



**MENTiSOFTWARE**  
SECURITY • COMPLIANCE • BEST PRACTICES

# State Privacy Laws

## MANAGING COMPLIANCE FOR SENSITIVE DATA

October 29, 2010

# Agenda

- **Understanding State Privacy Laws**
- **The Impact of Non-compliance**
- **What are your Options?**
- **MENTIS Sensitive Information Management™**
- **About MENTIS**
- **Summary/Q&A**



# Understand State Privacy Laws

# What are the Laws Meant to Protect?

- **Personal Information (aka - Personally Identifiable Information or PII)**

- Name
- Address
- SSN
- Birth Date
- Driver's License # (or State issued ID card #)
- Account #, Credit/ Debit Card #, Bank Account #, etc..

- **Breach**

- Unencrypted Data
- Unauthorized Access
- Including IT resources



# Recent State Privacy Laws

- **California Security Breach Notification Law (SB 1386)**
  - ➔ First of its kind in the U.S. (2003)
  - ➔ 46 states, the District of Columbia, Puerto Rico and the Virgin Islands now have laws on breach notification
- **Connecticut Privacy Law (SB 5658)**
  - ➔ Requires companies create and make public a privacy protection policy
  - ➔ Signed into law in 2008
- **Massachusetts Data Protection Law (MA 201 CMR 17)**
  - ➔ Furthers definition of PII and All to combination
  - ➔ Codifies PCI

*There's a domino effect for privacy laws – pay attention even if you don't do business in that particular state*



# What exactly are the guidelines?

## Massachusetts law requirements-

<b>Written Information Security program</b>	<b>Manual</b>
<b>Designate responsible employees</b>	<b>Manual</b>
<b>Identify internal &amp; external risks and evaluate effectiveness of current safeguards</b>	<input type="checkbox"/>
<b>PII Related employee policies</b>	<b>Manual</b>
<b>Disciplinary Measures</b>	<b>Manual</b>
<b>Prevent Access</b>	<input type="checkbox"/>
<b>Verify third-party compliance</b>	<input type="checkbox"/>
<b>Limit collection, retention and use of PII</b>	<input type="checkbox"/>
<b>Identify locations of PII</b>	<input type="checkbox"/>
<b>Restrict Access</b>	<input type="checkbox"/>
<b>Conduct regular monitoring &amp; annual reviews</b>	<input type="checkbox"/>
<b>Document actions</b>	<input type="checkbox"/>



# Who Does it Effect?

- **MA 201 CMR 17.00**
  - Store or Collect electronic information
  - Residents of the Common Wealth
- **Relationship does not matter**
  - Employee/ Employer
  - Customer/ Vendor
  - Constituent/ Government
- **Geography does not matter**
  - Personal information is what matters
  - Outsourcing
  - Off shoring



# STATE LAWS:

## The Impact of Non-Compliance

# Our View of Compliance has Changed

- Compliance is now the 'Minimum Standard'
- Compliance needs to be attained (and more)
- It's not about just getting the checkmark anymore
- Bottom line:
  - You need to go above and beyond compliance or risk significant exposures



# Fines and Penalties

- **California Security Breach Notification Law – SB 1386**
  - Cost to notify each person of breach
  - Lost business
  - Uncapped civil suit
- **Connecticut Privacy Law - SB 5658**
  - Civil penalty of \$500 for each violation
  - Up to \$500,000 for any single violation
- **Massachusetts Privacy Law - 201 CMR 17.00**
  - Up to \$50,000 per incident of improper record disposal
  - Attorney General may order an audit typically costing \$150,000
  - Courts can order punitive damages if there was negligence



# Data Breaches In the News...

- **Health Net**

- Settled lawsuit by CT Attorney General for \$250,000 and enter a corrective action plan and must pay an additional \$500,000 if the data is misused
- Over \$7 million in direct expenses so far

- **Yale Medical School**

- Approximately 1,000 individuals effected
- CT Attorney General is investigating breach
- Estimated direct cost - \$60,000 (does not include legal costs)

- **Heartland Payment Systems**

- Over 130 Million records breached
- Accrued \$139.4 million in expenses (\$26 million in legal fees)



# Data Breach Cases are Climbing

## WHO IS BEHIND DATA BREACHES?

**70%** resulted from external agents (-9%)

**48%** were caused by insiders (+26%)

**11%** implicated business partners (-23%)

**27%** involved multiple parties (-12%)

Source: Verizon – 2010 Data Breach Investigations Report



# All this Leads to...



**compliance  
rage?**



# What are your Options?

# What companies are doing today...

- **Rely on technology and application providers**
- **Custom/Manual Efforts**
- **Pay as you go Approach (Event-based audit and compliance reporting)**
- **Targeted Security/Compliance Solutions**



# Oracle Database and Applications Security

- PeopleSoft Security
- GRC Modules
- Oracle Database Vault, Audit Vault, Advanced Security and Data Masking Pack

**There are many tools but not integrated, requiring a lot of independent implementations. This makes it difficult to get a complete picture**



# Custom/Manual Efforts

- Heavy reliance on database scripting and manual efforts
- Need to gather and document sensitive data locations
- Separate scripts and reports to mask data in non-production databases and respond to audit/security requests
- Issues: Error prone, no automation or strict enforcement



# Pay as you Go Approach

- **Limited or no upfront investment**
- **Respond to audit and security requests on an ad hoc basis**
- **Need to ramp-up resources for the effort- stage databases, write reports**
  - Requires technical resources and domain expertise
- **Much more expensive in the long run. A single event can potentially drain resources from their daily activities.**



# Security/Compliance Solutions

- **Purpose-built solutions in the marketplace**
- **Add value to underlying application and database security**
- **Automation of security and compliance activities**
- **Upfront investment can pay for itself within a year**



# What's Next?

# Solution Requirements

A roadmap to compliance

**Challenge**

**Solution**

What is sensitive?

**Data Classification**

(Name, SSN, CC,,...)

Where is it stored?

**Discovery**

(Documented & Undocumented locations)

How is it exposed?

**Code Catalog**

(Application & DB Source Code)

Who has access?

**Access Review**

(Application & Database Access)

How to Protect?

**Access Control, Masking, Monitoring**

ASSESS

REVIEW

REMEDIATE

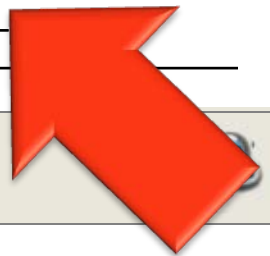
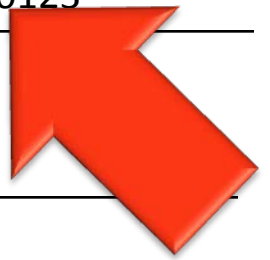
# Data Discovery is Critical

## USUAL/KNOWN/ DOCUMENTED Locations

Module	Table	Column	Data
HR	PER_ALL_PEOPLE_F	NATIONAL_IDENTIFIER	345-67-8901
AR	AR_CUST_TRX_ALL	CARD_NUMBER	4567-1234-6789-0123

## UNUSUAL/ UNKNOWN/ UNDOCUMENTED Locations

Module	Table	Column	Data
AP	AP_BANK_ACCOUNTS_ALL	DESCRIPTION	345-67-8901
CUST	MEX_KITCHEN	TX32	345-67-8901
HR	PER_ALL_PEOPLE_F	LAST_MEDICAL_TEST_BY	345-67-8901
CUST	MEX_KITCHEN	TX07	4567-1234-6789-0123
AUDIT	AUDIT_TRAIL	COLUMN_VALUE	4567-1234-6789-0123
AP	AP_INVOICES_ALL	DESCRIPTION	4567-1234-6789-



# MENTIS Sensitive Information Management™

# Solution Requirements

A roadmap to compliance

Challenge

Solution

**MENTIS**

What is sensitive?

**Data Classification**

(Name, SSN, CC,,...)



Where is it stored?

**Discovery**

(Documented & Undocumented locations)



How is it exposed?

**Code Catalog**

(Application & DB Source Code)



Who has access?

**Access Review**

(Application & Database Access)



How to Protect?

**Access Control, Masking, Monitoring**



ASSESS

REVIEW

REMEDiate

# MENTIS – How We Do It



DISCOVER

PROTECT

MANAGE

Sensitive Information Management™ Platform

- **Discover** and classify all sensitive data locations, including user and program level access
- **Protect** sensitive data by masking/scrambling at application and database levels
- **Manage** database and application environments through regular auditing, monitoring and reporting
- **Repeat** process to keep up with changing legislation & requirements for sensitive data



# Lessons learned

Don't try this manually!

- **Manual processes do not scale**

- Applications & Databases too complex
- Large volumes of data/ processes/ code
- Upgrades/ Patches

- **Compliance is not one-time**

- This is an on-going mandate
- Evolving legislative landscape
- Not just Mass; Impending Federal

- **Collaboration is difficult**

- Most core functions are too technical
- Very little non-IT insight into processes possible
- Hard to document and prove

## How Long?

- **Manual: 3-4 months**
- **Resources - ??**



# Benefits of the MENTIS approach

## Proven method

- **Automated**

- With built-in metadata and data-classifications
- Sensitive Data Discovery
- Pre-configured for Oracle EBS and
- Customizations discovered automa

- **Repeatable & Scalable**

- Keep ahead of legislative or mandate changes
- Comply today, and scale for tomorrow

- **Collaboration is essential**

- Data Classifications bridge the language gap
- Independent review and sign-off on processes and protections
- Audits will become a breeze

**How Long?**

**• Approach: 2-3 weeks**



# About MENTIS

# About MENTIS...

## Our Purpose

- Founded by Database, GRC and Audit experts
- Visionary - Rajesh Parthasarathy
- Early to market with 'masking' point solution for PeopleSoft

## The Problems we Solve

- Corporate databases and applications are constantly evolving and must have regular discovery and security reviews
- Sensitive data requires ongoing management from an audit, compliance and access perspective

## Our Solution

- Comprehensive suite of products for managing sensitive information across enterprise applications & databases

## Our Reach

- Brand name customers worldwide – across a variety of industries
- Multiple resellers and implementation partners including HP, 3i Infotech



# Summary/Q & A

# MENTIS – Automating Your Compliance Efforts

Mass law requirement	MENTIS Coverage
Written Information Security program	Manual
Designate responsible employees	Manual
Identify internal & external risks and evaluate effectiveness of current safeguards	✓
PII Related employee policies	Manual
Disciplinary Measures	Manual
Prevent Access	✓
Verify third-party compliance	✓
Limit collection, retention and use of PII	✓
Identify locations of PII	✓
Restrict Access	✓
Conduct regular monitoring & annual reviews	✓
Document actions	✓



# Thank you!