

THE POWER OF EXPERIENCE

GOVERNANCE RULES FOR E-DISCOVERY: BEING PROACTIVE

Presented by
Fred V. Diers
Director

Governance, Risk & Compliance Practice

www.judge.com

fdiers@judge.com

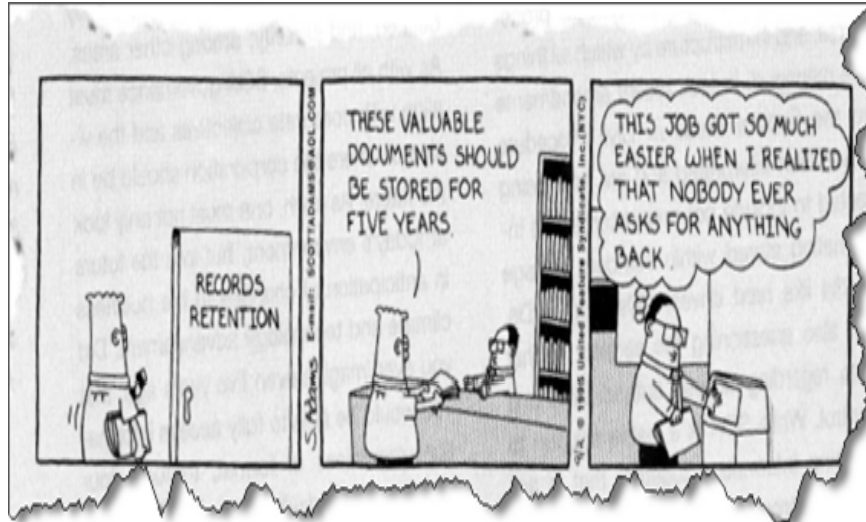


RESULTS THROUGH THE POWER OF EXPERIENCE

Topics Covered

- Being Reactive or Proactive to E-Discovery
- Identifying external impacts on organizations resulting in change management
- Determining 'compliance' reality
- Clarifying the Governance Package scope
- Developing the package
- Implementing the program





Reactive vs. Proactive

E-Discovery reactive response results from lack of information knowledge due to:

- Traditional in-house counsel attitude of settling out of court
- Confidence of paper repositories are in order and accessible
- IT responsiveness in producing desired data without regard to wasted resources
- Confidence in search tools to 'crawl' through data repositories without regard to amount of data, number of repositories and cost of review



Reactive vs. Proactive

E-Discovery reactive response leads to:

- Engaging forensic firms to compile index data from tapes, image hard drives on laptops and home computers, and provide results to counsel
- Employing e-mail journaling to capture all incoming and sent e-mails creating duplicate repositories that may conflict with country privacy laws
- Necessitating counsel to review mountains of extraneous data charging large hourly fees dramatically increasing the cost of production
- Once a set of electronic information is produced, a copy of that data must be preserved until all appeals are adjudicated which could be decades



Reactive vs. Proactive

E-Discovery proactive response leads to:

- Collaboration between IT, Legal, and Records Management
- Knowledge of the number of data repositories
- Knowledge of external factors impacting the business
- Sound and auditable enterprise compliance rules
- Effective information volume reduction programs
- Realistic hold order policy integrated with information compliance rules
- Accessibility to information through classification standards
- Employing the right information tools



External Factors

Since 2002, 4 major events have caused organizations to refocus on the need for compliant information controls:

- HIPPA
- SOX
- Federal Rules of Civil Procedures
- Government bailouts (TARP)

The days of de-regulation are over!!!



External Factors

Management has been looking for someone to assist with addressing external factors and implementing compliant solutions including:

- IT
- Legal
- Technology Vendors
- External Consultants
- Records Managers



Today's E-Discovery Objectives

- To implement a compliant and flexible governance program for staff and business unit's document handling and preservation processes
- To enable enterprise knowledge of and access to electronic and physical records today and in the future
- To reduce information volumes ensuring preservation of complete and trustworthy records



Today's E-Discovery Objectives

- To ensure records' chain of custody from creation through disposition
- To control information duplication, processing and storage
- To work with IT to develop processes for preserving and accessing electronic records with long retention periods
- To work with IT to dispose of electronic records



Governance Enterprise Rules

The foundational enterprise rules:

- Records Management Policy
- Retention Schedule
- Electronic Messaging Policy
- Hold Order Policy
- Enterprise and local information processing procedures



Governance Functional Rules

Organization specific rules can include:

- Inactive Media Policy (Back-up tapes)
- Legacy Data Retention Policy
- Acquired or Dissolved Business Unit Retention Policy
- HR Personnel Records Privacy Policy
- Records Security and Archive Policy

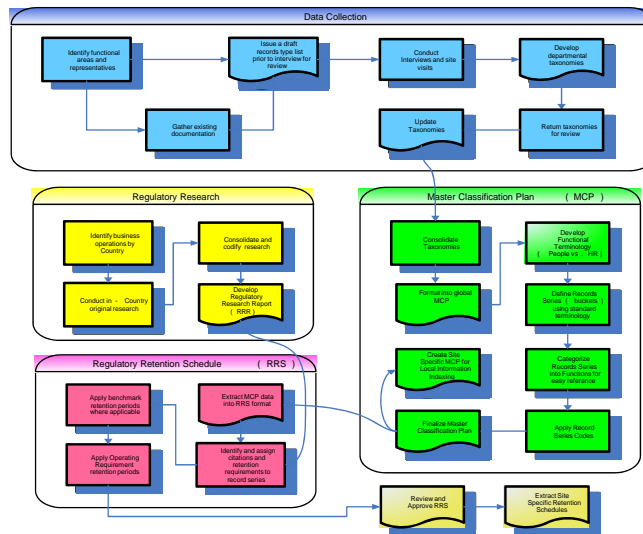


Records Management Policy

- Policy defines life cycle of all information regardless of media or type.
(No longer is there a differentiation between record or non-record or data versus document versus record)
- Policy defines governing body oversight responsibilities
- Other information governance policies and procedures link with the Records Management Policy and retention schedule



Retention Schedule



Retention Schedule

- First step is researching government regulations that impact the business
 - Original Research not hearsay
- International research includes:
 - Countries that the organization conducts business
 - Local regulations requiring original records retained in-country
 - Privacy requirements
 - Treaty requirements (e.g. EU, WHO, etc.)



Judge Consulting Group Retention Regulatory Research Report

Source Title: Aliens and Nationality, Immigration and Nationality, Immigration, General Penalty Provisions, Unlawful employment of aliens; Employment verification system
United States Code

Citation: 8 U.S.C. 1324a(b)(1)
Impacted Industries: General

Quotation:
The requirements referred to in paragraphs (1)(B) and (C) of subsection (a) of this section are, in the case of a person or other entity hiring, recruiting, or referring an individual for employment in the United States, the requirements specified in the following three paragraphs: (1) Attestation after examination of documentation (A) In general - The person or entity must attest, under penalty of perjury and on a form designated or established by the Attorney General by regulation, that it has verified that the individual is not an unauthorized alien by examining - (i) a document described in subparagraph (C) and (ii) a document described in subparagraph (D). Such attestation may be manifested by either a hand-written or an electronic signature. A person or entity has complied with the requirement of this paragraph with respect to examination of a document if the document reasonably appears on its face to be genuine and that is sufficient to meet the requirements of the first sentence of this paragraph, nothing in this paragraph shall be construed as requiring the person or entity to solicit the production of any other document or as requiring the individual to produce such another document. (2) Documents establishing both employment authorization and an identity. A document described in this subparagraph is an individual's - (i) United States passport; (ii) resident alien card, alien registration card, or other document designated by the Attorney General, if the document - (I) contains a photograph of the individual and such other personal identifying information relating to the individual as the Attorney General finds, by regulation, sufficient for purposes of this subsection, (II) is evidence of authorization of employment in the United States, and (III) contains security features to make it resistant to tampering, counterfeiting, and fraudulent use. (3) Documents evidencing employment authorization - A document described in this subparagraph is an individual's - (i) social security account number card (other than such a card which appears on the face that the issuance of the card does not authorize employment in the United States) or (ii) other documentation evidencing authorization of employment in the United States which the Attorney General finds, by regulation, to be acceptable for purposes of this section. (4) Documents establishing identity of individual - A document described in this subparagraph is an individual's - (i) driver's license or similar document issued for the purpose of identification by a State, if it contains a photograph of the individual or such other personal identifying information relating to the individual as the Attorney General finds, by regulation, sufficient for purposes of this section; or (ii) in the case of individuals under 16 years of age or in a State which does not provide for issuance of an identification document (other than a driver's license) refers to in clause (i), documentation of personal identity of such other type as the Attorney General finds, by regulation, provides a reliable means of identification. (5) Authority to prohibit use of certain documents - If the Attorney General finds, by regulation, that any document described in subparagraph (B), (C), (D) as establishing employment authorization or identity does not reliably establish such authorization or identity or is being used fraudulently to an unacceptable degree, the Attorney General may prohibit or place conditions on its use for purposes of this subsection.

Impacted Records:	Record Retention:	Special Instructions:
Citizenship verification form - in the case of the recruiting or referral for a fee (without hiring) of an individual	Date of the recruiting or referral + 3 years [Refer to 8 U.S.C. 1324a(b)(3)]	
Citizenship verification form - in the case of the hiring of an individual	Longer of hire date plus 3 years or termination plus 1 year [Refer to 8 U.S.C. 1324a(b)(3)]	



Retention Schedule

Consolidating codified information into an enterprise retention schedule listing:

- Classification standards (Record Series) with definitions and sample record types
- Media and record designation (vital, historical, GxP, SOX, etc.)
- Copy and official retention periods
- Applicable regulatory citations
- Records custodians



Retention Schedule

- Format structure for mapping to ECM software tables
- Publish a retention schedule quick reference guide
- Create local schedules linking to the enterprise retention schedule



Electronic Messaging Policy

- Defines the scope of information that are saved via E-mail, Instant Messages, PDA's, Voice Over IP, Blogs, etc.
- Defines software used to Vault or Journal E-mails such as HP's Email Archiving© for Microsoft Exchange© or Symantec
- Defines the use or non-use of .pst or archive folders on personal hard-drives
- Sets retention policies for standard folders (in-box, sent items, etc.)



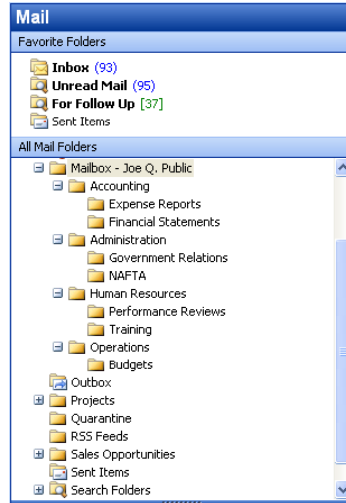
Electronic Messaging Policy

- Sets content based preservation standards for utilization with ECM or E-mail Vaulting Tools
- Provides content based folder structure using Function or Bucket organization
- Sets folder retention periods
- Provides auditable compliance practices



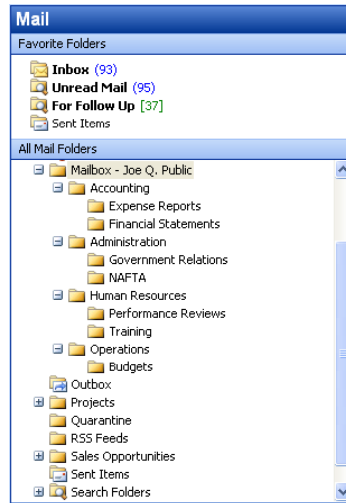
Electronic Messaging Policy

- Mailbox added folder structure:
 - Accounting 12 years
 - Administration 3 years
 - Human Resources 10 years
 - Operations 5 years



Electronic Messaging Policy

- Self auditing for e-mail deletion of PST's or local archives folders
- Messages not moved to a designated folder will be auto deleted as follows:
 - In-box 180 Days
 - Sent items 90 Days
- E-mails/attachments that associate with other electronic documents should be combined



Inactive Media Policy

- Defines the disaster recovery process for electronic data stored on servers including back-up tapes, replicated servers, or hosted hot sites
- Focuses on IT and the use of back-up as a disaster recovery requirement not a data store
- Addresses archive, and other IT interim or off-line data storage



Inactive Media Policy

- Sets minimal retention for back-up media (e.g. tapes as full, differential, daily and weekly backups)
- Incorporates retention into the overall retention periods for retained categories
- Eliminates restore requests from users
- Defines journaling versus vaulting avoiding duplicate storage and preserving privacy issues



Hold Order Policy

- Sets document preservation rules for ESI and physical records
- Defines format, scope, and responsibilities associated with litigations, audits or investigations
- Provides details on matter, date ranges, impacted personnel, and subject, and key search terms



Hold Order Policy

- Provisions release notification processes and reminders
- Identifies hold order management tools
- Conforms with the Federal Rules of Civil Procedure
- Identifies the organizations '30b6' witness



Program Implementation

Governance package roll-out strategy includes:

- Executive management commitment
- Change management
 - How data, documents, and records are used, disseminated, stored, and disposed
 - What is the media to preserve company records



Program Implementation

Governance package roll-out strategy includes:

- Ongoing program communication and education
- Performance rewards and penalties relating to adherence to the governance rules
- Technology identification facilitating conformance to program standards
- Compliance auditing



Program Benefits

- Reduces management decision processes
- Enables organization personnel access to needed information
- Provides sustainable information volume reduction
- Manages lifecycle of structured and unstructured information



Program Benefits

- Raises management's comfort level of ethical conformance to the rules
- Minimizes document handling burdens
- Decentralizes use and access of information by employing centralized standards
- Makes the Records Management program a core information function



QUESTIONS?

Fred V. Diers
Vice President
Governance, Risk & Compliance
Judge Consulting Group
www.judge.com

