Dollars and Sense: Risk-Based Decision Making in Privacy Investment

eHealth 2015

Darcelle Hall, John Zachariah

MD+A Health Solutions

120 Carlton Street, Suite 416
Toronto, ON M5A 4K2
t. 416.642.2081
f. 416.642.2082
e. info@mdahealth.ca
w. www.mdahealth.ca

Introduction: How risk drives decision-making

- Organizations need to make decisions on where and how to mature their privacy programs
  - Competing priorities and constrained budget
  - Limited information for senior decision-makers
- Today's objective: identify conditions under which you can meaningfully identify and manage privacy risk to support the maturity of your program
  - Supports informed decision-making about where to allocate resources (time, budget and people)

md+a health solutions

Privacy program as a risk management tool

- Any organization managing PHI as a custodian under PHIPA is at risk
  - Your privacy program provides the basis for effective privacy risk management
  - Even large and complex organizations have not fully developed all the components of their privacy programs

- But what are the risks … ?

md+a health solutions

What does the media have to say?

- Recent articles in media (e.g., Toronto Star) that have focused on:
  - Inappropriate access by employees of health care providers
  - Lack of requirement to notify IPC in the event of breaches (i.e., lack of accountability)

What issues have captured the attention of the IPC?

- Health Orders from the IPC have addressed:
  - Inappropriate access by employees
  - Inappropriate management of PHI/inadequate safeguards
  - Issues regarding individual access to records

What are the common risks from our PIAs?

- Common risks identified in PIAs include:
  - Absence of appropriate agreements and policies (incomplete definition of privacy obligations)
  - Limited clarity regarding employee and agent access to PHI
  - Absence of proactive auditing procedures (many ad hoc and reactive auditing procedures)
  - Gaps in information security safeguards (firewalls, access controls, encryption, etc.)

Privacy program as a risk management tool

- Don’t play whack-a-mole!
- Focus required on managed program development
  - Review, update and implement privacy policy and procedure
    - If you don’t have policies, create them
  - Communicate expectations through training
  - Review for compliance

md+a health solutions

Review for compliance

- Look for evidence of compliance with the standard that your program has established
  - You need ***evidence*** to do this properly
  - You can determine compliance through audits, assessments, interviews, etc.
- This is an opportunity for ***privacy risk identification***

md+a health solutions

Risk management: the missing step

- Organizations do not always know how to manage privacy risk
  - Addressed on an ad hoc basis (e.g., policy update)
  - Not reported to senior management
  - ***Not documented***
- Organizations need to actively understand and manage risks
  - Rather than simply reacting to the risks

md+a health solutions

Managing privacy risk

- Privacy program should maintain procedures for management of risk, including:
  - Ongoing review and remediation
  - Reporting to leadership on risk management status
    - Leadership should report back, correct course where needed

md+a health solutions

Managing privacy risk

- Privacy program must review risks on an ongoing basis to ensure
  - Risks have been appropriately prioritized
    - Potential impact, legislative compliance, etc.
  - Every risk has an associated strategy for management
    - Privacy program requires input from other areas of the organization (e.g., IT for encryption)

Conclusion: Risk-based decision-making

- Appropriate privacy risk management supports
  - Disciplined remediation of privacy risk ***through privacy program mechanisms***
  - Informed decision-making and targeted investment of people, time and resources

md+a health solutions

Questions?

- Darcelle Hall
  darcelle@mdahealth.ca

- John Zachariah
  john@mdahealth.ca