Manulife Financial

For your future™

Protection of Privacy and Confidentiality (Canada, other Asia, and Support)

Self-Learning Module

Manulife Business Processing Services

Source: https://manulife.csod.com, July 2011

Privacy Overview

Source: http://www.traderbytes.com/support/privacy.php

Privacy Incidents

Protecting personal information is important for many reasons, including complying with laws and our organization's policies. But the most important reason is that good practices provide benefits—and negligence can hurt. Trust, loyalty, and brand value all depend on doing the right thing. Even simple mistakes can drastically harm people and companies.

Source: http://www.mommyposh.com/privacy-policy/

Privacy Incident

Here are examples of people affected by both good and not-so-good privacy practices:

Example 1

- **Managing an Incident**
  - "I'm a regional HR manager. A couple of weeks ago, I left my company laptop in my car while I was eating lunch, and it was stolen! The laptop contained personal information for several thousand employees in my region.

    Now, my organization is struggling to prevent any further damage to this whose information may be compromised. My coworkers are worried about whether their information may be compromised. I'm concerned about all of the customers whose information has been breached. And I'm worried about losing my job!"

Source: Compass

Privacy Incident

Example 2

- **Providing Choice**
  - "For me to fully engage with a company, I need to be given a choice about how that company will use my personal information. When I choose not to have them share my information with other companies or use it for other purposes, I need to believe that they'll respect that choice.

    When I receive unsolicited offers against my wisher, I find it annoying and disrespectful. For me, this is more than customer service--this is online trust."

Source: Compass

Privacy Incident

Example 3

- **Maintaining Growth**
  - "As an organization, we have focused on treating personal information with extra care and doing whatever is necessary to ensure it remains protected.

    Of course, we offer great products and services, but I think our commitment to privacy has also increased trust, enabled global business growth, and helped build respect with both our customers and employees."

Source: Compass

Privacy Incident

Example 4

- **Securing Personal Information**
  - "I found out the hard way that identity theft really does happen. I recently applied for a car loan and was denied due to 'a poor credit score'. It turns out my personal information was leaked and an identity thief ruined my credit score.

    It hasn't been a quick fix to repair this; I'm still working with credit companies to clear my name."

Source: Compass

Introduction

Privacy incidents are rarely caused by malicious acts or someone attempting to sabotage our organization. More often than not, they stem from simple inattention to detail that leads to personal information being exposed—and loss of consumer and employee trust.

With the rapid increase in online activity and information accessibility, customers and employees have become more concerned about how their personal information will be stored and used. Additionally, regulators are increasingly proactive in holding companies liable when they violate customers' and employees' trust.

Source: Compass

Introduction

Here are some examples of privacy incidents that you can easily avoid by paying attention to detail:

- A laptop or briefcase stolen because it was left in the back seat of a car.
- A package containing personal information redirected due to an incorrect address.
- An e-mail with personal information sent to the wrong e-mail address, or a fax sent to the wrong fax number.
- A document with personal information falls into the wrong hands because it wasn't discarded in a secure shredder bin.

Defining Privacy

- First, let's take a moment to define what we mean by privacy in the commercial world. **Privacy** is an individual's expectation that organizations will use their personal information in limited ways and protect it from disclosure to unauthorized parties. This includes protecting personal information including identifiers like account numbers, names, addresses, and Social Insurance Numbers, as well as other personal information gained through transactions or a corporate employment context.
- Privacy goes hand-in-hand with confidentiality; the protection of proprietary business information such as strategic plans, financial data, and other internal information critical to business operations.
- As an organization, we have a professional and legal commitment to employees, shareholders, and customers to respect and protect both personal and proprietary information.

Source: Compass

Importance of Privacy

- A key to our business is building and maintaining our customers' trust, reducing risk, and simply doing what is right.
- Simple mistakes—such as misplacing a document, losing a laptop, or accidentally leaking an e-mail—can result in privacy incidents that can have devastating and long-lasting effects on our organization, our customers, and, as a result, on you.

Importance of Privacy

- Here are a few examples of such privacy incidents and their associated consequences to our organization.
  - **Sample 1**

    Privacy Incident

    — Employee takes home outgoing mail, which contains disks with employee and customer information, and loses them.

    Consequences

    — Could require notification of the incident to impacted customers as well as to governmental agencies. Customers could move business to a more trusted company.

Source: Compass

Importance of Privacy

- **Sample 2**

  Privacy Incident

  - Personnel files are lost, misplaced, or mistakenly made available on an external Web site.

  Consequences

  - May require notification of a data breach to government agencies and each individual affected. This is both expensive and time-consuming and could require extensive privacy investigations, disciplinary actions, as well as negatively impact employee morale.

Source: Compass

- **Sample 3**

  Privacy Incident

  - Proprietary business initiatives are leaked.

  Consequences

  - Proprietary knowledge lost to a competitor, reduced revenues, and/or profits.

Source: Compass

Importance of Privacy

- **Sample 4**

  Privacy Incident

  - Customer or employee data is misused and shared with partners without the customer's or employee's knowledge and/or consent.

  Consequences

  - Loss of customer confidence, damage to the company's reputation, potential legal action and substantial legal fines.

Source: Compass

- **Sample 5**

  Privacy Incident

  - Media reports that an organization's improper document disposal exposes sensitive personal information

  Consequences

  - Public embarrassment, loss of brand value, and loss of customer and employee trust.

Source: Compass

Private Information

So, what information needs to be protected? Any information used to identify, contact, or locate an individual is **Personally Identifiable Information (PII)** and must be kept private. It only takes a few pieces of personal information, like name, address, date of birth, and Social Insurance Number, to put a person at risk for identity theft.

It's critical that you are aware of the policies and procedures to protect any information under your control, as well as what could happen if this information were leaked.

A good rule of thumb is to treat all personal information as if it were your own. Apply the same protection you would expect others to apply to your PII. Take a moment to review **examples of PII** and **Non-PII**.

Private Information

PII

- Every day our customers, advisors and our employees share their **Personally Identifiable Information** (PII) with Manulife Financial. In return, they expect us to keep that information confidential and to keep it safe. Our responsibility to safeguard all personal information in our possession or control is not only what Canadian privacy laws require: it's also the right thing to do, and it embodies Manulife's PRIDE values.
- Given the volume and range of personal information Manulife collects and uses on a daily basis, this is a significant commitment. But it's a commitment that is integral to our business at Manulife and one that our customers, employees, and agents rely on when they entrust Manulife with their personal information.
- In Canada, personal information is **any factual or subjective information, recorded or not, about an identifiable individual**.

Private Information

PII – Examples:

- Name
- Home address
- Account, policy or credit card number
- E-mail address
- Age
- Date of birth
- Place of birth
- Driver's licence number
- Social Insurance Number
- Occupation and income
- Ethnic origin
- Physical characteristics such as height, weight, and blood type
- Genetic information
- Fingerprints
- Opinions, evaluations, and comments
- Social status
- Occupation
- Employer
- Credit history
- Medical status or history
- Criminal convictions
- Existence of a dispute between a consumer and a commercial organization
- Intentions to acquire goods or services, change jobs, travel plans, etc

Private Information

NON-PII

- If information cannot be used to uniquely identify a single person then it is not PII. It is often the act of combining different pieces of personal information that causes it to become PII. Information can still be private, in the sense that the person may not wish for it to become publicly known, without it being personally identifiable. So for example, a person's place of employment by itself is not PII however, if you combine it with the person's name, address and date of birth, then this information is PII.
- **Examples:**
  - a report showing how many Manulife Financial customers live in each province
  - the age groupings and average policy values for those customers
  - An employee's name, title, business address or telephone number

Handling Personal Information

Our organization's business practices involve handling personal and proprietary information. Every day we collect, store, use, share, manage, and destroy information. We are responsible for respecting and protecting this information.

Think about an instance when you provided personal information to a company. Just as you would expect to have a say in how your information is used, we also must provide our customers and employees with the same choice and honor their privacy decisions.

We are committed to following global privacy principles to ensure information privacy and security. Our privacy promises, as well as laws and regulations, create legal obligations we must meet.

Handling Personal Information – Basic Privacy Principles

Notice

- We provide clear explanations to our customers and employees of the personal information we collect, how we use it, with whom we share it, and how we safeguard it.

  Disclosing our information practices supports our commitment to transparency, providing our customers and employees a basis for their informed consent.

Source: Compass

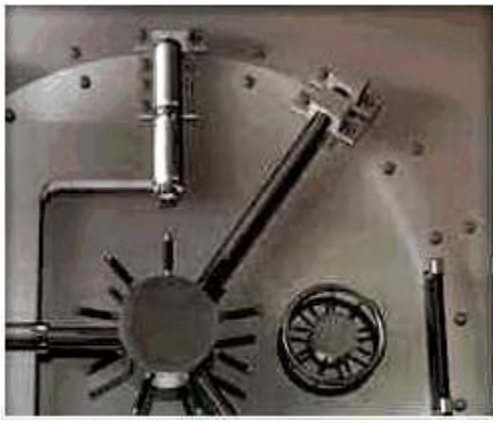
Access

- People have a legal right to request access to their personal information. Organizations have a legal obligation to respond to these requests within defined time frames. We offer secure personal information and to correct or amend it.

Source: Compass

Handling Personal Information – Basic Privacy Principles

- **Security**
  - We take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.



Source: Compass

- **Data Integrity**
  - We take steps to ensure that personal information is accurate and kept up-to-date, and to rectify inaccurate data.

Source: Compass

Ten Privacy Principles

Manulife Financial abides by **Ten Privacy Principles**. These principles are based on the federal government's privacy legislation, the *Personal Information Protection and Electronic Documents Act*.

1. **Accountability:** We are responsible for personal information under our control. We have designated individuals who are responsible for monitoring our ongoing compliance with the Privacy Principles.

2. **Identifying purposes:** The purposes, for which personal information is collected, will be identified by us, or through our, or your, authorized representatives.

3. **Consent:** Your consent is required for the collection, use and disclosure of personal information, subject to certain exceptions. Such exceptions are set out in the law and include where legal, medical or security reasons make it impossible, or impractical, to seek consent. Your consent may be expressed in writing. It may also be given verbally, electronically, or through our, or your, authorized representatives. In certain circumstances, it may also be implied.

4. **Limiting collection:** The collection of your personal information must be by fair and lawful means, and be limited to that which is necessary for the purposes identified.

Ten Privacy Principles

5. **Limiting use, disclosure and retention:** Your personal information may only be used or disclosed for the purposes for which it was collected, other purposes you consent to, or as required or permitted by law. It may only be kept for as long as is necessary to satisfy the purposes for which it was collected, or as required or permitted by law.

6. **Accuracy:** Any personal information that is collected, used or disclosed should be as accurate, complete and as up-to-date as is necessary for the purpose for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards that are appropriate to the sensitivity of the information, in order to protect your personal information from unwarranted intrusion, release or misuse.

8. **Openness:** Information about our privacy policies and practices for managing your personal information shall be made available to you.

9. **Individual access:** Upon written request, you will be informed of the existence, use and disclosure of your personal information and you will be given access to it, subject to certain exceptions, as permitted by law. You may also verify the accuracy and completeness of your information, and request that it be amended, if appropriate.

10. **Inquiries and concerns:** You may contact us if you have any inquiries or concerns about our privacy policies and practices.

Privacy Responsibilities

Now that you are familiar with our organization's privacy commitments, take a moment to learn about your role in upholding these responsibilities.

- **Privacy Awareness**
  - **Q:** "I don't handle personal information. Why do I need to know about privacy?"
  - **A:** In an information-driven business like ours, we are all surrounded by personal and business information, even if your job doesn't have specific data handling requirements. When you collaborate with colleagues on a task or use our network resources, you are exposed to private information that need to be protected.

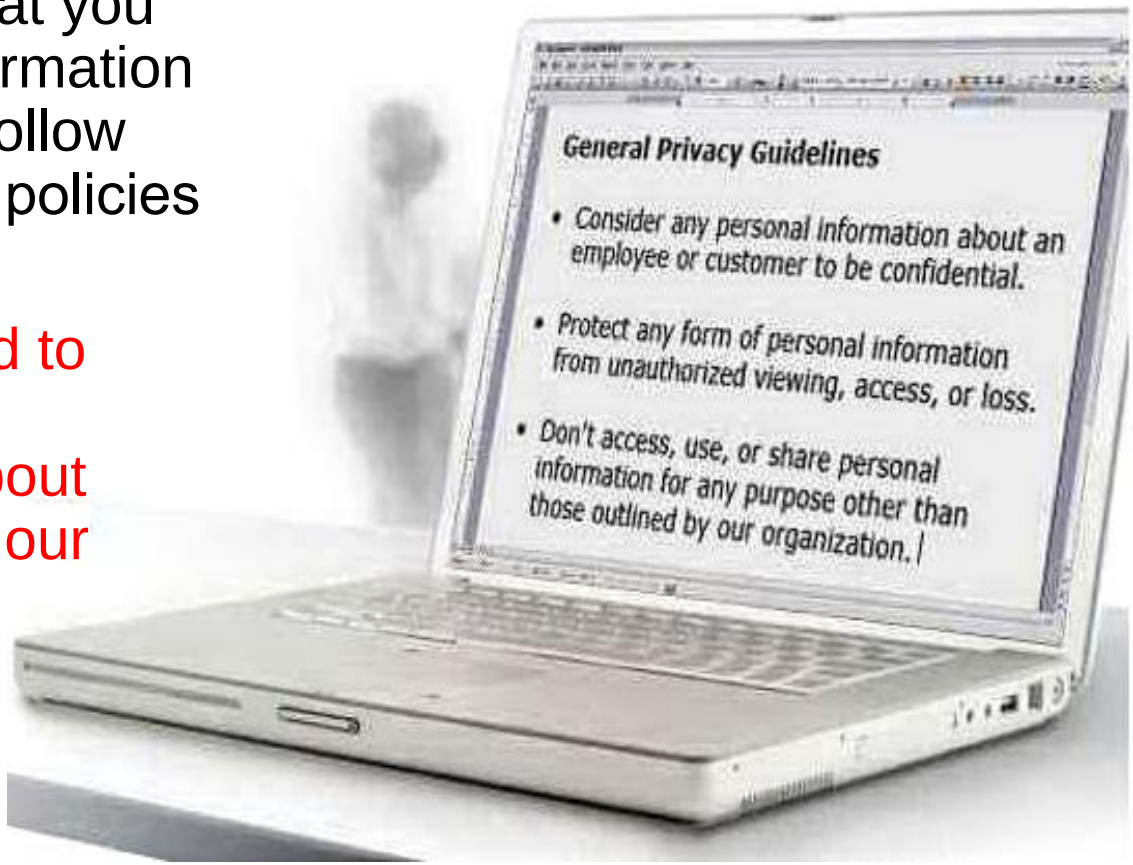
    Everyone needs to learn the privacy basics to make privacy-aware decisions, recognize non-compliant actions, and keep information secure.
- **Daily Responsibilities**
  - **Q:** "What are my daily privacy responsibilities?"
  - **A:** All employees are expected to understand and follow good privacy practices, including knowing and carrying out the actions needed to help safeguard personal information.

    These practices include simple procedures, like using strong passwords, properly handling electronic and printed information, and following policies for using personal and business confidential information.

Privacy Policies and Procedures

The only way to ensure that you are handling personal information properly is to review and follow our organization's privacy policies and procedures.

All employees are required to access and review these materials to learn more about privacy actions specific to our organization.



Source: Compass

Basic Security Procedures

Following basic security procedures supports privacy by preventing unauthorized access to personal information. These procedures are very important when using computers and other devices for information collection and storage as well as disposing of electronic data.

Basic Security Procedures

- **Clean Desk Guidelines**
  - At all times, employees must safeguard Manulife Financial confidential information, as well as the personally identifiable information of our customers, advisors and employees. This requirement includes appropriately protecting confidential or personally identifiable sensitive information on your desk or anywhere within your work area. One important way to protect that information is to ensure that when you are absent from your desk or work area, all documents containing sensitive information are properly stored out of sight and cannot be accessed by unauthorized individuals.
  - Examples of Manulife Financial confidential information that must be safeguarded:
    - New product development details
    - Company bank account numbers and account values
    - Company financial results not yet made public
  - Each business unit is responsible for developing and implementing reasonable practices and procedures to safeguard all sensitive information in their possession. This includes safeguards designed:
    - to secure all materials with sensitive information, even when such materials are not being used.
    - to assure that access to the workspace is appropriately restricted and controlled through the use of such devices as key-card access doors and appropriate supervision and monitoring of visitors.

Basic Security Procedures

- **Clean Desk Guidelines – Cont.,**
  - Following are required means for safeguarding all materials containing sensitive information:
    - locked file cabinets
    - locked desk drawers
    - locked rooms or offices
    - during business hours opaque files can be used to conceal documents that are being worked on during the day
    - encryption of electronic devices.
  - **Following are required means for safeguarding information on your computer when you are away from your desk/work area:**
    - lock your workstation with CTRL-ALT-DELETE
    - don't write your password(s) down
    - laptops must be locked to a docking station
    - use encrypted devices to protect information
    - properly secure USB sticks, Blackberrys, CDs, etc.
  - If multiple employees require access to materials or documents being appropriately kept under lock and key, duplicate keys can be provided to those persons who have a legitimate need to access those documents; and the master key/back-up key must always be stored in a secure location.

*****NO SENSITIVE DOCUMENTS SHOULD EVER BE LEFT UNATTENDED/UNSECURED ON A DESK, WITHIN A WORK AREA OR ANYWHERE ELSE.**

Basic Security Procedures

- **Document Destruction** – Dispose of all paper documents and electronic media containing personal or proprietary information in locked and secured bins to ensure that they are properly destroyed.
  - Disposal in Trash
    - We've all heard the stories about personal information that is disposed of in trash and later found strewn across parking lots or blowing in the wind. The fact is that disposing of any document containing personal or sensitive information in the trash is just plain dangerous. Trash is collected from all Manulife buildings and transported to land fill sites or other locations. At any point in that journey, it is accessible to virtually anyone – in fact, "dumpster divers" target trash to locate personal information that can be used to commit identity theft or other fraudulent acts. **Never dispose of any document containing personal or sensitive information in the trash!**

Basic Security Procedures

- **Hardware**
  - Before recycling or disposing of computer equipment, follow company policies to remove personal or business data, ensuring that it cannot be recovered.
- **Passwords**
  - Use strong passwords for everything. Never share them with anyone, remember to change them regularly and never write them down.
- **Network Access**
  - Lock your screen when you leave your computer to prevent unauthorized access to the network. Always use secure wireless connections when accessing personal or proprietary information.
- **Encryption**
  - Encrypt personal and proprietary information to prevent unauthorized access from third parties.
- **Printers, photocopiers, fax machines**
  - Ensure you don't leave documents at printers, photocopiers and fax machines unattended for any length of time. Use extra care when inputting fax numbers.

Incident Reporting

A final way to ensure privacy is to recognize and report incidents.

A **privacy incident** is any situation where personal or proprietary information is lost, stolen, or otherwise improperly disclosed or used. An incident could be anything from a lost or stolen laptop or information being accessed, used, or shared inappropriately.

If you witness a privacy incident or even a situation that just doesn't seem right, you have a responsibility to act immediately and contact the appropriate person to investigate the incident. Remember, our organization is relying on you to be mindful and trustworthy, and follow our incident reporting procedures.

Source: Compass

Remember:

Our greatest privacy defense lies in your hands, and just as you rely on others to keep your information secure, our customers and your fellow employees rely on you to take the necessary actions to protect their information.

Source: Compass

Thank you! This is the end of the module. Please proceed to answering the Privacy Policy Quiz.

Click Here

Thank you

Manulife Financial

For your future™