



faxing simplified. anytime. anywhere.



Faxing Dilemmas in an age of Privacy

Authors

This document was prepared by:

Jin Shin, General Counsel and Program Manager

Nymity Inc.

1 Yonge St., Suite 1801
Toronto, ON M5E 1W7
Tel.: 416.214.7838
Fax: 416.946.1178
Email: jin.shin@nymity.com

Terry McQuay, President

Nymity Inc.

1 Yonge St., Suite 1801
Toronto, ON M5E 1W7
Tel.: 416.214.7838
Fax: 416.946.1178
Email: terry.mcquay@nymity.com

This document is protected under the copyright laws of Canada and other countries. This document contains information that is proprietary and confidential to Nymity Inc. or its technical alliance partners. Any use or disclosure in whole or in part of this information without expressed written permission of Nymity Inc. is prohibited. © 2010 Nymity Inc. All rights reserved

Faxing Dilemmas in an Age of Privacy

Purpose

The purpose of this paper is to discuss the privacy implications of transmitting personal information via the facsimile given the legislative requirements to protect the same. As such, this paper will provide a comprehensive analysis of the issues respecting fax transmissions that may lead to privacy breaches, Canadian legislative requirements to protect personal information, examples of privacy breaches related to faxing and best practice recommendations for faxing.

Overview

In order to achieve the above purpose, this paper will address the following questions:

1. How can privacy breaches occur when faxing personal information?
2. What are some examples of recent privacy breaches involving faxing personal information?
3. Are organizations required by law to safeguard personal information when faxing the same?
4. What are the consequences of a privacy breach?
5. What are the immediate steps organizations can take to reduce the threat of privacy breaches?
6. Are there alternative methods of faxing that are less likely to result in privacy breaches?

Table of Contents

Purpose	2
Overview	2
Table of Contents	3
Introduction / Executive Summary	4
The Pitfalls of the Traditional Method of Faxing	5
Privacy Legislation	6
Privacy Commissioners’ Role	6
PIPEDA Complaint Investigation Cases	6
PIPEDA Case #226	
The Commissioners’ Investigative Report RE: Dynacare & Viewpoint	7
Alternatives to the Traditional Method of Faxing	7
a. Password Enabled Fax Machines	
b. Fax Server Technology	
c. IP Fax / Internet Fax	
d. Fax Dialing Servers	
Call to Action – GMAC Case for IP Faxing	9
Conclusion	10
Sources	11
Appendix “A”	12
Appendix “B”	13

Introduction / Executive Summary

As Canadian society moves further towards an information based economy, compliance with legislation that protect individuals' personal information is of growing concern for all organizations. In this regard, modern day office machines, in particular fax machines, have allowed businesses to transmit and receive personal information instantly. The implications of sending and receiving personal information via fax machine within the context of privacy will be addressed herein.

As a matter of practical exercise, this paper will analyze the privacy issues surrounding the use of fax machines to transmit personal information that may lead to a privacy breach. These privacy issues will be illustrated by way of examples wherein the use of fax machines has lead to privacy breaches. In particular, the privacy breaches relating to the use of fax machines that have recently made the news headlines will be highlighted in this paper.

Further, this paper will identify and analyze the Canadian legislative requirements of the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), Alberta's *Personal information Protection Act* ("AB PIPA"), British Columbia's *Personal Information Protection Act* ("BC PIPA"), and Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* ("PQ PPIPS") (hereinafter collectively "Privacy Legislation") for the "safeguarding" of personal information as it relates to the issues associated with using fax machines. This analysis shall be accompanied by an overview of the Privacy Commissioners' functions, PIPEDA privacy complaint cases and best practice recommendations for mitigating the chances of privacy breaches while using the fax machine.

Lastly, this paper shall discuss the alternatives to the traditional method of faxing, such as internet faxing offered by Protus IP Solutions which may significantly improve the safeguards for personal information required by Privacy Legislation. In this respect, this paper will look at how Protus IP Solutions was able to resolve the safeguarding issues for General Motors Acceptance Corporation surrounding the faxing of personal information. Organizations must examine privacy safeguards in accordance with the sensitivity of the information when faxing. Privacy concerns and legislation require safeguards that are appropriate to the sensitivity of the personal information.

Pitfalls of the Traditional Method of Faxing

Increased use of fax machines by organizations has transformed the fax machine into an essential tool. Fax machines provide organizations with the ability to send and receive documents relatively instantly. Given that a faxed document is a true representation of the original, it can be considered a reproduction or even qualify as an original document. That said, notwithstanding the value and convenience of the fax machine, there remains some privacy safeguarding issues that need to be addressed.

"In my view, not only faxes were misdirected. The bank's trust was also misdirected."

"In our privacy-conscious age, businesses must protect their customers' sensitive files. They should treat it as a sacred duty."

Excerpts from the Toronto Star (December 2, 2004) article, "Trust Misdirected at CIBC." by Ellen Roseman

Lessons learned from the news headlines and privacy complaint investigation findings associated with faxing has shown that not restricting access to the fax machine and misdialing the fax numbers are the most common mistakes that lead to privacy breaches. That said, it should be noted that regardless of the cause, unintended disclosure of personal information from a privacy perspective is a privacy breach, whether that information is personal information of customers or employees. Therefore, unintended disclosure occurs when personal information is disclosed without the consent of the individual of which the information is about.

Privacy breaches may occur due to the physical location of the fax machine itself. Privacy breaches of this nature are most often the result of personal information being received on unrestricted fax machines that are placed in open areas where people passing by may view the contents of the faxes received or inadvertently pick up a fax that was not intended for them.

"A second businessman says the Canadian Imperial Bank of Commerce (CIBC) has been faxing him confidential customer information for several years - the second such privacy breach revealed in less than two weeks, the Montreal Gazette reported on Wednesday, according to the Canadian Press."

"Local businessman Stephen Oakes told the Gazette the CIBC has been sending private information about its customers to his toll-free number for four years, CP reported."

"The Office of the Privacy Commissioner of Canada is investigating the West Virginia case to determine whether the bank violated privacy laws. An official at the privacy office told the Gazette on Tuesday the CIBC has contacted them again to confirm a new breach, CP reported."

Excerpts from Toronto Star (December 8, 2004) article "Report: 2nd Man Received Confidential CIBC Data," by the Canadian Press

For the reasons noted in the preceding paragraph, access to fax machines that transmit and receive personal information should be restricted to only those employees that have been authorized.

Misdialing a fax number is a common cause of privacy breaches. Recent stories in the news and cited herein demonstrates the importance of ensuring that fax numbers are correctly dialed. Therefore, faxing safeguards should incorporate measures that minimize the likelihood of misdialing fax numbers.

The implication of inadequately safeguarding personal information has the potential for serious repercussions to organizations. A privacy breach may result in an organization suffering damage to its reputation and being subject to a privacy complaint investigation, in addition to legal sanctions by the privacy commissioner and/or by the individual that the personal information relates to. Thus, it is imperative for organizations to implement Privacy Legislation compliant faxing solutions.

"Five of Canada's six biggest banks have now been cited for mistakenly faxing private customer information to unknown third parties, amid allegations they failed to take steps to remedy the situation."

Excerpts from London Free Press (December 15, 2004) article "Fax errors plague banks," by the Canadian Press

Privacy Legislation

Implementation of privacy safeguards for fax machines when receiving and transmitting personal information is not only good business, it is now the law. As of January 1, 2004, all private sector organizations engaged in commercial activities became subject to PIPEDA. However, provincial organizations in Alberta, British Columbia and Quebec may be subject to the respective provincial private sector privacy legislation. The primary subject of Privacy Legislation is “personal information.” Personal information is information that is about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Privacy Legislation contains provisions that require the subject organizations to safeguard personal information in their possession. Privacy Legislation is based on ten principles that govern the collection, use and disclosure of personal information. In the foregoing respect, disclosure without the consent of the individual for which the information is about constitutes a privacy breach. Privacy Legislation contains provisions to safeguard personal information against such disclosures. As such, for purposes of discussion herein, the principle of “Safeguards” will be discussed.

Within the context of privacy, the principle of “Safeguards” requires organizations to protect personal information regardless of the format, with safeguards appropriate to the sensitivity of the information. Most commonly, sensitive information includes financial and health information. However, some information may only be sensitive within a particular context. Measures to safeguard information may include physical measures, organizational measures, technological measures, and employee training measures.

For the complete text of the “safeguarding” provisions as contained in Privacy legislation, please see Appendix “A”

Privacy Commissioners’ Roles

The Privacy Commissioners’ responsibilities are to ensure that organizations collect, use and disclose personal information in a manner that is responsible and transparent. Privacy Legislation governing personal information provides the Privacy Commissioners with the authority to ensure organizations within their respective jurisdiction are held accountable for their information handling practices.

The Privacy Commissioners are impartial and nonpartisan, which means that they can act independently to investigate complaints from individuals. This mandate extends to both the public sector and the private sector.

PIPEDA Complaint Investigation Cases

The following PIPEDA complaint investigation case demonstrates the importance of implementing appropriate fax safeguards. In addition, this case provides insight into fax safeguarding considerations.

PIPEDA Case #226: Company’s collection of medical information unnecessary; safeguards are inappropriate

In this case, a former employee of a telecommunications company complained that the company it did not have appropriate safeguards in place to protect sensitive personal medical information from unauthorized access. This complaint was determined to be well-founded on the grounds that the fax machine used to receive sensitive medical information was accessible, in an unlocked room and that it was inappropriate to have medically untrained human resources personnel to collect medical diagnoses about employees.

For additional information on PIPEDA Case #226, please see Appendix “B”

The Commissioners' Investigative Report RE: Dynacare & Viewpoint

Further to a story published in the *Edmonton Journal* in July of 2004, wherein managers of an apartment building received facsimile transmissions containing personal medical information from Dynacare and Viewpoint, companies servicing the health industry, the Commissioners, for the first time, commenced a joint investigation into this matter.

In both cases, the joint investigation was unable to determine who within Dynacare and Viewpoint was responsible for erroneously transmitting sensitive medical personal information to the wrong fax number. Nonetheless, both Dynacare and Viewpoint were found to have contravened PIPEDA, as each company had disclosed personal information without consent.

As a result of the investigation findings, both companies implemented corrective measures to mitigate the likelihood of future privacy breaches of this nature.

Assistant Commissioner's recommendations to Dynacare and Viewpoint companies:

- Implement and follow the Office of the Privacy Commissioner's prescribed best practice for faxing personal information.
- Implement measures to notify individuals whose personal information has been inadvertently disclosed via misdirected facsimiles.
- Review and update employee confidentiality/privacy agreements on a yearly basis.

Alternative Solutions to the Traditional Method of Faxing

Further to the best practice recommendations prescribed by the Office of the Privacy Commissioner of Canada, the following solutions may be more appropriate for organizations that require a higher degree of privacy safeguards than that available with the traditional method of faxing.

a. Password Enabled Fax Machines

A password enabled fax machine ("PEFM") is able to restrict access until the appropriate password is entered. To transmit a fax, the sender is required to input a password before being able to dial a fax number. To receive a fax transmission, the PEFM stores the received faxes onto its internal memory until the appropriate password is entered.

Notwithstanding the password feature, the PEFM is essentially no different than a traditional fax machine, as it also utilizes the regular phone lines (often referred to as public switched telephone network or "PSTN") for transmissions. Therefore, like that of the traditional fax machine, PEFM transmissions are easily monitored and tapped. Moreover, the PETM lacks features that would mitigate the likelihood of misdialing the fax number.

b. Fax Server

A fax server allows users connected to a network to send and receive faxes from their desktop. Outbound faxes are sent from the desktop to the fax server and then from the fax server over a modem/telephone line connection to the intended fax recipient. Therefore, similar to a traditional fax machine and PEFM, fax server transmissions are also easily monitored and tapped. Moreover, the fax server also lacks features that would mitigate the likelihood of misdialing the fax number.

"IP Fax systems from Protus IP have provided Nymity with appropriate safeguards for our faxed based ordering system. Our customers include credit card information on fax order forms with the knowledge and assurance that their personal information is forwarded to our order processing department in a safeguarded manner."

Terry McQuay, President of Nymity Inc.

c. IP Fax System / Internet Fax

Internet Protocol ("IP") fax systems, also known as "internet faxing" is growing in popularity over that of the traditional faxing method. IP fax systems involve transmitting and receiving faxes over the internet or private intranets via email for at least part of its journey. In addition, IP fax systems are integrated into an organizations' computer infrastructure as it utilizes the same network.

IP fax systems may help achieve greater levels of privacy safeguards, thereby mitigating the likelihood of privacy breaches and ensuring Privacy Legislation compliance. In this respect, companies such as Protus IP Solutions, a leader in providing secure internetbased faxing solutions, provides organizations with a secure alternative to the traditional method of faxing.

Internet based faxing services allow organizations to send and receive faxes using existing email accounts and the internet. Such IP faxing methods are inherently more secure than traditional faxing methods. The following are additional privacy safeguarding benefits of IP fax systems:

- Given the integrated nature of IP fax systems, unauthorized access to faxes are virtually eliminated because the faxes do not just sit in an open tray to be pickup by the recipient. Instead, faxes are stored on the organization's protected network server or the recipient's password protected email inbox.
- Additionally, the integrated nature of IP faxing may reduce the potential for human error when dialing frequently used fax numbers. Fax machine numbers contained in contact programs, such as Microsoft Outlook reduces the potential for misdialing frequently use fax numbers.
- This level of integration also provides the fax sender with a real-time fax receipt confirmation via email, further reducing the potential of sending faxes to the wrong recipient.

IP fax systems are inherently more secure than other forms of faxing, including the traditional method of faxing. Such systems are better able to meet the "best practice recommendations" for faxing personal information as prescribed by the Office of the Privacy Commissioner of Canada. In the foregoing regard, the integrated nature of IP fax systems with that of computer networks allow strict access controls because faxes are for the most part sent and received via the computer that would be password protected by the user. Moreover, systems integration allows IP fax systems to take advantage of computer based "contact" information software, such as Microsoft Outlook. This level of integration not only ensures an additional level of password protection, but it also ensures that frequently dialed fax numbers are not misdialled as the user would simply select the fax number from the contact information already in the computer. IP fax systems, such as that offered by Protus IP Solutions' MyFax provide a real-time confirmation via email when the fax is received by the recipient. This confirming email feature of IP fax systems provides an additional layer of privacy safeguard by reducing the chances that a fax transmission sent to a wrong party would go unnoticed.

Notwithstanding that no system is 100% secure and given the foregoing, IP faxing provides a greater degree of privacy safeguards over that of traditional faxing, password enabled fax machines and fax servers. Therefore, where appropriate, the implementation of an IP fax system will provide the greatest degree of faxing safeguards available today.

d. Fax Dialing Servers

As stated in the foregoing, IP fax systems provide the greatest degree of faxing safeguards for most businesses; however, for organizations such as banks, where signature images need to be captured for verification purposes and/or require forms that are not electronically available to be faxed, IP fax systems may not be appropriate. For these types of organizations, fax dialing servers may provide an alternative to IP faxing.

Fax dialing servers provide an additional level of faxing safeguards over that of the traditional faxing method by placing programmable dialing restrictions on fax numbers. This technology ensures faxes are only sent to numbers on an "approved" fax number list. Organizations that employ this technology must establish and maintain a fax number database programmed into the fax dialing server. Therefore, fax numbers dialed on fax machines connected to a network that utilizes a fax dialing server will be matched against the approved list, and if the fax number does not match, the fax transmission will fail. The fax dialing server may be programmed to dial fax numbers that are not on the "approved" list only upon inputting the proper authorization access code prior to transmitting the fax.

Unlike IP fax systems, fax dialing servers primarily restrict the fax numbers dialed to only those in the “approved” fax number database. Organizations that choose to implement fax dialing servers must also consider and implement other safeguarding measures that fax dialing servers do not address. Therefore, organizations that implement fax dialing servers should also implement the following additional safeguarding measures:

- Advise and prepare the intended fax recipient to receive the fax transmission.
- Ensure fax cover sheets are always used when transmitting faxes.
- Program the fax dialing server to only transmit faxes upon the fax number being correctly dialed twice. The effect of this redundancy is to further reduce the chances of misdialing fax numbers that are not in the “approved” fax number database.
- Further to transmitting the fax, confirm with the intended recipient that the fax was actually received.

GMAC Case for IP Faxing

GMAC Residential Funding of Canada, Limited (“GMAC-RFOC”) receives 12,000 to 15,000 pages of faxed documents monthly relating to real property mortgage financing. Prior to GMAC-RFOC’s rapid business growth in this area, all faxes received were managed by one staff position and then distributed accordingly. However, as GMACRFOC’s business continued to grow, so did the number of faxes it received. As such, in late 2003, GMAC-RFOC recognized the need to improve the administration of faxed documents that are received.

At the time of consideration, GMAC-RFOC realized that an appropriate fax solution is one that not only meets the safeguarding requirements of Privacy Legislation, such as PIPEDA, but one that is also able to manage the sheer volume of faxed documents in a cost effective and efficient manner. The primary faxing solutions that were considered by GMAC-RFOC was the fax server system and the IP fax system. After careful consideration of the legislative requirements and business objectives, GMAC-RFOC chose to implement the IP fax system. GMAC-RFOC determined that the IP fax system provides the greatest degree of faxing safeguards that are appropriate for the sensitivity of the information being faxed. Such sensitive information may include, but are not limited to, letters of employment, mortgage applications and voided cheques. The inherent cost savings of the IP fax solution was also a feature that did not go unnoticed. Implementation and administration costs would be minimal, and given that the IP fax system virtually eliminates the need for fax machines, GMAC-RFOC was also able to save the costs associated with fax machines.

In consideration of the foregoing, GMAC-RFOC chose to implement an IP fax system offered by Protus IP Solutions branded as MyFax. The benefits presented by MyFax to GMAC-RFOC are significant. MyFax is inherently more secure than other faxing alternatives. Given the sheer volume of sensitive information faxed to GMAC-RFOC, MyFax’s safeguarding features have allowed GMAC-RFOC to easily safeguard its faxed documents. GMACRFOC is now able to administer faxing in the same manner it administers network ID’s, as faxes can now be sent and received via email over the internet directly to the recipient’s password protected computer. This level of control drastically reduces the likelihood of sensitive information being inadvertently disclosed, lost or destroyed as received faxes no longer sit in a tray until they are picked up by the intended recipient. Instead, all received faxes sit in the recipient’s email inbox, following them wherever they go. Since the adoption of MyFax, a mortgage broker is now able to send a fax to a GMAC-RFOC mortgage underwriter directly, as faxes are received into the specific underwriter’s email inbox. Within the context of privacy safeguards, this is the most important feature of MyFax. This feature prevents unauthorized disclosure of personal information by eliminating excess handling of the same. For GMAC-RFOC, MyFax has enabled it to meet the legislative requirements of safeguarding personal information that is appropriate for the level of information sensitivity.

RE: Protus IP Solution’s MyFax

“A great fax solution... so elegant, so simple. The power is in its simplicity.”

Cameron Beheshti, Senior Counsel, Canada of GMAC Residential Funding of Canada, Limited

“Administration of the MyFax system is very easy... it was up and running in under 24 hours.”

Xavier Zinn, Chief Privacy Officer and Systems Engineer of GMAC Residential Funding of Canada, Limited

MyFax enables users to fax through email. This feature allows the user to “dial” frequently used fax numbers from their desktop computers’ integrated contact software, such as Microsoft Outlook, thereby reducing the possibility of misdialing fax numbers. Notwithstanding the foregoing, if a faxed document is inadvertently sent to a wrong party, the sender will be notified as MyFax automatically emails the sender a confirmation of where the fax document was sent. This feature allows the sender to take corrective action to resolve an inadvertent disclosure, thereby providing the sender with an opportunity to mitigate the potential for damages in a timely manner. In addition to the faxing safeguards of MyFax as stated above, MyFax was easy to implement at GMAC-RFOC, as it did not require any additional hardware and setup time was less than 24 hours. MyFax has proven to be cost effective to GMAC-RFOC as it allows for the reduction in the costs of maintaining fax machines and the manual administration of faxed documents (i.e. paper, ink toners, repair costs and labour cost associated with manual distribution). The administration of MyFax at GMAC-RFOC is now simply and securely handled by the IT department. In this case, GMAC-RFOC’s Systems Engineer is also its Chief Privacy Officer.

Conclusion

Fax machines have made it easy for organizations to transmit and receive information almost instantly. Even though the traditional method of faxing has served organizations well over the years, information safeguards associated with faxing must be examined by all organizations. Addressing the safeguarding issues surrounding faxing is not only good business, it is now a legislative requirement. As consumers and organizations realize the importance of privacy, all organizations must assess and review their fax handling policies and procedures to ensure legislative compliance. Compliance in the foregoing regard requires all organizations to implement adequate infrastructure to prevent privacy breaches.

Many organizations update their business machines every few years, but traditional fax machines are often overlooked. Until now, there have not been many reasons to replace traditional fax machines used by most organizations. For many organizations, adoption of new fax technologies is not an option, but a necessity as today’s fax technology is driven by legislative and business requirements. Alternative fax technologies, such as MyFax by Protus IP Solutions offers organizations a true alternative to the traditional method of faxing by helping organizations to mitigate the potential liabilities associated with privacy breaches and by meeting organizations’ business objectives to reduce operational costs.

Sources

1. Nymity's PIPEDA Reference Guide at:
<http://www.nymity.com/pipeda/pipeda.asp>
2. Nymity's AB PIPA Reference Guide at:
http://www.nymity.com/ab_pipa/ab_pipa_reference.asp
3. Nymity's AB PIPA Reference Guide at:
http://www.nymity.com/bc_pipa/bc_pipa_reference.asp
4. Nymity's PQ PPIPS Reference Guide at:
http://www.nymity.com/pq_ppips/ppips_reference.asp
5. Nymity's Frequently Asked Questions at:
http://www.nymity.com/faq/question_index.asp
6. The Office of the Privacy Commissioner of Canada website RE: PIPEDA Case #226 at:
http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031031_e.asp
7. The Office of the Privacy Commissioner of Canada website RE: Faxing Personal Information at: **http://www.privcom.gc.ca/fs-fi/02_05_d_04_e.asp**
8. The Office of the Privacy Commissioner of Canada website RE: Misdirected faxes containing health information end up in apartment managers' hands at:
http://www.privcom.gc.ca/media/nr-c/2004/ab_041221_e.asp
9. The Office of the Information and Privacy Commissioner of Alberta website RE: Investigation Report H2004-IR-001 at:
<http://www.oipc.ab.ca/ims/client/upload/H2004-IR-001.pdf>
10. P. Platt, L. Hendlisz, and D. Intrator. Privacy Law in the Private Sector – An Annotation of the legislation in Canada, Canada Law Book inc. 2004.
11. Protus IP Solutions website at: **<http://www.protus.com/index.asp?pg=1>**
12. Bouchard, Thaddeus. "IP Fax Moves into the Mainstream." CTI Magazine March 1999. Jan 12, 2005
<http://www.tmcnet.com/articles/ctimag/0399/0399omttool.htm>
13. McQuay, Terry. **Interview with Ron Lalonde, Chief Privacy Officer for CIBC. Feb. 2005.**
14. McQuay, Terry and Shin, Jin. Interview with Cameron Beheshti, Senior Counsel for GMAC Residential Funding of Canada, Limited. Notes taken on Jan. 21, 2005
15. McQuay, Terry and Shin, Jin. Interview with Xavier Zinn, Systems Engineer and Chief Privacy Officer for GMAC Residential Funding of Canada, Limited. Notes taken on Jan. 21, 2005

Appendix "A"

"Safeguards"

Clause 4.7, Principle 7 of PIPEDA states:

4.7

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

- a. physical measures, for example, locked filing cabinets and restricted access to offices;
- b. organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
- c. technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Section 34 of AB PIPA states:

An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Section 34 of BC PIPA states:

An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

Section 10 of PQ PPIPS states:

Every person carrying on an enterprise who collects, holds, uses or communicates personal information about other persons must establish and apply such safety measures as are appropriate to ensure the confidentiality of the information.

Appendix “B”

PIPEDA Case #226: Company’s collection of medical information unnecessary; safeguards are inappropriate

FACTS:

- A former employee of a telecommunications company complained that the company it did not have appropriate safeguards in place to protect sensitive personal medical information from unauthorized access.
- The complainant objected to the fact that the employer instructs its employees to send medical reports by facsimile to its human resources office – a form of transmission that does not afford an adequate degree of privacy for personal medical information, particularly for reports that contain medical diagnoses.
- In addition, the complainant was worried that employees who do not have a legitimate need to handle this information, such as human resources staff, might view it.

FINDINGS:

- The Assistant Commissioner determined this Complaint to be well-founded on the following grounds:
- Given that medical information is very sensitive personal information, the safeguards in place were not appropriate.
- The fax machines used to receive sensitive personal medical information was kept in accessible, unlocked room.
- It was not appropriate for the company to make a practice of receiving employee medical reports by fax, whether at the local human resources office or at the head office.
- The Assistant Privacy Commissioner questioned the company’s practice of having human resources people receive and process medical reports containing diagnostic medical information about individual employees.
- The Assistant Privacy Commissioner stressed that the Office is strongly of the view that any organization that collects medical diagnoses about employees for any purpose must only do so with strict safeguards in place.
- In this case, it was determined that it was mainly medically unqualified human resources personnel, both in local offices and at corporate headquarters, who receive, note, interpret and process, for the purpose of administering the company’s disability plans, highly sensitive medical diagnoses.

RELEVANCE:

- Medical information is considered to be very sensitive information. As such, strict safeguards must be in place when faxing personal medical information.

Further Considerations from PIPEDA Case #226

The Assistant Privacy Commissioner made the following recommendations:

- The company should revise its policy and procedures for collecting and handling employee medical reports, with particular emphasis on the purposes and practices regarding diagnostic information.
- Take appropriate steps to ensure that employees obliged to submit a medical report are explicitly informed that they have a right to ensure that diagnostic information be kept in strict confidentiality, that they have the option of sending the form in strictest confidence directly to medical staff in health services and that the alternative means that human resources staff will receive this information;
- Ensure that managers, if presented with a medical report, refuse to accept it and instruct the employee to send it as recommended in (a); and
- Ensure that the corporate human resources unit no longer receives diagnostic information about individual employees.
- The company should revise its letters of notification to employees on short-term disability so as to clarify that employees have the option of sending long-term disability information directly to the insurance company.

About MyFax

MyFax is the fastest growing Internet fax service used by individuals, small, medium, and large businesses to send and receive faxes using existing email accounts or the web. MyFax offers services in North America and Europe, including the United Kingdom, to industries recognized among the fastest growing adopters of internet fax including finance, insurance, real estate, healthcare, transportation and government. More than 15,000 new customers subscribe to MyFax each month. Additional information is available at www.myfax.com and www.myfax.uk.com.

Toll-free: 1-866-657-9885 | 613 733-0000 | Email: sales@myfax.com

© 2010 Protus®. All rights reserved. Protus®, MyFax® are trademarks of Protus®. Other trademarks referenced in this document are the property of their respective owners. Customers are solely responsible for ensuring regulatory compliance.