it is a security issue, as businesses and individuals "fear that data may not be adequately protected in a third country due to different standards in different countries. The differentiation between national legislation may affect the effective prevention of cross-border data security breach and the complexity of determining the competent court due to complicated connecting factors such as the establishment of the controllers (cloud customers/clients) and the location of data centres, which may pose a further threat to rights protection" (Wang, 2013, p. 60). As much as legal and security risks top the list of problems with storing data in the cloud, there are other challenges that are more grounded in social and technological factors, such as the intersection between our definitions of cloud computing and the rapid advancement of technology. Although several laws might provide the framework for future legislative action to address these issues, the development of technology has again outpaced the development of relevant legislation." (Parker, 2014, pp. 400-1). Despite the immense benefits and promises of cloud computing, Parker suggests that we should not move so hastily towards the cloud until we have first figured out how to protect end-users' privacy, which under current laws and regulations are at the mercy of cloud providers and other forces that seek to take advantage of lax protections.

In addition, there is a lack of control when outsourcing to third-party cloud computing providers, which is a problem that is further exacerbated by a lack in clarity and uniformity between laws, both nationally and internationally, leading to breaches and misuse of data. The result is a buyer-beware situation in which due diligence and contracts between users and providers are key to protecting personal data and ensuring accountability. Stephen Turner states that ultimately the decision to move to the cloud may end up being more about costs than the protection of personal information, as "the cloud model might be acceptable to organizations concerned more about costs than the value of their information" (2013, p. 6). Protecting privacy rights should never be largely left up to providers and consumers, but current laws are not adequate enough, and the way many organizations and companies have mishandled our private information is reflective of this and the general underappreciation of risks associated with cloud

computing. Therefore, those using cloud computing services need to be vigilant and proactive. Despite numerous risks, consumers may not have much of a choice at the moment, as they face a situation in which they have to decide between accessing important or essential services and not being able to participate in those services at all.

5. Conclusions

We presented the preliminary findings of this study at the InFuture 2015 conference.

While this study reports only a small part of the law comparison, literature review and one case study, it points toward both the need and the value of examining privacy and security related laws and techniques in the field. The findings imply there is still the potential for risks in the cloud. Therefore, continuous improvement is needed in protecting person-specific information at institutions that are held to high privacy and security requirements.

6. Products

6.1. Comparative Summary of PIPEDA, HIPPA, and Privacy Act

	PIPEDA	HIPPA	Privacy Act 1974
ORIGIN	● Received Royal Assent on April 13, 2000 ● Following Royal Assent, was implemented in phases over a three-year period that began on January 1, 2001. ● Came into effect to promote consumer trust in electronic commerce. ● In 2000, the need for private sector privacy legislation at that time was clear – Canadians were demanding adequate privacy protection in a new digital economy. ● PIPEDA was also intended to reassure the European Union that the Canadian privacy law was adequate to protect the personal information of European citizens.	● HIPAA enacted August 21, 1996. ● The impetus for the creation of the HIPAA Privacy Rule due to the shift of medical records from paper to electronic formats, increasing the potential for individuals to access, use, and disclose sensitive personal health data. ● Previous legal protections at the federal, tribal, state, and local levels were inconsistent and inadequate in protecting individual privacy.	● The Privacy Act enacted September 27, 1975. ● Privacy Act had its origins in the late 1960's when people became concerned about abuses that could occur with computer data banks. ● Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal. ● Congress was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an

			individual's social security number.
PURPOSE	● Sets out ground rules for how private sector organizations can collect, use or disclose personal information in the course of commercial activities. ● Balances an individual's privacy rights with the need of organizations to collect, use or disclose personal information for legitimate business purposes i.e. reasonable and appropriate purposes.	● Primary goal of the HIPAA Privacy Rule is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs. ● The HIPAA Privacy Rule assures that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.	● To balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. ● To restrict disclosure of personally identifiable records maintained by agencies. ● To grant individuals increased rights of access to agency records maintained on themselves; and the right to seek amendment of agency records maintained on themselves. ● To establish a code of "fair information practices".
TARGET AUDIENCE	● PIPEDA targets federal works, undertakings or businesses, and applies to organizations' commercial activities in all provinces, except	● HIPAA's Privacy Rule apply to covered entities, those being: health plans, health-care clearinghouses, and to any health-care provider who transmits health information in	● The Privacy Act applies to the executive branch of the federal government. The Executive Branch encompasses administrative

	organizations that collect, use or disclose personal information entirely within provinces that have their own privacy laws, which have been declared substantially similar to the federal law. ● PIPEDA does not apply to organizations that are not engaged in commercial activity e.g. non-profit, political parties, and charity groups.	electronic form in connection with transactions for which the Secretary of Health and Human Services has adopted standards under HIPAA. ● The Privacy Rules affect the day-to-day business operations of all organizations that provide medical care and maintain personal health information.	agencies, government corporations, and government-controlled corporations. ● Only U.S. citizens and lawfully admitted aliens are given rights under the act. ● The Act does not apply to records kept by state and local governments or by private companies or organizations.
STRUCTURE	● Six parts. ● Part 1 covers "Protection of Personal Information in the Private Sector". ● Part 2, entitled "Electronic Documents", seeks to provide for the use of electronic alternatives where federal laws contemplate the use of paper to record or communicate information or transactions. ● Part 3 amends the *Canada Evidence Act*. ● Part 4 amends the *Statutory Instruments Act*. ● Part 5 amends the *Statute Revision Act*.	● Two main sections: Title I dealing with Portability and Title II that focuses on Administrative Simplification. ● Title II establishes a set of standards for receiving, transmitting and maintaining healthcare information and ensuring the privacy and security of individually identifiable information. ● Title II contains the Privacy Rule and houses HIPAA's privacy provisions. ● Within HHS, the Office for Civil rights has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.	● The Privacy Act safeguards privacy through creating four procedural and substantive rights in personal data. ● First, the act requires government agencies to show an individual any records kept on him or her. ● Second, the act requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. ● Third, the act places restrictions on how agencies can share an individual's

	● Part 6 covers the "Coming Into Force" of the other Parts of the Act. ● Under PIPEDA, the Office of the Privacy Commissioner has an ombuds function. The Commissioner does not have order-making authority but, rather, functions as a sort of mediator, conciliator, and educator. ● The Commissioner does not have any power under PIPEDA to enforce the findings and directives to the respondents.		data with other people and agencies. ● Fourth, the act lets individuals sue the government for violating its provisions. ● There are, however, several exceptions to the Privacy Act, e.g. government agencies that are engaged in law enforcement can excuse themselves from the Act's rules. ● Individuals who are denied access to their records may file an administrative appeal with the agency withholding the information. ● A basic requirement to show that the Act applies is that the records are contained within a "system of records".
FEATURES	● The core features of PIPEDA include: obtaining consent and identifying the purpose for the collection of personal information, procuring additional consent, express consent in some cases, for any	● The Privacy Rule regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information, PHI. PHI is individually identifiable health information that is transmitted or	● Provides the Government with a framework to conduct its day-to-day business when that business involves the collection or use of information about individuals.

	secondary uses or disclosures of the information. ● To make consent valid, the act requires communicating to individuals what personal information is being collected, and how it will be used, disclosed, and protected.	maintained in any form or medium (e.g., electronic, paper, or oral). ● Provides national standards for protecting PHI. ● Regulates how covered entities "use and disclose" certain PHI. ● Gives patients more protection and control over their PHI. ● Sets boundaries on the use and release of health records. ● Establishes appropriate safeguards protecting the privacy of PHI.	● Privacy Act puts various requirements on agencies involving collecting only relevant and necessary information, transparency, consent, safeguards, access to records, and providing public with opportunity to correct records. ● The Act requires that agencies give public notice of their systems of records by publication in the Federal Register.

6.2. The mandatory and optional privacy requirements of the three acts

	PIPEDA	**HIPPA**	**Privacy Act 1974**
PRIVACY REQUIREMENTS (MANDATORY)	● "Personal information" includes information in any form, such as: o Age; o Name; o ID numbers; o Income; o Ethnic origin; o Blood type; opinions; o Evaluations; o Comments;	● Elements comprising "PHI": o Geographic subdivisions smaller than a State; o Elements of dates directly related to an individual; o Phone numbers; o Fax numbers; o E-mail addresses; o Social security numbers; o Medical record numbers;	● Each agency that maintains a system of records shall: o maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be

	o Social status; o Disciplinary actions; o Employee files; o Credit records; o Loan records; o Medical records; o Existence of a dispute between a consumer and merchant. ● A privacy breach occurs when there is unauthorized access to, or collection, use, or disclosure of personal information, unless the Act authorizes it. ● Consent must be meaningful, and can be either expressed or implied: o Expressed consent is given explicitly orally, in writing, or through a specific online action and does not require inference; and o Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. ● Mandatory Exceptions to Access Principle (general	o Health plan beneficiary numbers; o Account numbers; o Certificate/license numbers; o Vehicle identifiers and serial numbers; o Device identifiers and serial numbers; o URLs; o IP address numbers; o Biometric identifiers; o Full face photographic images and comparable images; and o any other unique identifying number, characteristic, or code. ● A <u>covered entity</u> "may not use or disclose protected health information (see above), except either: o As the Privacy Rule permits or requires; or o As the individual who is the subject of the information authorizes in writing." ● Group health plans must provide notice of privacy practices in accordance with the elements set out in the Privacy Rule. ● Covered entities are required to have policies in place by which to accept	accomplished by statute or by executive order of the President; o collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; o inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual – (A) the authority (whether granted by statute, by executive order of the President) which

	obligation to provide access to severable and non-severable personal information upon request). Organizations must refuse access if the information: o If it would reveal personal information about another individual unless there is consent or a life-threatening situation; or o If an individual requests that he or she be informed of information disclosed to a government institution in certain specified cases, or for access to the information itself, and the government institution objects to the institution complying with the access request.	or deny individuals' requests for restrictions on uses and disclosures. ● A Privacy Rule Authorization is an individual's signed permission to allow a covered entity to use or disclose PHI that is described in the Authorization for the purpose and to the stated recipient. Must contain core elements and required statements per the Privacy Rule.	authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to the Act; and (D) the effects on the individual, if any, of not providing all or any part of the requested information; o publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include – (A) the

			name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be

			notified at their request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at their request how they can gain access to any record pertaining to them contained in the system of records, and how they can contest its contents; and (I) the categories of sources of records in the system; o maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

			o prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to the Act, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes; o maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity; o make reasonable efforts to serve notice on an

			individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record; o establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this Act and the penalties for noncompliance; o establish appropriate administrative,

			technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; o at least 30 days prior to publication of information under the Act, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data,

			views, or arguments to the agency. ● Agencies may only share information if there is a written agreement between the agencies that has been submitted to the Committee on Government Affairs of the Senate and the Committee on Government Operations of the House, and has been made available to the public. ● Disclosure of records that are retrieved from a system of records is prohibited. There are various exceptions falling into two classes: o The agency may disclose information with permission from the individual; o or if it can meet one of the following twelve conditions: ▪ the disclosure is to an agency employee who normally maintains the

			record and need it in the performance of duty; ▪ the disclosure is made under the FOI Act; ▪ the disclosure is for a "routine use;" ▪ the disclosure is to the Census Bureau for the purposes of a census survey; ▪ the disclosure is to someone who has adequately notified the agency in advance that the record is to be used for statistical research or reporting, and the record is transferred

			without individually identifying data; ▪ the disclosure is to the National Archives and Records Administration as a record of historical value; ▪ the disclosure is to an agency "of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity," and if the record is provided in response to a written

			request by the head of the agency; ▪ the disclosure is made where there are "compelling circumstances" affecting someone's health or safety, and the person whose health or safety is affected is sent a notification of the disclosure; ▪ the disclosure is made to Congress, or any committee or subcommittee within Congress; ▪ the disclosure is made to the

			Comptroller General in the course of the duties of the General Accounting Office; ▪ the disclosure is made pursuant to a court order; ▪ the disclosure is made to a consumer reporting agency in accordance with 31 U.S.C. 3711(e).

PRIVACY REQUIREMENTS (OPTIONAL)	● Discretionary Exceptions to Access Principle (general obligation to provide access to severable and non-severable personal information upon request). Organizations may refuse access if the information: o Is protected by solicitor-client privilege; o Would reveal confidential commercial information; o Would reasonably be expected to harm an individual's life or security; o Was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law;	● Covered entities may decide whether to obtain an individual's consent in order to use or disclose PHI for treatment, payment, and health care operations purposes, and with regard to the content of the consent and the manner of obtaining it. ● Covered entities may establish a policy requiring individual consent in order to make certain other disclosures that are otherwise permitted without individual consent or authorization. ● Covered entities are not required to agree to an individual's request for restriction on uses and disclosures (but they are required to have policies in place by which to accept or deny such requests). ● Covered entities may establish a policy for granting restrictions for certain other disclosures that are otherwise permitted. ● Group health plans may describe limitations on uses and disclosures that go beyond the requirements of the Privacy Rule that it voluntarily adopts. ● An Authorization may, but is not required, to include additional, optional elements so long as they are	● For agencies sharing information through a "matching agreement," an agreement may be renewed at the discretion of the agencies. ● "Routine use" exception does not have to be a purpose identical to the purpose for collecting the record, it only has to be a compatible purpose.

	○ Was generated in the course of a formal dispute resolution process; or ○ Was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or a related investigation. ● Organizations may collect personal information without the individual's knowledge or consent only: ○ If it is clearly in the individual's interest and consent is not available in a timely way; ○ If knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;	not inconsistent with the required elements and statements and are not otherwise contrary to the Authorization requirements of the Privacy Rule.	

	○ For journalistic, artistic or literary purposes; ○ If it is publicly available as specified in the regulations. ● Organizations may <u>use</u> personal information without the individual's knowledge or consent only: ○ If the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation; ○ For an emergency that threatens an individual's life, health or security; ○ For statistical or scholarly study or research (must notify Privacy Commissioner); ○ If it is publicly available as specified in the regulations;		

	○ If the use is clearly in the individual's interest and consent is not available in a timely way; or ○ If knowledge and consent would compromise the availability or accuracy of the information and collection was required to investigate a breach of an agreement or contravention of a federal or provincial law. ● Organizations may <u>disclose</u> personal information without the individual's knowledge or consent only: ○ To a lawyer representing the organization; ○ To collect a debt the individual owes to the organization; to comply with a subpoena, a warrant or an order made by a court or other body with		

	appropriate jurisdiction; o To FINTRAC as required by the *Proceeds of Crime and Terrorist Financing Act*; o To a government institution that has requested the information, identified its lawful authority to obtain the information, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; or is for the purpose of administering any federal/provincial law;		

	o To an investigative body named in the Regulations of the Act or government institution on the organization's initiative when the organization has reasonable grounds to believe that the information concerns a breach of an agreement, or a contravention of federal, provincial, or foreign law, or suspects the information relates to national security, the defence of Canada or the conduct of international affairs; o If made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal/provincial law; o In an emergency threatening an individual's life, health, or security (the organization must		

	inform the individual of the disclosure); o For statistical, scholarly study or research (must notify Privacy Commissioner); o To an archival institution; o 20 years after the individual's death or 100 years after the record was created o If it publicly available as specified in the regulations; or if required by law.		

7. References

Cloud Security Alliance. (2016, February). The Treacherous 12 – Cloud Computing Top Threats in 2016. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

Determann, Lothar and Oliver Zee. “Cloud Provider Obligations as Business Associates under HIPAA.” Computer and Internet Lawyer 30.6 (2013): 16-18.

Gleeson, N. & Walden, I. ‘It’s a jungle out there’?: Cloud computing, standards and the law. (2014). European Journal of Law and Technology, 5(2). Retrieved from http://ejlt.org/article/view/363/460

Hashizume, K., Rosado, D., Fernandez-Medina, E., & Fernandez, E. (2013, February 27). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5). Retrieved from https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5

Office of the Privacy Commissioner of Canada. (2010, March). Reaching for the Cloud(s): Privacy Issues related to Cloud Computing. Retrieved from https://www.priv.gc.ca/media/1723/cc_201003_e.pdf

Parker, Joshua S. “Lost in the Cloud: Protecting End-User Privacy in Federal Cloud Computing Contracts.” Public Contract Law Journal 41.2 (2012): 385-409.

Ryan, James. “The Uncertain Future: Privacy and Security in Cloud Computing.” Santa Clara Law Review 54 (2014): 497-525.

Szeto, Melodie and Ali Miri. “Analysis of the Use of Privacy-Enhancing Technologies to Achieve PIPEDA Compliance in a B2C e-Business Model.” Paper presented at the Eighth World Congress on the Management of eBusiness, WCMeB 2007, Toronto, Ontario, July 11-13, 2007.

Turner, Stephen. “Benefits and Risks of Cloud Computing.” Journal of Technology Research 4 (2013): 1-7.

Waggott, G., Reid, M., & Koczerginski, M. (2013, December). Cloud Computing: Privacy and Other Risks. Retrieved from http://www.mcmillan.ca/Files/166506_Cloud%20Computing.pdf

Wang, C. (2010, October 29). Q&A: Demystifying Cloud Security – An Empowered Report: Getting Past Cloud Security Fear Mongering. Retrieved from

http://resources.idgenterprise.com/original/AST-0036145_G2A_demystifying_cloud_security.pdf.

Wang, F. (2013). Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction. European Business Law Review, 24(5), 589-616.

Yang, Y. Tony and Kari Borg. “Regulatory Privacy Protection for Biomedical Cloud Computing.” Beijing Law Review 3 (2012): 145-151.