ZASIO

Recordkeeping Compliance: Retention and Beyond

Alec T Pechota
Analyst / Licensed Attorney
Zasio Enterprises, Inc.

Jared Walker
Analyst / Licensed Attorney
Zasio Enterprises, Inc.

October 2015

Article

ZASIO

Recordkeeping Compliance: Retention and Beyond

As a core component of information governance (IG), records management is responsible for the systematic control of the creation, use, maintenance and disposition of a corporation's recorded information. At its foundation, a strong records management program must identify the legally-mandated recordkeeping requirements applicable to the corporation's business activities to minimize the risk of regulatory non-compliance. Failure to comply may result in both civil and criminal penalties as well as possible adverse determinations in litigation and regulatory investigations.

Both private and public entities alike are subject to jurisdictional laws and regulations. Recordkeeping mandates may apply to broad business functions such as human resources and accounting, and to industry specific activities such as banking, securities, pharmaceuticals and insurance. From a global perspective, five (5) common recordkeeping requirements emerge from the legal landscape. These include laws relating to retention, storage format, location, destruction and protection; each significant in the formation of compliant record retention policies and procedures.

Retention | Format | Location | Destruction | Protection

Generally Accepted Recordkeeping Principles®[1]

ARMA International developed the Principles to foster general awareness of information governance standards and principles. The Principles include: Principle of Accountability, Principle of Integrity, Principle of Protection, Principle of Compliance, Principle of Availability, Principle of Retention, Principle of Disposition and Principle of Transparency. The recordkeeping requirements discussed in this article touch on several of these areas including protection, compliance, retention and disposition.

Retention

The ARMA Principle of Retention succinctly states that an entity must "retain its information for an appropriate time, taking into account all operational, legal, regulatory and fiscal requirements, and those of all relevant binding authorities."[2] At the heart of effective records management is the determination of the period of retention driven by both legal mandate and the operational needs of the corporation.

Legal Requirements
Literally thousands of laws and regulations exist domestically and internationally that dictate how long various records must be kept. While most laws and regulations provide a "floor" (minimum retention time period), others provide an equally important "ceiling" (maximum time period a record may be kept)[3], often concerning records with privacy concerns.

In addition to providing time periods of retention, many laws specify an event "trigger," or point of time at which the required retention period begins. These triggers vary widely and may range from creation of the record, to a specified occurrence or event[4], to the end of the year in which the record is created, or to the expiration of a contract. Corporations must understand and be mindful of such triggers when calculating and fulfilling retention periods. For example, compare a requirement to keep a record for 5 years with a requirement to keep the record for 5 years after termination of employment. In the latter instance, the period of retention would clearly exceed 5 years in totality.

Operational Needs
After legal requirements are identified regarding the retention period of a record, a corporation must take into account its operational needs when determining the appropriate life cycle of the record. These needs may take into account fiscal and tax-related considerations, departmental needs and uses, and industry practices, to name a few. From a legal perspective, a risk assessment should be conducted to help identify and minimize potential risks and legal repercussions associated with retaining a record for too long or too short a period of time.

Where legal provisions govern retention periods, they must be integrated into a corporation's retention schedule. Afterward, operational needs may be considered, but will never drive the period of retention below that required by law.

Storage Format

As a basic principle in records management, the legal and operational value of a record is not determined by its format, e.g. paper or electronic. Content is the primary factor. However, corporations must not ignore those laws and regulations which provide the requirements for acceptable record storage media formats; electronic storage formats being most relevant.

While most retention requirements are silent as to allowable storage formats, as a ground rule, "U.S. law permits the retention of records in any form provided that a particular form is not specifically mandated or prohibited by legal statutes or government regulations."[5] Commercially, this rule is supported in theory by the Uniform Electronic Transactions Act, which has been adopted in all but three U.S. states and "establishes the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures, removing barriers to electronic commerce."[6] Similar laws have been enacted internationally.[7]

Domestic and international laws are continuously being updated to address the ever-changing technological landscape of modern business by specifically addressing electronic media as an acceptable form of storage. In such instances, particular focus should be directed to conditional mandates which may be placed on corporations should they elect to store records electronically. For example, both the Securities Exchange Act[8] and the Commodity Exchange Act[9] require electronic storage media to be preserved on a non-rewriteable, non-erasable format, such as write once, read

many ("WORM") optical storage media. Such qualifications may significantly impact a corporation from financial, operational and technological standpoints—just another example of how multiple departments within a corporation must work together to ensure a compliant and functional records management program.

Location

In addition to format considerations and requirements, corporations must be cognizant of and adhere to any location requirements or restrictions placed on the records by law. Location requirements are varied, spanning from macro geographical specifications (such as an obligation to retain records within a particular country or state)[10] to more specific parochial requirements (such as a directive for retention to occur at company headquarters or a specific office).[11]

When considering record location, a company must also be aware of and take into account any national restraints on removal or extraterritorial storage of data kept within a country's borders.[12] Such considerations call for thoughtful and strategic planning by a corporation and its records management program when determining the most effective and beneficial location to store its records.

With proper foresight, understanding and implementation, a corporation can not only ensure compliance with location mandates, but also promote maximum efficient retrieval and use of its records, and even avoid potential legal sanctions for non-compliance.

Destruction

A record's information lifecycle begins at creation and ends at destruction (if not retained permanently). Although there is an abundant amount of legislation providing for the creation and retention of records, relatively few touch upon the manner of destruction. Those that address destruction methods vary in specificity and typically involve records containing confidential or personal data.[13] Legislation may even require records to be kept of actual destruction practices.[14]

While the proper destruction of records is significant, of equal importance is the recognition of when records should not be destroyed. In the event of impending litigation or regulatory examination, there exists a duty to preserve those records which are known to potentially hold evidentiary value. The breach of this duty is known as spoliation of evidence. Violations may result in adverse inferences, sanctions or other severe penalties.

Destruction of records must be carried out in accordance with the law and pursuant to a corporation's retention schedule and destruction policy, which should address both acceptable destruction methods and litigation hold procedures. In the absence of applicable legal provisions, records containing confidential or personal data must be destroyed in such a manner as as to render the information incapable of being reconstructed. Corporations should continuously assess its destruction policy to assure the destruction methods being utilized are in line with current regulatory requirements, existing technology and industry standards.

Protection

Protection requirements cover the physical security and integrity of the records or data being kept, as well as substantive protection of the contents of the records or data. Physical protection requirements may include instructions to keep records safe from flood or fire damage[15], while data content protection provisions may include requirements to store records in a secure location so as to prevent theft or unauthorized access.[16] As discussed above, regulations may also require corporations to preserve records in a non-rewriteable, non-erasable format, thus insuring the integrity and authenticity of the document in question.

In order to avoid costly and reputation-damaging data breaches, irretrievable loss of critical records, or other undesirable and potentially catastrophic consequences, a corporation should utilize sufficient protection measures in its record retention plan. An information governance officer or similar appropriate c-suite level executive should coordinate carefully with the corporation's IT officers as well as other departments to ensure systematic and company-wide compliance with record protection laws and internal initiatives.

Conclusion

Recordkeeping compliance is multifaceted and cannot be fully achieved by focusing on retention periods alone. As a result, corporations must approach records management in a holistic manner and consider *all* relevant components in the creation, use, maintenance and disposition of a corporation's recorded information.

Alec Pechota
Mr. Pechota is a licensed attorney and an Analyst in the Consulting Division at Zasio Enterprises, Inc.

Jared Walker
Mr. Walker is a licensed attorney and an Analyst in the Consulting Division at Zasio Enterprises, Inc.

1 ARMA International, Generally Accepted Recordkeeping Principles®, available at: http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles (accessed on August 26, 2015).

2 Id. at Principle of Retention.

3 See e.g. Utah Code § 34-46-203 (2014) (requiring employers to destroy information collected during an employee applicant selection process after two years); United Kingdom, Employment Practice Code, pt. 1, s.1.7.2 (2011) (mandating that employers destroy vetting exercise information within 6 months).4

4 See e.g. 12 Alaska Admin. Code § 52.450 (2015) (pharmacies to keep prescription drug orders for two years after the date of filling or last dispensed refill); Switzerland, Regulation on Protection against Dangerous Substances and Preparations 813.11 2005, t. 3, c. 1, art. 45 (manufacturers of chemical substances to retain assessment and classification documents for 10 years after a product is last placed on the market).

5 William Saffady, Ph.D., Managing Electronic Records, p. 121 (4th ed., ARMA International 2009).

6 Uniform Law Commission, Electronic Transactions Act, available at: http://www. uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act (accessed on September 11, 2015); see also Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001, et seq. (2000) (less comprehensive, but also establishing legal equivalence of electronic records and signatures at the federal level).

7 See e.g. South Africa, Electronic Communications and Transactions Act, No. 25 of 2002; Australia, Electronic Transactions Act, No. 162 of 1999; Hong Kong, Electronic Transactions Ordinance, CAP 553 2000.

8 17 C.F.R. § 240.17a-4 (2015).

9 17 C.F.R. § 1.31 (2015).

10 See e.g. HRS § 269-8 (2015) (stating that public utilities must keep their records within the state of Hawaii); India, Companies (Accounts) Rules, 2014, s. 3, sub. 5 (mandating that electronic back-up records of corporations be kept "in servers physically located in India").

11 See e.g. K.S.A. § 40-3805 (2015) (requiring Kansas insurance administrators to keep transactional records at their "principle administrative office"); Israel, Companies Law 5759-1999, pt. iv, c. 1, s. 124 (requiring companies to keep corporate documents at their registered office).

12 See e.g. Russia, Federal Law No. 242-FZ (2014), "On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of the Procedure of Personal Data Processing in Information and Telecommunication Networks" (recently enacted law requiring personal data of Russian citizens to be stored on databases physically located in Russia); Singapore, Personal Data Protection Act 2012, pt. vi, s. 26 (prohibiting transfer of personal data to a country or territory outside Singapore except in accordance with requirements prescribed).

13 See e.g. Idaho Code § 39-1394 (2015) (providing specific examples of acceptable destruction methods of patient records including burning or shredding); 24 Del. C. § 1761 (2015) (providing for the disposal of patient records in manner that ensures confidentiality).

14 See e.g. 13.10.23.10 NMAC (2015) (requiring health care insurers to keep logs of all medical charts destroyed).

15 See e.g. ALM GL ch. 66A, § 2 (2015) (Holders of personal data in Massachusetts to take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat); NAC 645B.080 (2015) (Nevada mortgage brokers to store original notes in a fireproof room or container).

16 See e.g. Wis. Adm. Code DHS 92.03 (2015) (custodians to keep health treatment records in a secure manner to ensure that unauthorized persons do not have access to the records).

ZEICS-A-102215-1 Rev. 1 October 2015

ZASIO