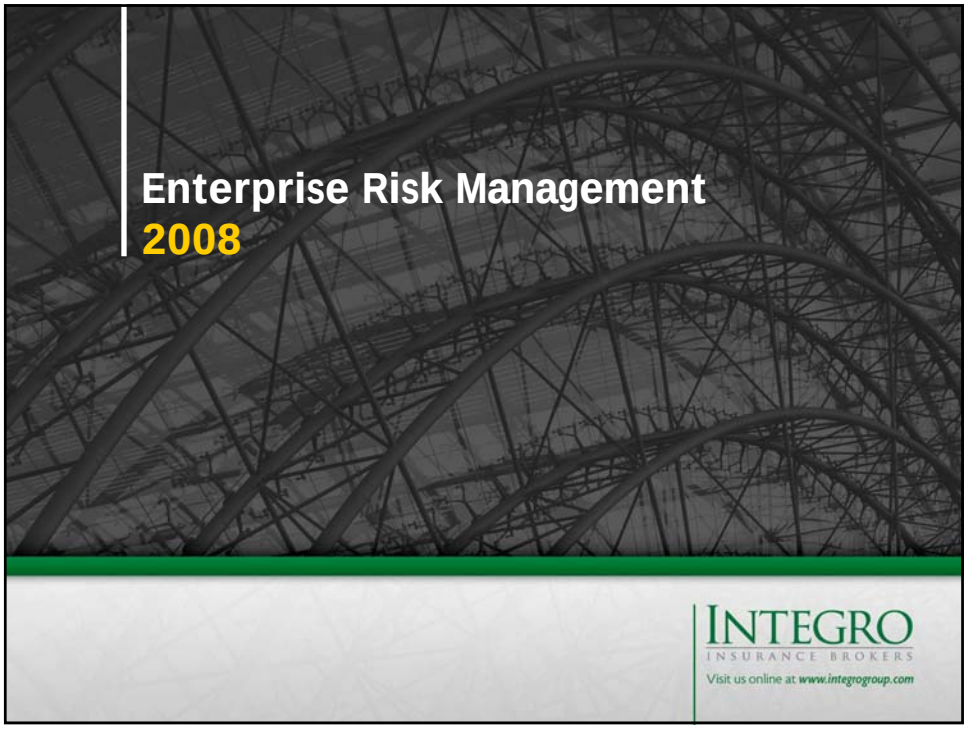


ERM Defined

INTEGRO INSURANCE BROKERS

- "A process, effected by an entity's board of directors, management and staff, applied in strategy setting and across the enterprise, designed to:
  - identify potential events that may affect the entity,
  - manage risks within its risk appetite, and
  - provide reasonable assurance regarding the achievement of entity objectives."

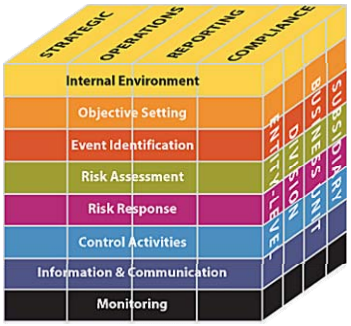
Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO

The ERM Framework

INTEGRO INSURANCE BROKERS

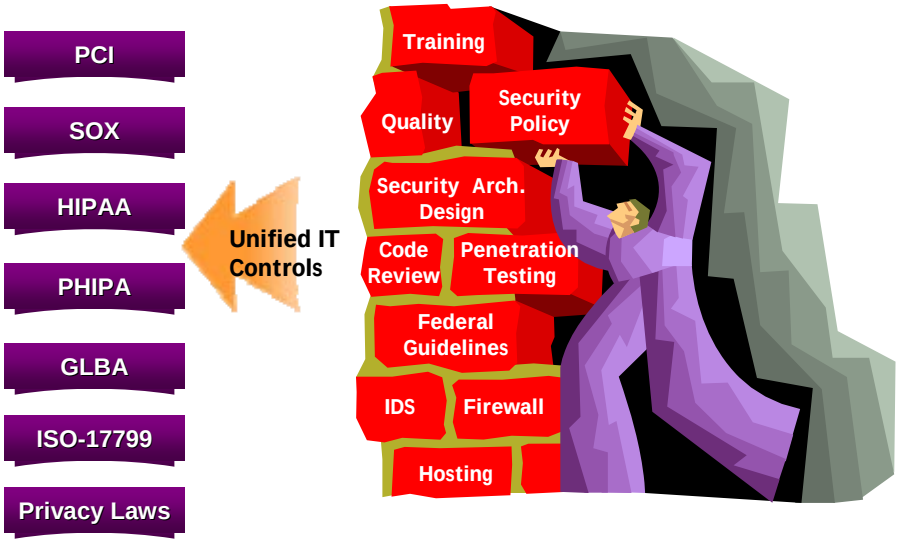
Entity objectives can be viewed in the context of four categories:

- Strategic
- Operations
- Financial
- Compliance



Building a Unified Enterprise–wide Compliance Program

INTEGRO INSURANCE BROKERS



Cyber (Privacy) Event Identification

- Differentiates risks and opportunities for an HCO.
- Events that may have a negative impact represent risks.
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting to protect and improve “cyber” management.

Event Identification

- Involves identifying those incidents, occurring internally (staff snooping in records) or externally (hackers to medical databases), that could affect strategy and achievement of objectives.
- Addresses how internal and external factors combine and interact to influence the risk profile of your HCO.

Notification Events

Year	Records Lost/Stolen	Incidents Reported	Incidents Per Week	States with Notification Laws
2007*	65,149,214	184	7.36	36
2006	49,679,260	346	6.65	30
2005	55,986,942	138	2.65	11
2004	31,895,900	21	0.40	1
2003	6,405,000	11	0.21	1
2002	4,960	3	0.06	0
2001	157,250	9	0.17	0

* The first six months of 2007

http://etiolated.org/statistics

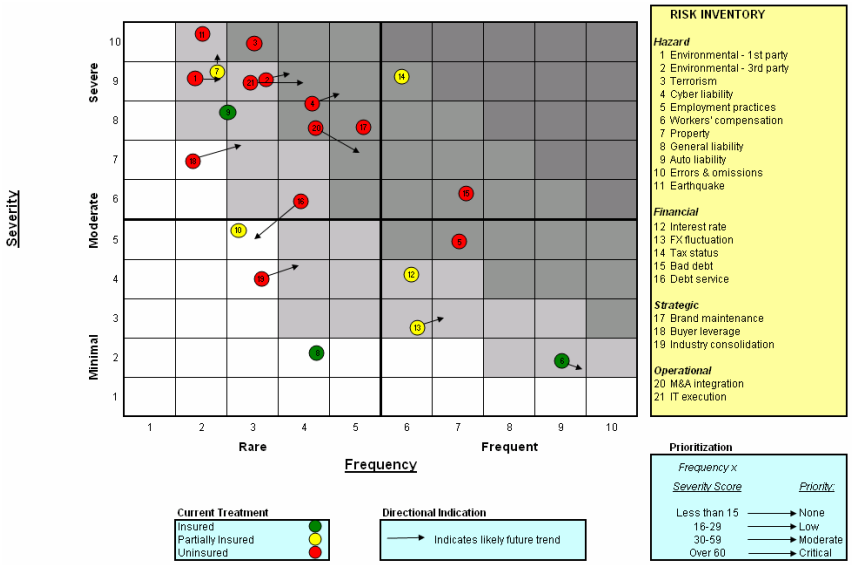
Risk Assessment

- Allows an entity to understand the extent to which potential events might impact objectives.
- Assesses risks from two perspectives:
  - Likelihood of a cyber attack
  - Impact of the attack on the HCO and on patients
- Is used to assess risks and is normally also used to measure the related objectives.

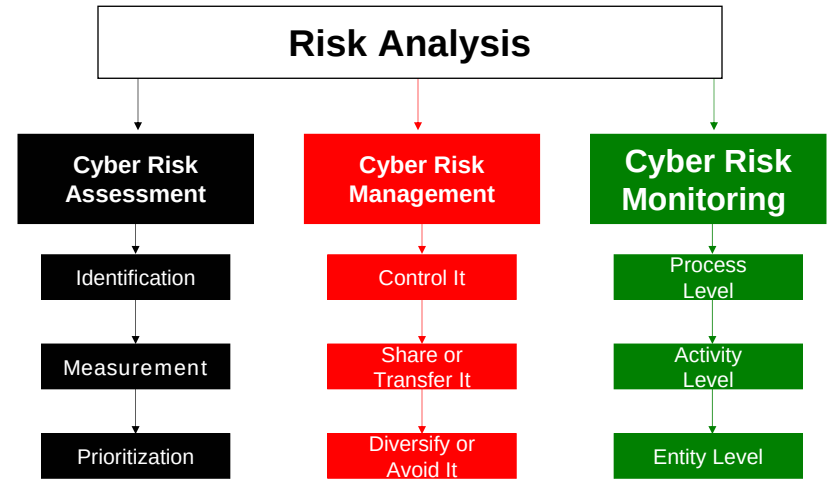
Risk Response

- Identifies and evaluates possible responses to risk.
- Evaluates options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.
- Selects and executes response based on evaluation of the portfolio of risks and responses.

Risk Assessment & Response: Integro Risk Map



Risk Analysis



Source: Business Risk Assessment. 1998 – The Institute of Internal Auditors

Example: HCO Call Center Risk Assessment of Cyber Hacker

IMPACT	PROBABILITY: Low	PROBABILITY: High
High	***Medium Risk*** • Loss of phones • Loss of computers • Loss of data	***High Risk*** • Bodily injury • Patient has a long wait, injury • Patient can't get through, injury • Delay in treatment
Low	***Low Risk*** • Fraud • Lost transactions • Employee morale	***Medium Risk*** • Loss of customer base • Equipment obsolescence • Repeat calls for same problem

But why bother? Economics of Data Breach

INTEGRO INSURANCE BROKERS

A hypothetical service provider compromises 100,000 accounts when a laptop computer is stolen. What is the potential financial impact?

Notify Clients and Provide Privacy Guard	$50 x 100,000 = $5 million
Fines and Penalties	$100,000 to $10 million
Loss of Clients	100,000 clients – 15% = 15,000 clients 15,000 x $100 in fees = $1.5m in lost fees
Fraud liability	1,000 accounts x $500 = $500,000
Reputation Loss	**PRICELESS!**

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Privacy Risk and Responses

Kathryn Frelick,
Miller Thomson LLP
June 26, 2008

2007 - Year of the Privacy Breach

- Annual Report on PIPEDA – Privacy Commissioner
  - number and scope of privacy breaches worldwide
  - "inexcusable security breaches" … "basic steps being ignored" … "human error or cavalier approach to security"
  - 21 voluntary breach reports this year … last year 34 voluntary reports total

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

What is Privacy Risk?

- Component of business risk resulting from the collection, use, retention and disclosure of PI
- Privacy threats include data breaches, complaints, non-compliance or over-compliance, which could result in financial loss, stakeholder dissatisfaction, reputational loss

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

What is a Privacy Breach?

- unauthorized access to or collection, use or disclosure of personal information.
- i.e. occurs in contravention of applicable privacy legislation (i.e. PHIPA) or have not taken reasonable steps to ensure PHI is protected against theft, loss, unauthorized use and disclosure, copying, modification or disposal

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Examples of Privacy Breaches

- Unauthorized collection of PHI
  - Video camera, camera phones
- Unauthorized disclosure of PHI
  - Lost or stolen laptop containing PHI
  - "Recycled" material used inappropriately
  - Intercepted video monitoring
- Unauthorized use of PHI
  - Staff inappropriately accessing health record

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Can Also Be . . .

- Misdirected faxes containing PHI
- Unencrypted electronic communications
- "Hallway" conversations
- Discussing PHI in social setting
- Providing PHI to a visitor or family member without the client's consent
- Accessing own/family member's health record

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Addressing Privacy Breaches

- How might you learn of a breach of privacy or confidentiality?
  - Report or complaint by client, care provider, etc.
  - Person who breached may self-report
  - Through audit, review, notification system
  - Through formal complaint to IPC or legal claim

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Addressing Breaches

- Prevention is the best strategy
  - Appropriate PHI safeguards in place
  - Appropriate privacy policies
  - Ensure education/training re: obligations
  - Regular reviews and audits
  - Proper storage, disposal, destruction
  - Privacy impact assessments for new systems, technologies, programs

. . . Still, breaches can happen . . .

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Steps for Addressing a Breach

1. Initiate Internal Protocol
2. Containment
3. Notification
4. Investigation/Remediation

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Step 1: Internal Protocol

- Initiate <u>as soon as potential breach is identified</u>:
  - Notify appropriate staff (e.g. Chief Privacy Officer, privacy contact person)
  - Depending on nature, seriousness, contact Sr. Management, Patient Relations, IT, Communications
  - Initiate internal investigation process
  - Follow organizational policies and procedures

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Step 2: Containment

- Identify scope of the potential breach and take steps to contain it:
  - Determine whether it was isolated incident or ongoing
  - Retrieve hard copies / secure electronic copies – lookback program
  - Ensure no copies of PHI were made/retained

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Step 2: Containment

- Determine whether breach would allow unauthorized access to other PHI and take appropriate steps
  - Suspend access
  - Change passwords/identification numbers
  - Temporarily shut down system

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Step 3: Notification

- Client(s) whose privacy was breached must be notified of the breach under PHIPA at first possible opportunity
- Manner of notification is not specified
  - Consider: sensitivity of information; potential detrimental effects for patient; best way to communicate information
- Not a requirement under PIPEDA, but advisable if risk to individual

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Step 3: Notification

- Advise client of:
  - Extent of breach
  - Specific PHI at issue
  - Steps taken by organization
  - Steps client should take (if any) – identify theft (i.e. fraud alerts/notifications)/care requirements
- May wish to solicit assistance of others (e.g. client's health care provider)
- May also notify IPC – positive statement in guidelines

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Step 4: Investigation and Remediation

- Conduct internal investigation
- Objectives:
  (1) Ensure immediate requirements of containment and notification have been addressed
  (2) Review circumstances around breach
  (3) Review adequacy of policies, procedures in protecting PHI

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Step 4: Investigation and Remediation

- Steps for investigation should be established through organizational policy
- Systemic perspective
  – Review, modification of organizational policies / procedures needed?
  – Is further education/training necessary?
  – How can we prevent breach, ensure compliance in future?

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Information and Privacy Commissioner's Role

- Powers of Commissioner:
  - Formal review of privacy breaches and complaints
  - Review of suspected non-compliance with PHIPA
  - Make orders and recommendations to organization or its agent, including enforceable orders

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Commissioner's Role

  - Authorize certain information collection practices
  - Educate, communicate with public about health privacy
  - Research health privacy issues
- Always co-operate fully with Commissioner in investigations

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Other powers

- Offences under *Provincial Offences Act* – significant fines
- Action for damages for breach of PHIPA
  - Statutory right to seek compensation for actual harm (where offence or final order)
  - Damages for mental anguish capped at $10,000 and only payable where willful or reckless

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Risk Management Considerations

- Ensure staff are educated/trained in privacy and confidentiality obligations
- Ensure appropriate policies and procedures are in place and followed

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

. . . Risk Management

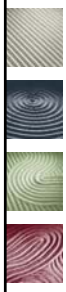
- Implement systems for identifying and preventing breaches
- Considerations for communication of breaches to client, public
- Legal advice for dealing with breaches

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

Q & A

- Questions?
- Comments?

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents



THANK YOU!

Kathryn Frelick
kfrelick@millerthomson.com

MILLER THOMSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents

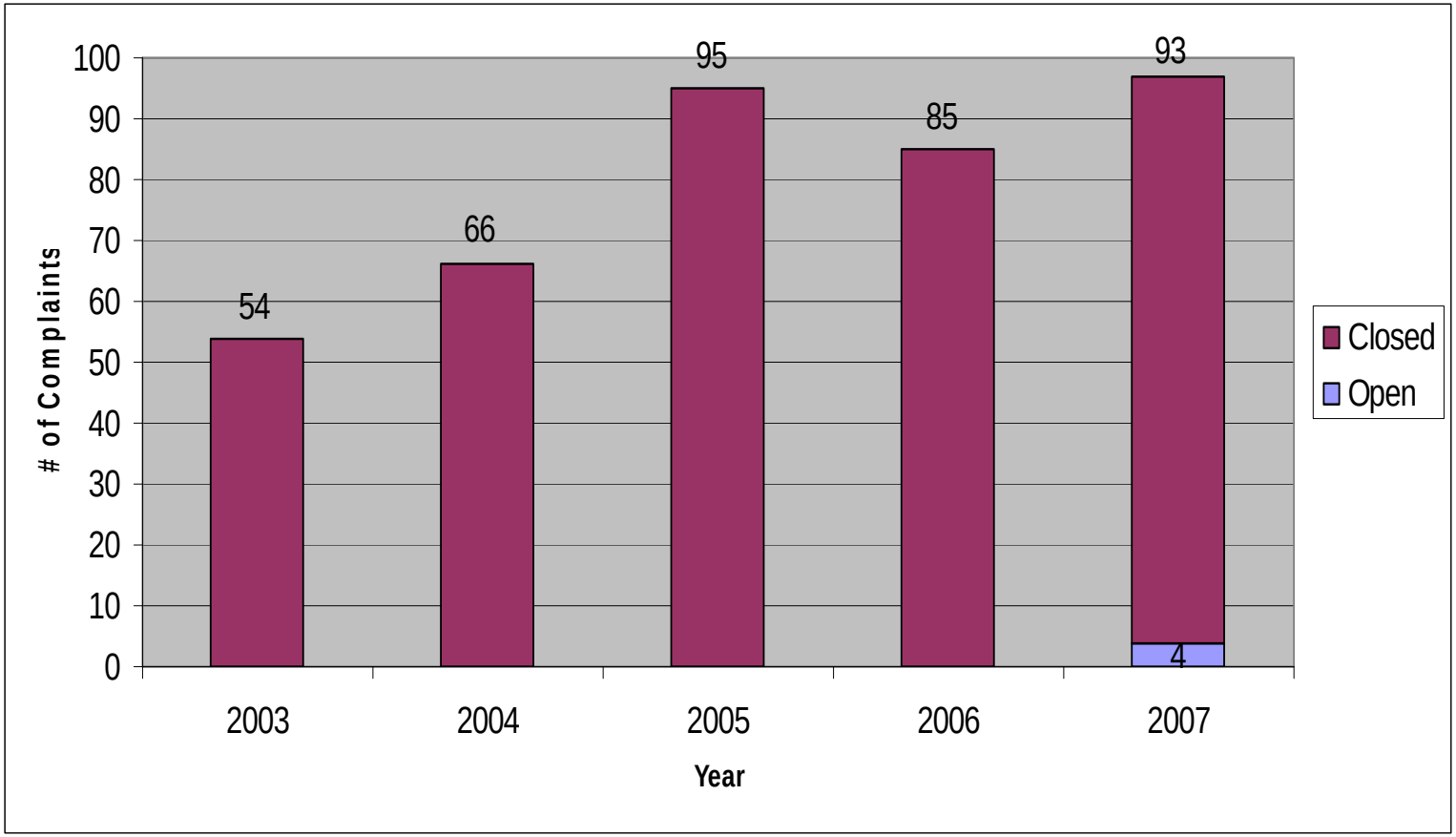
Managing Privacy Risk and Liability

Claims Management Implications

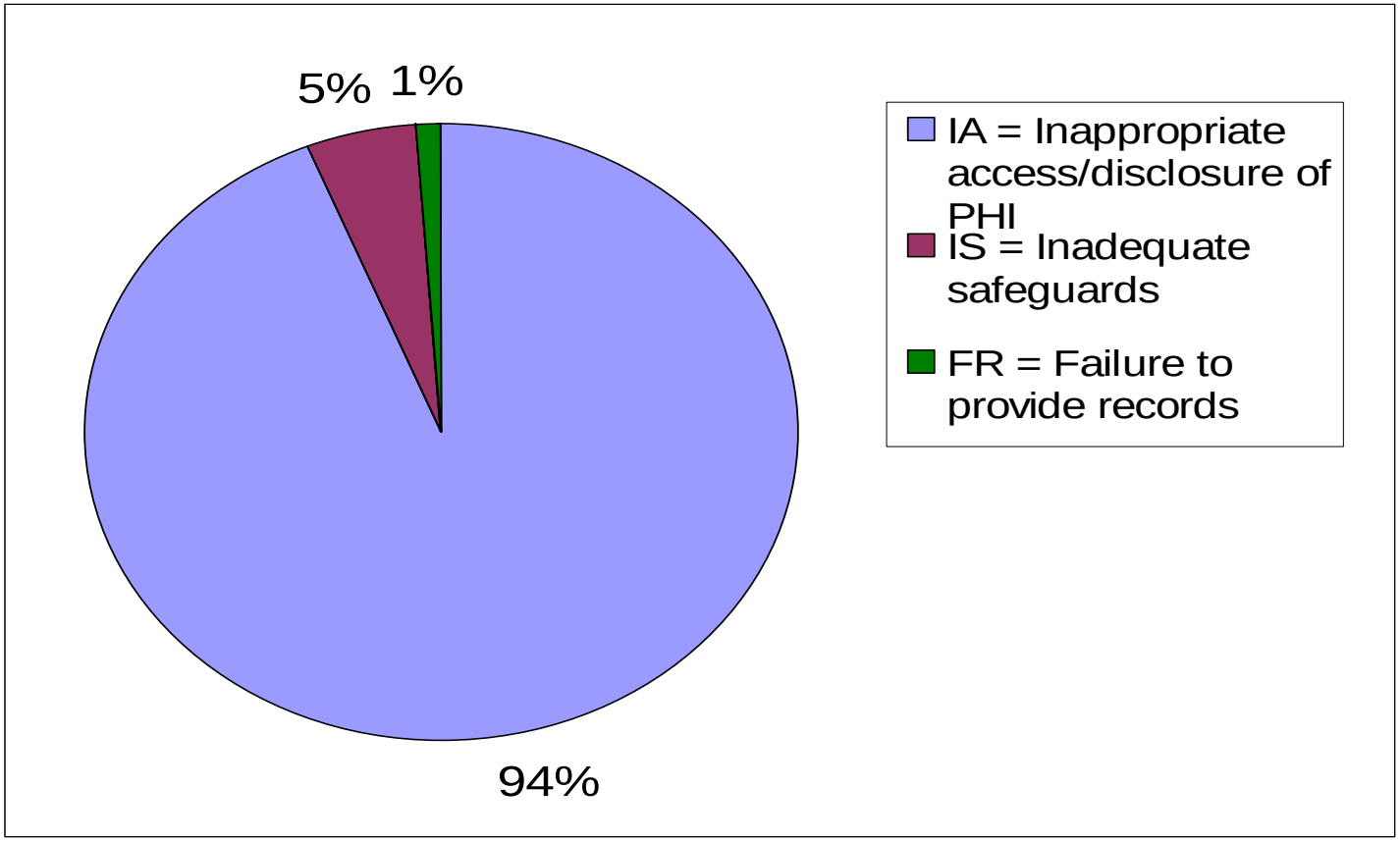
UMass Memorial's Experience

- UMass Memorial is the 2nd largest healthcare delivery system in Massachusetts
- System includes academic medical center with three campuses in Worcester, MA and four community hospitals
- System has a Chief Privacy Officer with privacy offices at all locations
- All locations insured through a captive – self insured for liability

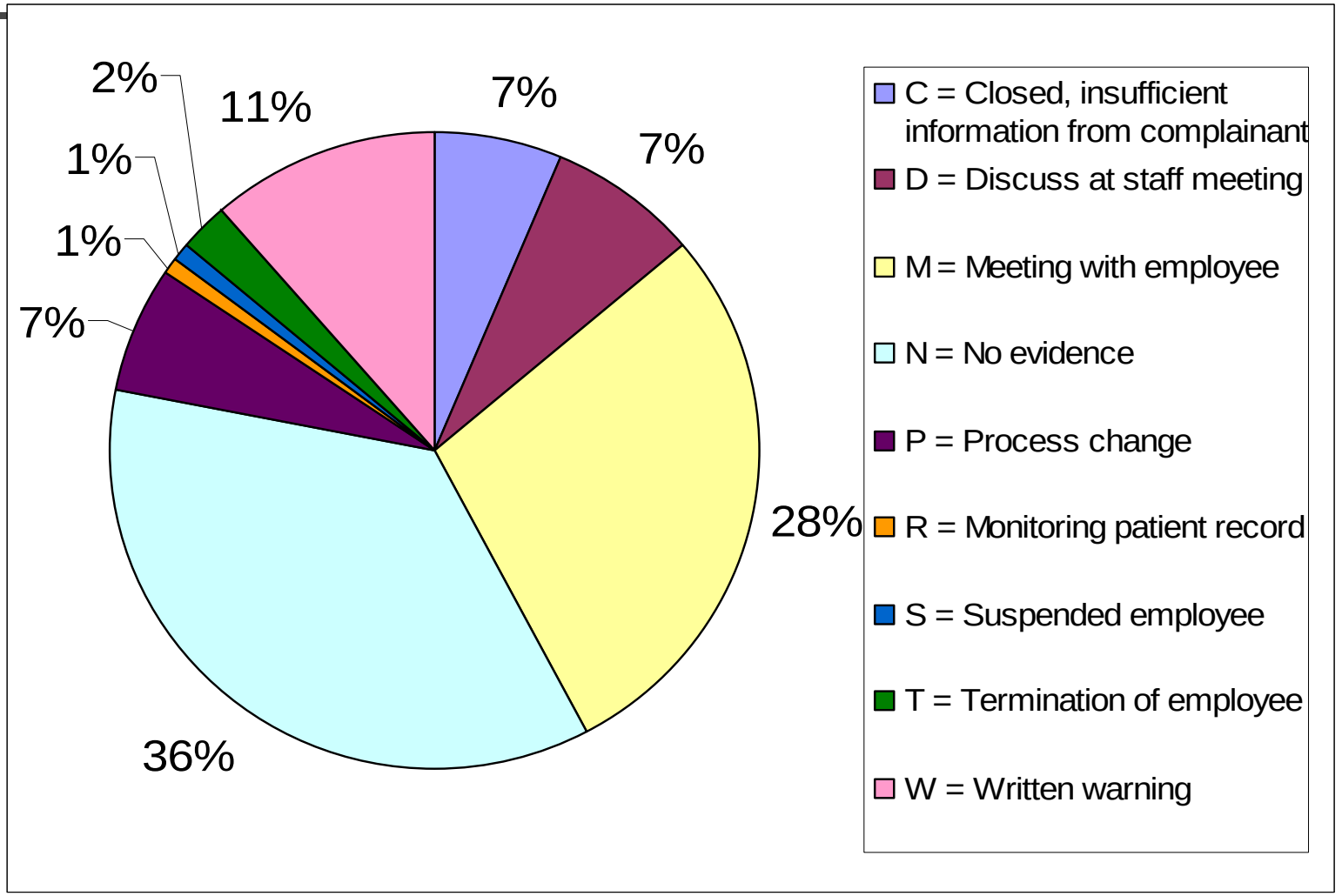
UMass Memorial Privacy Complaints - Annual Totals



UMass Memorial - 2007 Privacy Complaint Types



UMass Memorial - 2007 Privacy Complaint Resolution Types



UMass Memorial – Claim and Suit Experience

- 9 claims and suits since 2004
- 4 closed cases, 5 pending
- Closed cases – all settled
- 100% payment rate compares unfavorably with system. UMMHC typically closed 75% - 80% of claims and suits without payment
- Indemnity paid – approximately $200,000

UMass Memorial – Claim and Suit Experience

- Claims & Suits – mechanism for breach

  - Faxes - 2
  - E-mail/Internet - 1
  - EMR/MR - 5
  - Oral - 1

Event Management

Once a violation is reported/complaint made:

- Privacy Office initiates an investigation
- Investigative team is formed including representatives of HR, legal and claims as needed
- Written report is prepared
- Disclosure managed through Risk Management or Claims depending on circumstances

Event Management

- Disciplinary Action (Consistent with HR and Privacy Policies)
  - Retraining on privacy policies
  - Increased monitoring/surveillance
  - Verbal or written warning
  - Withdrawal of access
  - Suspension
  - Termination

Event Management

- Claim and Suit Management

- Once a formal claim is initiated, all investigation is coordinated by claims

- UMass Memorial chooses to accept this risk and to self insure it through our captive insurer as a professional liability claim – “medical records services”. We have been exploring risk transfer through a cyber liability policy

- Claims and suits presented to date have generally been “liability” cases

Event Management

- Claim and Suit Management
- Settlement Strategies
  - Disclosure/Early Offer
  - Mediation
  - Arbitration

Event Management

- Claim and Suit Management
  - Defenses raised
    - Adequate and appropriate training and orientation
    - Appropriate monitoring of employee
    - Intentional/Criminal Act by employee – potential to disclaim coverage
    - Limited/no damages

Loss Prevention

- UMass Memorial is developing a culture of Enterprise Risk Management
  - Risk Assessment Group composed of Senior Management and leaders of Risk Functions (Risk Management, Claims, Legal, Compliance, Internal Audit, Insurance)
  - Focus is on the identification and monitoring of most significant risks to organization
  - Examples include underperforming clinical services, financial controls at affiliate operations, IT infrastructure
  - Out of this effort has come the concept of “Risk Rounds” which include a discussion of a problem with appropriate case studies outlining issue, root cause of problem and contributing factors

Loss Prevention

- Risk Rounds
  - Privacy Risk Round presented to targeted departments and affiliate organizations
  - Examples - OB/GYN, billing, nursing – highlighting claim and suits from specific areas
  - UMass Memorial is seeking to move towards transparency and a decision has been made to use actual cases
  - Loss prevention strategies highlighted in case studies.

Privacy Case Study #1

Billing employee breaches confidentiality via improper access to EMR

Privacy Case Studies

- Incident – December 2004
- UMass Memorial billing employee became concerned about health status of an individual who provided child care services to her family
- UMM employee accessed child care worker's medical records via Meditech
- Obtained information that child care worker was being treated for an infectious disease

Privacy Case Studies

- Based on information obtained, UMM employee terminated the child care worker's employment
- In addition, the employee shared information concerning the child care worker with others in the community
- The child care worker sought representation from an attorney and a claim was filed within months of the breach

Privacy Case Studies

The Aftermath

- The employee was terminated after an investigation confirmed inappropriate access
- A complaint was made to the Office for Civil Rights
- The claim was settled for in excess of $140,000
- UMass Memorial absorbed significant costs for hiring a replacement employee and retraining staff on privacy issues

Privacy Case Studies

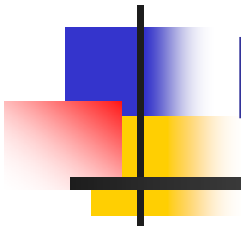
Root Cause of Problem

- Employee valuing perceived family responsibility higher than the duty to maintain confidentiality as a job responsibility/duty to UMass Memorial. This further caused the employee to use poor judgment in making an intentional and inappropriate access to the patient's PHI.

Privacy Case Studies

Contributing Factors

- Lack of periodic emphasis and retraining on privacy issues for department after initial orientation.
- Inadequate restriction of access to information. Employee had access to PHI beyond that needed for performance of duties.
- Lack of oversight and routine audit of employee activities that would have revealed improper access earlier. Missed opportunity for “damage” control.
- Inability of privacy training to account for cultural and family concerns that impact an employee’s ability to maintain confidentiality.



Privacy Case Study #2

Secretarial employee breaches confidentiality by disseminating information from “paper” record

Privacy Case Studies

- Incident – October 2004
- UMass Memorial secretarial employee became aware that a family friend had been diagnosed with a cancer when the patient scheduled a surgical appointment
- Access to PHI was via the “paper” record, including a biopsy result

Privacy Case Studies

- UMM employee disseminated information concerning cancer diagnosis via e-mail to others who knew patient
- The patient became aware of breach when she received phone calls expressing concern for her welfare
- The patient sought representation by an attorney and a claim was filed within weeks of the breach

Privacy Case Studies

The Aftermath

- The employee was disciplined after an investigation
- A complaint was filed with the Office for Civil Rights
- The civil claim could not be resolved due to the patient's anger, and a lawsuit was filed
- Eventually, the case was arbitrated, with a finding for the patient in excess of $50,000. Given protracted litigation, the defense costs exceeded $40,000

Privacy Case Studies

Root Cause of Problem

- Employee willfully ignoring training and office protocol in light of empathy and concern for a friend. This concern caused the employee to use poor judgment in disseminating protected health information via e-mail

Privacy Case Studies

Contributing Factors

- Lack of periodic emphasis and retraining on privacy issues for department after initial orientation
- Lack of office manager oversight concerning e-mail usage
- Inability of privacy training to account for family concerns and individual employee emotions that impact an employee's ability to maintain confidentiality

Privacy Case Study #3

Resident physician breaches confidentiality by improperly accessing EMR of his estranged wife

Privacy Case Studies

- Incident – April 2007
- UMass Memorial physician was involved in a divorce proceeding. On a number of occasions, the Meditech record for the physician's spouse and child were accessed
- Access to PHI was presumably for use during the custody proceedings for the minor child

Privacy Case Studies

- The patient was represented by counsel for divorce proceedings and became aware of the breaches through the court proceedings
- A subpoena was issued for UMass Memorial and a complaint was made
- The attorney representing the patient is considering legal options at this time

Privacy Case Studies

The Aftermath

- The involved physician was disciplined after an investigation determined inappropriate access
- The physician's actions negatively impacted his custody fight
- UMass Memorial has expended several thousand dollars in legal fees to respond to subpoenas
- There is the potential for a claim or suit

Privacy Case Studies

Root Cause of Problem

- Physician willfully ignoring training in light of his anger at spouse over custody battle. This anger and frustration caused the employee to use poor judgment in accessing protected health information in Meditech, and attempting to use it during the court proceedings

Privacy Case Studies

Contributing Factors

- Lack of periodic emphasis and retraining on privacy issues for physicians after their initial orientation
- Lack of supervision and support for physician during the difficult divorce proceedings
- Inability of privacy training to account for family concerns and individual employee emotions that impact an employee's ability to maintain confidentiality

Privacy Case Study #4

Billing employee commits identity theft by obtaining SS# from EMR and using it to commit fraud

Privacy Case Studies

- Incident – February 2005

- UMass Memorial billing employee accessed the PHI of a patient with her same name, and stole this individual's identity
- Access to PHI was via Meditech and billing databases the employee used in their billing activities
- The employee opened a credit card account in the name of the patient and made purchases

Privacy Case Studies

The Aftermath

- A complaint was made to UMass Memorial via the Patient Representatives
- The billing employee was suspended and an investigation was undertaken. She resigned voluntarily when faced with termination
- The patient retained and attorney and a suit was brought.
- Given the criminal activity, the billing employee is without insurance to cover the expenses associated with the suit

Privacy Case Studies

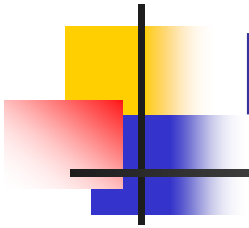
The Aftermath

- The investigation has shown the employee was appropriately trained, supervised and monitored, yet still breached patient confidentiality
- The employee faced legal action by the district attorney's office for identity theft
- UMass Memorial will likely have to expend thousands of dollars in legal fees to respond on behalf of the institution

Privacy Case Studies

Root Cause of Problem

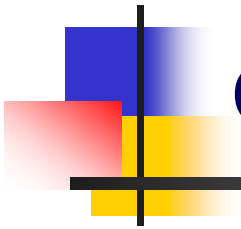
- Employee willfully ignoring training and office protocol and accessing PHI for dishonest purposes. The employee used poor judgment in committing a dishonest act.



Privacy Case Studies

Contributing Factors

- Lack of periodic emphasis and retraining on privacy issues for employees after their initial orientation
- Inability of privacy training to account for employee financial concerns and individual employee's dishonesty



Questions?