

# 2011 CIO ROUNDTABLE RETREAT

## Architecting Our Future

March 6 – 8, 2011

*The Arizona Biltmore*  
*Phoenix, Arizona*

*eSentio*  
Technologies



# Records Management - Local and Global Challenges

*Presented by Bob Dolinsky*

eSentio  
Technologies



# Records Management Requirements and Compliance – What a Maze!

HIPAA - HITECH

Ethical  
Walls

AML

SARBANES-OXLEY ACT

Legal Holds

Retention  
Schedules

Privacy Laws

IRS

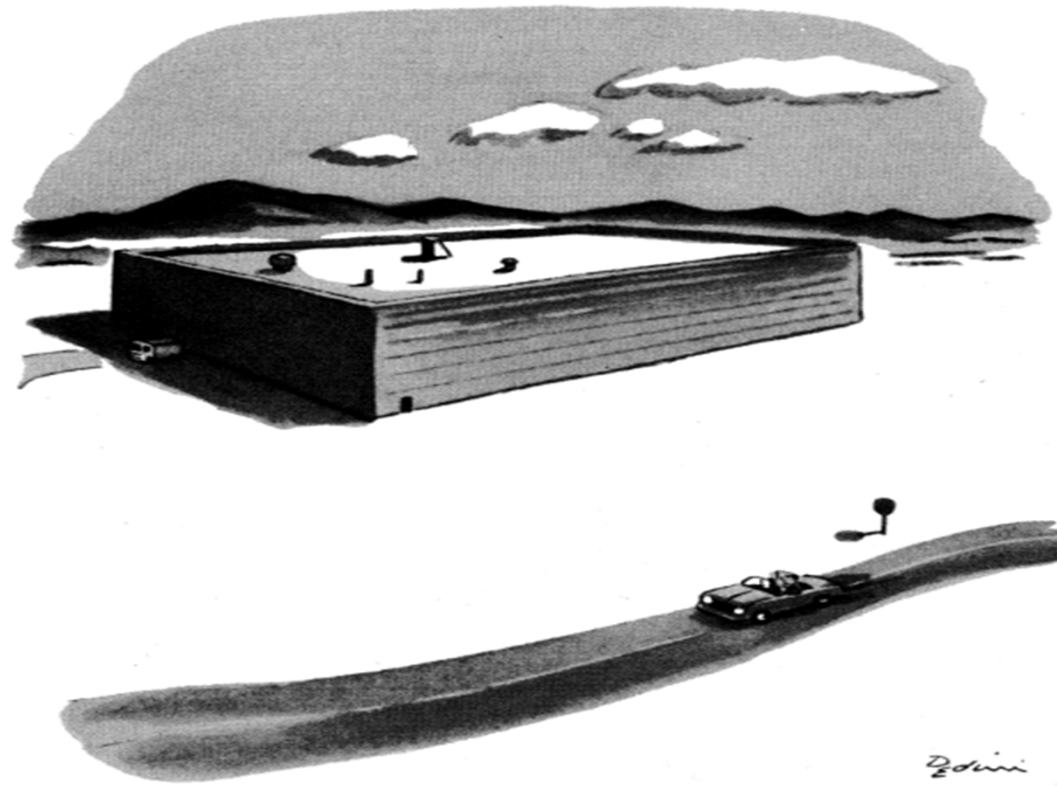
File Preservation



# Many Law Firms Have Not Implemented a Record Retention Plan



# Many Law Firms Have Not Implemented a Record Retention Plan and Records are Only Growing



*"That, my son, is where they store all the minutes  
of all the last meetings."*



# Records Management Challenges

- Attorney Mobility
- Compliance Issues
  - Global
  - Local
- Social Networking
- More Focus on Risk Management
  - Clients
  - Insurance Carriers



# Records Management Challenges

- Cloud Computing
- Storage Options



# Key Policy Components

- Retention
- Email
- Client Notification



# Key Policy Components

- Lawyers joining the Firm
- Departing lawyers
- Matter closing
- Governance



# ALAS Recommendations

- Only retain business records
  - Examples of non-business records; duplicates, drafts, and transient emails
- Establish and use standard folder structure
  - Apply to both paper and electronic files
- Develop a Records Retention Schedule



# ALAS Recommendations

- Implement email filing guidelines
- Apply Records Retention rules to email
- Close files at the conclusion of a matter
- Develop policies and procedures to enable legal holds



# Global Compliance Challenges – EU Privacy



# EU Data Privacy - Overview

- **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.**



# EU Data Privacy - Overview

- Unlike the United States, the European Union has addressed privacy and data protection in a much more rigorous way, primarily through Directive 95/46/EC. This Directive covers the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Data Protection Directive is made effective in each EU member state through implementing legislation such as the Data Protection Act in the UK. A U.S. firm operating in the EU will likely fall under the scope of the Data Protection Directive, which restricts the cross-border transfer of personal information.



# EU Data Privacy - Overview

- 'Personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- *Third countries* is the term used in EU legislation to designate countries outside the European Union. Personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.
- The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbor Principles were the result.



# EU Data Privacy - Overview

- The European Commission admits that its Data Protection Directive is outdated and is currently reading industry responses to a consultation before reviewing the law.
- Expected update in late 2011
- ABA is also looking at changes



# EU Data Privacy – What Is Covered

- Personal Data
- Litigation Discovery Materials
  - If it includes personal data
- If it includes nonpublic company information
  - Switzerland
  - Italy



# EU Data Privacy – Data Quality Principles

- Fairness
- Specific purpose
- Restricted
- Accurate
- Destroyed when obsolete
- Security
- Automated processing



# EU Data Privacy – How to Address

- Law Firms Can Deal with the Transfer of Data in Two Ways
  - Safe Harbor Certification – FTC – the US Side of the Firm promises to meet EU Data Privacy Requirements
  - Contractual Agreement Between Both Sides of the Data
    - Specific Contracts Are Prescribed – Model Forms
    - Agreements Must Be Filed With The EU
    - More Challenging Than Safe Harbor
      - Takes 30 Days to 4 Months
    - Better Approach if Data Will Be Transferred or Used Outside of the US (and EU) – A Real Issue in Global Firms



# EU Data Privacy – Safe Harbor Principles

These principles must provide:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.



# EU Data Privacy – US Safe Harbor Certification

- File Forms with the FTC
- After opting in, an organization must re-certify every 12 months. It can either perform a self-assessment to verify that it complies with these principles, or hire a third-party to perform the assessment. There are also requirements for ensuring that appropriate employee training and an effective dispute mechanism are in place.
- The Federal Trade Commission theoretically oversees this program but, to date, no company's procedures have been challenged as failing to meet these guidelines



# EU Data Privacy – US Safe Harbor Certification

- For “Safe Harbor” Protection, the Organization Must:
  - Subject itself to jurisdiction of the Federal Trade Commission (“FTC”)
  - Revise or create a privacy policy in compliance with the safe harbor principles
  - Publicly disclose its privacy policy
  - Unambiguously and publicly disclose its commitment to comply with the safe harbor principles



# EU Data Privacy – Enforcement

- No EU sanctions re Law Firms – but some in the EU have pushed for sanctions against a law firm in at least one situation
- At least one sanction against a US Corporation - Tyco
- Ongoing investigations re Facebook and Google
- No FTC enforcement to date



# One Example - HRIS

- **Consent:** Collecting "unambiguous" and "freely given" employee consents (although consents in the employment context are void in many EU countries as presumptively coerced)
- **Safe harbor:** Self-certifying under the EU/US Department of Commerce "safe harbor"
- **Model contracts:** Entering one of the EU-Commission-approved "model contractual clause" contracts
- **"Anonymize":** Sidestepping the data laws by completely "anonymizing" data (using employee ID numbers is not enough, so true "anonymization" is rarely practical in the HRIS context)



# EU Data Privacy – Other Issues

- Cookies
- Unsolicited Communications



# Other Compliance-Related Resources

- OFAC – Office of Foreign Assets Control
  - Commonly referred to as the ‘Terrorist Watch List’
  - [www.treas.gov/offices/enforcement/ofac/sdn/](http://www.treas.gov/offices/enforcement/ofac/sdn/)
- United Nations Security Council Resolution 1267
  - Individuals associated with: Al Qaida, Osama Bin Laden, and Taliban
  - [www.un.org/sc/committees/1267/consolist.shtml](http://www.un.org/sc/committees/1267/consolist.shtml)
- Directorate of Defense Trade Controls
  - Debarred Parties list of individuals who have been convicted of violating or conspiracy to violate the Arms Export Control Act (AECA)
  - [www.pmdotc.state.gov/compliance/debar.html](http://www.pmdotc.state.gov/compliance/debar.html)



# Other Compliance-Related Resources

- Bank of Canada
  - Suppression of Terrorism List
  - Similar to the Patriot Act in the U.S.
  - [www.osfi-sfif.gc.ca/osfi/index\\_e.aspx?ArticleID=524](http://www.osfi-sfif.gc.ca/osfi/index_e.aspx?ArticleID=524)



# Anti Money Laundering (AML)

- Resources
  - Bureau of Industry and Security (US Dept of Commerce)
    - Denied Persons List
  - Bank of England (Financial Sanctions Unit)
    - Consolidated List of financial sanctioned targets
  - World Bank (fraud and corruption policy)
    - Listing of Ineligible firms and individuals



# Other Compliance Considerations

- 30+ states have enacted privacy laws so far
- Massachusetts (201 CMR 17.00)
  - Data elements containing
    - SS#
    - Drivers License
    - Financial and/or credit card #'s
  - Encryption
  - Access Control
- **Health Information Technology for Economic and Clinical Health (HITECH) Act (2009)**
  - Law firms who handle health-related information are now bound by the same HIPAA security and privacy guidelines as healthcare providers.



# Discussion

