The Importance of PRIVACY in Project Management

Presented By: Carla Calabrese, CIPM Consultant

3rd Annual PMI Professional Development Days
May 17, 2017
You will learn

• What is privacy and what is considered personal information

• How to embed privacy into project management to lower risk and increase project success
  – Key ‘privacy by design’ principles/concepts
  – Benefits of privacy risk management in projects
  – Privacy Risk Management Tools and when to use them

• The Role of the Project Manager in Privacy Management
Get all the information you can, we'll think of a use for it later.
WHY DO ORGANIZATIONS NEED TO CARE ABOUT PRIVACY?
Why Does Privacy Matter?

• Privacy is fundamentally both a compliance/legal matter and a serious risk management issue
• Privacy class actions are exploding in Canada
  – Many within the public sector
• Even nominal damages spread across a large class can be significant
• Reputational and political harm can be even more consequential
Adverse Impacts/Harm to Individuals and Organizations

Adverse impact on the mental, physical, economic or social well-being of the individual to whom the information relates- e.g.:  
- hurt, humiliation  
- damage to reputation  
- stress, loss of business or employment  
- security risk  
- identity theft or fraud risk

-Stakeholders and the public express loss of confidence  
- damage to reputation  
- prolonged and highly negative media attention  
- significant economic implications to GNB  
- significant risk of litigation
Trend: Privacy Class Actions

- Class action litigation arising out of cyber and privacy risks is increasing in Canada.
- Privacy and cyber risks include
  - lost portable electronic storage devices,
  - uploads to an unsecure website,
  - improper disposal of computer equipment,
  - unauthorized access and dissemination by rogue employees,
  - cybercrime and business practices.
- More breaches and growing awareness of/concern about privacy rights have all likely contributed to the increase in class action proceedings.
- In addition, the recognition of a new tort for invasion of privacy by the Ontario Court of Appeal in 2012 has resulted in certification of privacy class actions based on the new tort.
What’s needed is an environment where protecting employees’ and clients’ privacy is top of mind for every new project or program; for significant changes to existing business or IT programs; and for every employee whenever handling personal information.
WHAT IS PRIVACY AND WHAT IS CONSIDERED PERSONAL INFORMATION?
What is Privacy?
Privacy is the right of individuals to decide/control to what extent information about themselves is shared with, used or accessed by others.

What is Confidentiality?
The commitment to keep a person’s personal information and/or personal health information private; to protect the information from being disclosed to others without the individual’s consent.

The privacy rights of individuals extend beyond the expectation that their information will be kept confidential or secure.
Privacy Legislation

• **Right to Information and Protection of Privacy Act (RTIPPA)**
  – NB public sector law that applies to personal information held or controlled by ‘public bodies’.

• **Personal Health Information Privacy and Access Act (PHIPAA)**
  – NB law applicable to the private and public sector that applies to personal health information collected, used disclosed, maintained or controlled by ‘custodians’.

• **Personal Information Protection and Electronic Documents Act (PIPEDA)**
  – Federal privacy legislation generally applicable to private sector organizations that collect, use and disclose personal information in carrying out commercial activities

• Other legislation as may be applicable to GNB’s collection, use or disclosure of personal information
Personal Information (*RTIPPA*)

PI means recorded information about an identifiable individual, including but not limited to,

(a) the individual’s name,
(b) the individual’s home address or electronic mail address or home telephone or facsimile number,
(c) information about the individual’s age, gender, sexual orientation, marital status or family status,
(d) information about the individual’s ancestry, race, colour, nationality or national or ethnic origin,
(e) information about the individual’s religion or creed or religious belief, association or activity,
(f) personal health information about the individual,
(g) the individual’s blood type, fingerprints or other hereditary characteristics,
(h) information about the individual’s political belief, association or activity,
(i) information about the individual’s education, employment or occupation or educational, employment or occupational history,
(j) information about the individual’s source of income or financial circumstances, activities or history,
(k) information about the individual’s criminal history, including regulatory offences,
(l) the individual’s own personal views or opinions, except if they are about another person,
(m) the views or opinions expressed about the individual by another person, and
(n) an identifying number, symbol or other particular assigned to the individual.
Personal Health Information (PHIPAA)

PHI means identifying information about an individual in oral or recorded form if the information:

(a) relates to the individual’s physical or mental health, family history or health care history, including genetic information about the individual,
(b) is the individual’s registration information, including the Medicare number of the individual,
(c) relates to the provision of health care to the individual,
(d) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,
(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance,
(f) identifies the individual’s substitute decision maker, or
(g) identifies an individual’s health care provider.
KEY PRIVACY BY DESIGN CONCEPTS
Privacy by Design (PbD)

• Focuses on preventing privacy risks, by compelling business leaders and developers to build privacy protection into, not just their technology, but also their business processes, physical design and networked infrastructure.

“In essence, it helps organizations to operate in a mode of what I call “default” privacy protection.” Ann Cavoukian
The 7 Foundational Principles

1. **Proactive** not Reactive; **Preventative** not Remedial
   Anticipate and prevent privacy issues before they happen by planning and budgeting for resources to complete a PIA /privacy analysis

2. Privacy as the **Default**
   During the Design/Development phases- Personal information is automatically protected in any IT system or business practice- by default

3. Privacy **Embedded** into Design
   Privacy is an element in the project plan during the Design phase- as an essential component of core functionality being delivered

4. **Full Functionality** –Positive-Sum, not Zero-Sum
   Business and IT work together with the Project team to accommodate all interests and objectives...’win-win’ not an ‘either/or’

5. **End-to-End Lifecycle Protection**

6. **Visibility and Transparency**

7. **Respect for User Privacy**
INCORPORATING PRIVACY IN PROJECT MANAGEMENT
Key Privacy Risk Management Tools

• Much like PRINCE2 and PMP Project Management methodologies, Privacy Management takes a risk based approach to assessing the likelihood and impact of privacy incidents.

• Privacy Management risk based tools:
  – Privacy Gap Analysis
  – Privacy Impact Assessment
What is a Privacy Impact Assessment (PIA)?

• A Privacy Impact Assessment (PIA) is a risk management tool
  – Helps determine whether a system, process or program involving personal information raises privacy risks
  – Proposes solutions to mitigate privacy risks

• Can be completed on new or existing systems, processes or programs, or services involving PI/PHI
Wait! Has anyone done a privacy impact assessment?
Objectives of a PIA

• Assess the extent to which a system/program/process meets **legislated and best practice** requirements for protecting personal information

• Identify and assess the privacy risks associated with implementing new or changed systems/programs and recommend options for managing and mitigating the risks

• Help the project team and business leaders address privacy risks proactively
When is a PIA needed?

• New projects, programs, services or systems
• Major changes to existing programs
• Changes in collecting, using or disclosing personal information
• Additional systems or data linkages
• Enhanced accessibility
• Re-engineering business processes
• Changes in technology
Two Types of PIAs

Preliminary or Conceptual PIA

- Completed during a project’s initiation/needs assessment (e.g. during the drafting of the business case)
- Identifies potential privacy issues at the project’s/program’s conceptual stage thus reducing negative impacts on the project budget/schedule later on
- Assesses:
  - Proposed goals/objectives of the proposed project, program, service or system
  - Types and sensitivity of PI that will be collected, used, disclosed and retained
  - Persons who will collect, use and disclose and/or have access to the PI
  - Legislative authority for the proposed collection, use and disclosure of PI
  - Roles and responsibilities of stakeholders re: accountability for the protection of PI
  - Aspects that are most likely to involve privacy risks
- Important because it helps projects develop a plan to avoid/mitigate any adverse effects and ensure privacy is considered from the beginning
Two Types of PIAs cont’d

Design Level or In-Depth PIA

- Completed during a project’s Design phase
- Is an in-depth privacy analysis of a project, program, service or system
- Ensures no new privacy risks have been created by the design
- Assesses:
  - Privacy analysis and privacy risks and recommendations identified in the Conceptual PIA and if they have been addressed in Design
  - Types and sensitivity of PI that will be collected, used, disclosed and retained
  - Access to and storage of the PI
  - Notification and consent requirements
  - Legislative authority for the collection, use and disclosure of PI
  - Governance
  - Close examination of technical architecture and business processes
  - The flow of data (personal information) between systems, stakeholders, programs
  - Safeguards
  - Privacy risks
Timing - When to Begin a PIA?

• A PIA may begin:
  – During the **Project Initiation/Needs Assessment phase** (Conceptual PIA) to identify potential privacy issues at a high level to guide program/system design decisions
  – During the **Design Phase** for a new project or system and before implementation
  – Early enough to allow time to complete the PIA and identify potential privacy risks before the new system/program goes live
  – When sufficient business process and technical documentation is available

• Ideally, if design changes are required to address risks, the timing of the PIA should allow for these to be completed before the system/program ‘goes live’
What are the Benefits of a PIA?

• Enables systematic identification and assessment of privacy and data protection risks during a project’s conceptual and design phases

• Supports compliance with privacy legislation and other policy and organizational requirements

• Avoids costly rework or delays on projects by dealing proactively with potential privacy issues that may arise, during the design phase

• Reduces the likelihood and impact of privacy breaches associated with the new system or program

• Brings accountability and responsibility for ensuring privacy is addressed

• Demonstrates due diligence/effective risk management by building privacy protections into the design from the outset of the project
What’s Involved in Conducting a PIA?

• Review documentation and conduct initial interviews to understand the application of the proposed solution/program/system
• Validation of PIA scope and development of a workplan for review with the Project Steering Committee or Sponsor
• Document understanding of business processes, data flows and data storage locations
• Legislative analysis
  – Identification and analysis of applicable legislation
• Privacy analysis
  – Assessment of personal information data flows in the context of privacy legislation and privacy principles
  – Identify personal information to be collected, used and disclosed and the purpose
  – Identification of legislative authority(ies) for collection, use and disclosure of personal information
  – Review relevant privacy and security policies, agreements, contractual clauses
  – Review of methods for protecting of personal information in transit and storage
  – Review of consent and notification issues
• Identify and assess risks / potential impacts to individuals’ privacy and validate with the Project Steering Committee or Sponsor
  – Identify risk mitigation recommendations
ROLE OF THE PROJECT MANAGER
Your Role in Privacy Management

- **Planning and Budgeting** for the resources (time, cost) to carry out a PIA / privacy analysis
  - Reinforce with Project Sponsors/Business Owners the need to and benefits of completing a PIA for projects/programs/services or systems involving PI/PHI

- **Quality**- ensuring the project/program/service or system complies with privacy legislative requirements

- **Risk management**
  - Incorporate privacy risk assessment tools as part of the documentation required during each Project Phase/Gate
  - Identify and treat privacy risks as part of the project risk log
  - Ensure stakeholders are informed of major privacy risks and how they are being mitigated
  - Ensure key risks are mitigated before ‘go live’

- **Procurement / Contracts**
  - Work with Procurement to ensure privacy requirements are appropriately incorporated in all public tenders, vendor requirements, contracts and agreements

- **Communication and Change Management**
  - Open communication with the vendor, third party service providers, developers and business owners during all phases of the project to ensure privacy requirements are incorporated in the design and prevent privacy breaches during the project phases e.g. testing
  - Work with the Project Steering Committees, Sponsors, Business Owners and Project Team Members to create privacy awareness and the importance of privacy in project management
Summary

Project managers have a key role to play in helping their organizations identify, mitigate and manage privacy risks for each new project/program/service and/or system by incorporating privacy by design concepts and privacy risk management tools into the project management lifecycle.
So, it's agreed—we go ahead with the information-matching.
Thank You

Carla Calabrese, CIPM

www.maraconsulting.ca

Privacy Consulting  Project Management
Technology Consulting  Business Consulting