Compliance Requirements for Record Retention

William Saffady

www.saffady.com

What you will learn

- What is compliance?
- What are the varieties of compliance requirements?
- What is their role in record retention?

What is Compliance?

- **Dictionary definitions**

- Merriam Webster**:** The act or process of doing what you have been asked or ordered to do
- Cambridge**:** The act of obeying an order rule or request
- Oxford: Practice of obeying rules or requests made by people in authority

- **Some synonyms**: agreement, assent, concurrence, conformity, consent, obedience, observance

- **Antonym**: noncompliance

Varieties of Compliance for Record Retention

- Legal and regulatory requirements
- Contractual requirements
- Standards and norms
- Internal mandates
- Societal compliance

Legal and Regulatory Compliance

- Types of requirements
  - Minimum retention periods
  - Maximum retention periods
  - Destruction of confidential or sensitive information
  - Preservation of information that is relevant for litigation, government investigations, other legal proceedings.

Minimum Retention Periods

- All countries specify minimum requirements for records of common business functions – examples: business formation, accounting, taxation, employment
- Sector-specific recordkeeping requirements: banking, food processing, healthcare, insurance, pharmaceuticals, etc.
- Compliance is not negotiable but inadvertent noncompliance is possible
- Accurate identification of relevant requirements is a challenge
  - National
  - State
  - Local

Maximum Retention Periods

- Mandate destruction of information when retention period elapses
- Data protection and privacy laws best known examples
- Information must be destroyed when no longer needed for its original
- GDPR is vague about time limits
- But open to interpretation: personnel records example

Contractual Compliance

- Contractor creates and maintains records in the course of its work for contracting party
- Examples: outside counsel, third party administrators
- Some contracts specifically for recordkeeping – example: commercial record centers and cloud-based storage services.
- Contract may state that contracting party owns information that contractor creates or collects on its behalf
- If ownership is not addressed, contract may specify retention requirements that contractor must satisfy

Contractual Compliance

- Immediate destruction of information in contractor's possession, including backup copies and information held by subcontractors
- Return specific information to contracting party, subject to exceptions for legal reasons
- Transfer information to a third party
- Retain information for a minimum period of time
- Disposal method specified
- Noncompliance issues

Standards and Industry Norms

- No omnibus national or international standards for retention of information
- Retention requirements in specialized business or technical operations – Example: ISO 13485, ISO 10407
- Most standards discuss retention in a general way
  - Examples: ISO 15489, ISO 9001
  - Acknowledge importance but no compliance mandates
  - Retention decisions are left to organization that creates and maintains information

Standards and Industry Norms

- Examples of industry and professional norms that address record retention:
  - ABA Informal Opinion 1384—cautions against destroying certain client information
  - NAIC model regulation—insurance companies must keep policy records for 3 years after termination, claim records for 3 years after closure, declined underwriting files for CY+3 years
  - APA Ethics Code—psychologists must keep former clients' records long enough to facilitate provision of services later – 7 years for adults
  - AHIMA practice brief—keep medical records for minimum of 10 years from last encounter

Standards and Industry Norms

- Standards and norms present retention guidelines rather than requirements
- Useful as benchmark for best practice
- Do not specify disciplinary rules or penalties
- Have legal effect only in context of a contract
- Principal negative consequence is damaged reputation
- Not clear whether violations rise to level of professional misconduct or actionable offense

Internal Mandates

- Usually specified in retention schedule and associated policies and procedures
- Not limited to legal compliance; considers the operational and possibly scholarly value of information
- Government agencies must comply with archival legislation
- No comparable requirement for non-governmental entities
- Codes of conduct the basis for compliance mandate
- May be explicit or implied

Internal Mandates

- Infractions may be unintentional
  - Unaware of policies
  - Lack of training – retention schedules can be long, complicated, difficult to use
  - Reluctance to discard information due to uncertainty about future need
  - Retention action not a high priority
  - Electronic record purging seems less urgent than disposal of paper records

Internal Mandates

- Enforcement
  - Self-certification
    - Written attestation of compliance
    - May be managers or all record custodians
  - Audits
    - Focus on failure to destroy records with elapsed retention periods
    - May be performed by records manager, internal auditors, consultant, etc.
    - Problems and corrections discussed with record custodians and supervisors
    - Objective is to obtain compliance not punish noncompliance

Societal Compliance: Ethical Issues

- Retention decisions based legal or operational requirements may pose ethical challenges
- Some examples:
  - School district wants to destroy special education records to minimize offsite storage costs
  - Charity wants to retain donor records for future fundraising
  - Gastroenterology practice wants destroy patient records to facilitate move to smaller office
  - Company wants to destroy financial records to minimize discovery costs

Societal Compliance: Ethical Issues

- Ethical principles
  - Avoidance of harm
    - Well established in professional ethics--example: medicine, law
    - Stakeholder theory of business ethics—consider interest of all stakeholders
  - Principle of double effect
    - Action must be legal
    - Benefits to organization must outweigh the harm to other stakeholders
    - Sacrifice some benefits to minimize harm

Societal Compliance: Ethical Issues

- The benefit cannot result from intentional harm to another, or it must outweigh the harm
- The problem of preemptive destruction to reduce exposure to legal actions
- Not legally prohibited but principle of avoidance of harm applies
- Makes business sense but may harm plaintiffs in cases involving wrongful termination, employment discrimination, defective products, illegal competition
- Must consider principle of double effect to determine whether practice is justifiable

Societal Compliance: Environmental Requirements

- Data center operations are energy-intensive – storage accounts for much power consumption
- Energy demands for digital storage large and growing
- Indefinite retention of digital information incompatible with sustainability goals
- Green archiving: short retention periods and timely purging
  - Exception for records needed for scholarly or scientific research
  - Purge duplicate records as soon as possible
  - Data compression can reduce storage requirements

Questions and speaker contact information

Bill Saffady

wsaffady@saffady.com

Phone or text: 917 304 7922