

Examining the Relationship Between Privacy Compliance and Information Management

**Sandra Smith-Frampton
Sr. Risk Manager, Privacy Compliance
ATB Financial
Alberta, Canada**

**March 7, 2007
3:00pm – 3:45pm**

Session Objective

- ★ **To understand how privacy compliance can be established through:**
 - **identifying and managing personal information banks**
 - **implementing corporate retention and disposition programs; and**
 - **leveraging existing electronic information management tools**

Privacy Legislation

Compliance and Breach Resolution is knowing:

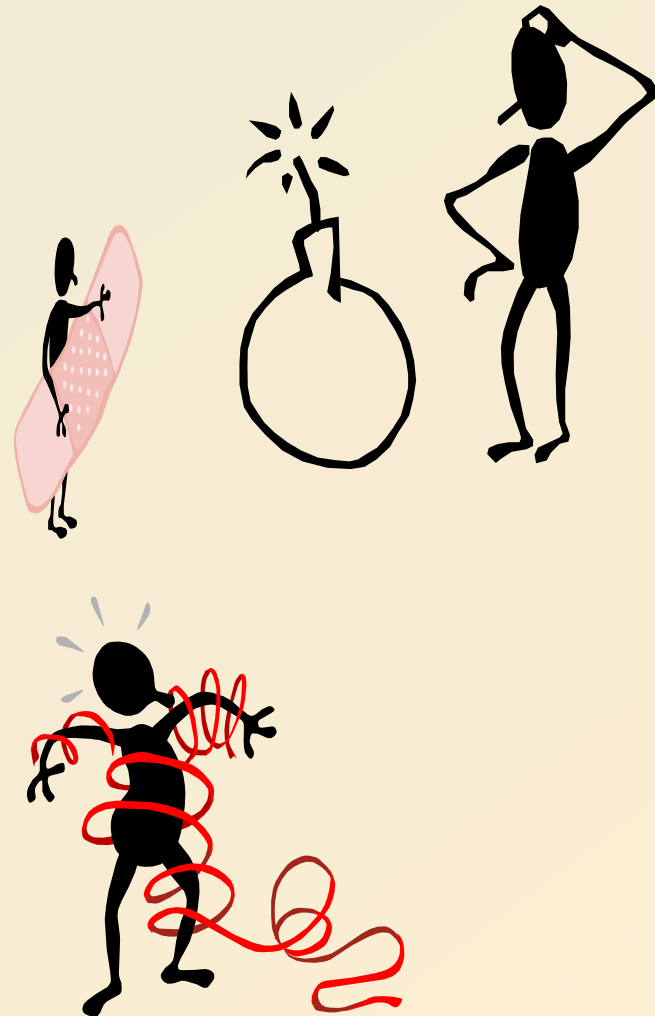


- ★ Where the personal information (PI) in question resides
- ★ Who has access to it?
- ★ How is it used?
- ★ To whom is it shared?
- ★ How long should it or does it need to be kept?

Fact or Fiction?

Many Organizations

- ★ Continue to grow information stores
- ★ Apply the “spatial concept”
- ★ See file management as a clerical responsibility
- ★ Don't have the tools to identify the documentation needed for a privacy complaint



Privacy Challenges

★ Accountability

- Control over personal information resources

★ Identifying purposes

- Ensuring personal information uses are not compromised

★ Retention/destruction/security

- Risk of destroying too soon or too late
- Ensuring adequate security
- Tracking and controlling access



Challenges Continued

- ★ Accuracy

- Accountability, evidence,

- ★ Consent and correction

- Consistency

- Tracking and recording annotations

- ★ Compliance challenges

- Fines, offences, public orders

- Other Acts:

- Patriot Act, Sarbanes-Oxley, Securities Administration and Internal Controls Requirements, Electronic Transactions Act, Criminal Code, etc.



Destroy or Not to Destroy

★ obligations to track and keep

★ silent on when to destroy

RISKS

- Destroying what the law requires keeping
- Keeping what must be destroyed
- Destroying what litigation strategy dictates keeping
- Exposure to allegations of improper destruction

Some edocs believed to be destroyed can be revived by searching hard drives/back-up tapes = considerable costs

Criminal Intent

- ★ Knowingly or Wantingly
 - Obstructing justice
 - Fraudulently removing or concealing
 - Data management mischief
- ★ Morgan Stanley – 2 Billion awarded
- ★ Indictable offences – Sarbanes Oxley, Gramm-Leach-Bliley, C-Sox



Key Compliance Concepts

★ Balancing Quantity and Quality

— Completeness and Reliability:

— Ensuring accurate representation when documenting events or transaction details

— Authenticity:

— Recording what it says it is: secured, sent, viewed and received by intended persons only

— Useability:

— A record can be retrieved and understood fully and independently, with proper security, and when required

— Retention:

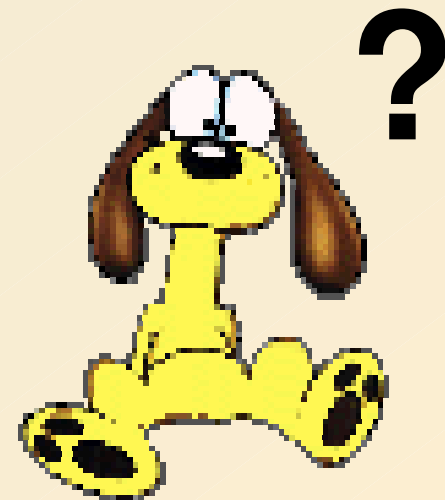
— Information is not retained longer than required

The Convergence Puzzle



Okay....

Now we know the WHY
What about the HOW



Information and PIB Registry

BLOCK: Legal Services

PRIMARY TERM: Contracts and Agreements for Service

PRIMARY CODE: L180

SCOPE NOTES: Information specific to contractual arrangements for internal or external sourcing. May contain contractual obligations, audit schedules, payment schedules, company contact information/data and personal information of involved parties, such as name financial data, and other personal identifiers.

CROSS INDICES: XXX Finance - Accounts Payable
(Not here - there!) XXX HR - Recruitment

CROSS REFERENCES: contractor or employee name, agreement number, agreement specifics

MASTER:

DEPARTMENT OF RESPONSIBILITY: Legal		LOCATION: CC Building
RIDER: completion or expiry of contract	RETENTION PERIOD: 2-8-0 LEGAL RATIONALE: S.31 ss(a) Statutes of Limitations Act	FINAL DISPOSITION: Selective Retention
ESSENTIAL VALUE: YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	BUSINESS VALUE : <input type="checkbox"/> PERMANENT <input type="checkbox"/> HISTORICAL <input checked="" type="checkbox"/> FINANCIAL <input type="checkbox"/> SCIENTIFIC <input checked="" type="checkbox"/> LEGAL <input type="checkbox"/> OPERATIONAL <input checked="" type="checkbox"/> ADMINISTRATIVE	MEDIA: Paper / electronic
ACCESS STATUS: <input type="checkbox"/> FULL ACCESS <input type="checkbox"/> INTERNAL ACCESS ONLY <input checked="" type="checkbox"/> RESTRICTED INTERNAL ACCESS		<input checked="" type="checkbox"/> PERSONAL INFORMATION BANK
IF INTERNAL ACCESS ONLY OR RESTRICTED - WHY? Access is restricted until contract is finalized		

Identification Process: Identified by a single alpha assignment representing the contract. Both the electronic data entry and the paper file must list cross indices.

COPY:

DEPARTMENT OF RESPONSIBILITY: Legal		LOCATION: CC Server
RIDER: completion or expiry of contract	RETENTION PERIOD: 2-0-0 LEGAL RATIONALE: duplication	FINAL DISPOSITION: destroy
ESSENTIAL VALUE: YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	BUSINESS VALUE : <input type="checkbox"/> PERMANENT <input type="checkbox"/> HISTORICAL <input type="checkbox"/> FINANCIAL <input type="checkbox"/> SCIENTIFIC <input type="checkbox"/> LEGAL <input type="checkbox"/> OPERATIONAL <input checked="" type="checkbox"/> ADMINISTRATIVE	MEDIA: Electronic
ACCESS STATUS: <input type="checkbox"/> FULL ACCESS <input type="checkbox"/> INTERNAL ACCESS ONLY <input checked="" type="checkbox"/> RESTRICTED INTERNAL ACCESS		<input checked="" type="checkbox"/> PERSONAL INFORMATION BANK

Signature:	Title:	Date:
------------	--------	-------

Personal Information Bank Registry

#	Function / Activity	Records Series	Owner / Responsible Office	Personal Information	Subjects	Security	Retention	Collection, Use Disclosure
	Human Resources Recruitment	Payment Information		Information including: name, number, educational background, affiliations, personal and specialties and any information contained in a resume; interview notes, reference check notes correspondence, e-mails, copies of photo ID, birth date, sex, length or time at addresses, criminal history question, SIN,			Current year plus 1	Owners – recruitment implied consent
L00	Legal - External						Current year plus 6	
L00	Legal - Internal					Consistent with General Information Security Strategy	Current year plus 6	Owner – conflict of interest, risk management -- implied consent
L02	Legal Agreements / Contracts		Interest, Sourcing	Corporate Data, Payment Schedules Experience, Records and/or Documents specific to a contract or agreement		Copy Hard copies retained by & available to HR, Joint Interest, Land and Sourcing	Termination of contract plus 6 years	Owners -- Production, Revenue & Cost Allocation, Contract Administration, Contract Payments -- implied consent Revenue Canada – tax purposes -- Exception

Information Management Makes...

- ★ Retrieval easy
 - Time spent tracking and retrieving can be costly to a company
- ★ Finds the information impacted
 - Retrieving incorrect information can be time consuming and embarrassing
- ★ Fulfils obligations to retain, destroy, dispose
 - Lost, unaccounted for, and data kept too long can have both privacy and legal implications. If you have it you produce it

Integrated RM/Security/Privacy Tools

- Personal information registries
- Security asset/inventory management
- Security classification marking
- User access management/tracking (role and case-based)
- Record location and access rights
- Collection/use/disclosure tracking
- Privacy Impact Assessment data flow analysis
- Disclosure logs
- Consent descriptors

Compliance is Having...

Check-in/check-out procedures

- Understanding the flow of information is an investment

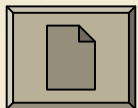
System logs and reporting mechanisms

- Requests require documenting what has been searched

Audit trails

- A system that tracks location and users of information regardless of media

Capability to search millions of records in seconds



- Manual searches disrupt operations

Compliance Achieved By...



Non-Compliant

Compliant

- ★ Ascertaining the flow of information
- ★ Having an electronic system to locate information regardless of its media
- ★ Avoiding manual searches - they disrupt operations
- ★ Applying legislated retention and disposition vs. the “spatial concept”
- ★ Knowing who is responsible for and has access to the information
- ★ Documenting privacy complaints with the certainty nothing has been missed

Compliance Defined

- ★ Only collect, record and keep information that is needed
- ★ Only use it for purpose collected
- ★ Only share it with those that need it
- ★ Track collection, use, disclosure, format, storage, correction, access and security
- ★ Always assume that someone else will eventually get to see it

Key to minimizing business liability is to have an effective RIM/EDMS and record retention program in place...

Not just for privacy compliance but as proactive business practice

Fallacy and Reality

Current privacy law does not
state

*“organizations must have RIM and/or
EDMS to be privacy compliant”*

Reality is...

Privacy compliance can leverage RIM /
EDMS as a tool to mitigate the risk of
litigation, investigation, audits and
embarrassment

***“Privacy is not an obstacle.
Privacy is a tool...
an information management tool”***

AND

***“Compliance... is building privacy into
business culture and core values”***

Sandra Smith-Frampton
Sr. Risk Manager, Privacy Compliance
ATB Financial
October 2006

Examining the Relationship Between Privacy Compliance and Information Management

Please Complete Your Session Evaluation

Sandra Smith-Frampton
**Sr. Risk Manager, Privacy Compliance/
Corporate Privacy Officer**
ATB Financial
ssmithframpton@atb.com