

Deloitte.

Public Records and Web 2.0: Records Governance Considerations

John Lazuk, Certified Records Manager

Deloitte Financial Advisory Services LLP

May 12, 2009

Speaker information

John Lazuk, Certified Records Manager (CRM)

- jlazuk@deloitte.com or 404.460.3351
- 25 years in the records and information management profession
 - State agency and local government advisor
 - Records & Information Manager for a Fortune 200 company
 - Independent consultant
- Senior Manager, Legal Business Consulting practice, Deloitte Financial Advisory Services LLP
 - Records governance policies and guidelines
 - Records retention schedules
 - E-discovery preparedness
 - Electronic records management
- This presentation should be not considered legal advice or opinion nor interpretation of laws and regulations. Attendees should consult with their legal counsel concerning such matters.

Electronic records governance program components

Key aspects and components of an electronic records governance program.

Compliance with:

- Laws, judicial opinions and decisions, standards of practice, employees, and public expectations
- Privacy and confidential information requirements
- Agency e-discovery strategy

Trustworthiness of:

- The information governance and management processes
- Records that are unaltered, secure, accessible
- Disposition following state and agency requirements, including secured destruction of confidential information

The **Records Management Policy**, the **Record Retention Schedule**, and the **Records Management Manual** establish the framework for the management, retention, and disposition of all records and information.

Information Governance: The policies and people who govern the retention and disposition of all corporate information.

Records Management: The efficient and systematic control of the creation, receipt, maintenance, use and disposition of records in accordance with established retention schedules, including processes for capturing and maintaining evidence of and information about agency activities and transactions in the form of records.

The **Agency Records Policy** contains the authorization, development, and approval processes for the records program, its staff and management structure, and policies and practices concerning the retention and disposition of all information.

The **Records Retention Schedule** which covers all records types created and maintained by the agency and provides minimum periods for how long to retain.

The **Records Management Manual** supplements and implements the Policy and contains focused guidelines and instructions for accomplishing various tasks in support of the Policy, including public access to records, information security, and others.

A vital accompaniment is the **e-Discovery Strategy**, the combination of processes and systems to identify, preserve, and collect records relevant to existing or reasonably anticipated inspection, investigation, or litigation and to safeguard them from alteration or destruction until the matter is resolved.

What is a record?

Florida government agencies follow Title 10, Chapter 119.011

- "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.
- (2) "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

Public access to records

Chapter 119.07 Inspection, examination, and duplication of records; exemptions.

- (1)(a) Every person who has custody of a public record shall permit the record to be inspected and examined by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public record or the custodian's designee...
 - Section provides detailed list of exempted information (personal or medical identifiable, et al)
- c) Even if an assertion is made by the custodian of a public record that a requested record is not a public record subject to public inspection and examination... the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request requesting the right to inspect, examine, or copy the record was served on or otherwise made to the custodian of the record...

Public access to records

Chapter 2008-218, Laws of Florida, amending s. 500.148, F.S. PART I
Florida's Government in the Sunshine Law, provides a right of:

- Access to governmental proceedings at both the state and local levels. The law is equally applicable to elected and
- Appointed boards and has been applied to any gathering of two or more members of the same board to discuss some
- Matter which will foreseeably come before that board for action. There are three basic requirements of s. 286.011, F.S.:
 - (1) meetings of public boards or commissions must be open to the public;
 - (2) reasonable notice of such meetings must be given; and
 - (3) minutes of the meetings must be taken.
- Taken from, *Government in the Sunshine Manual*, 2009 at

Florida government agency records retention requirements

Chapter 1B-24, Florida Administrative Code

- Florida State Archives provide General Schedules to help agencies develop their records retention schedules
- Agencies are to review and expand to include records not covered in these schedules
 - Submit Department of State Form LS5E-105REff.2-09, "Request for Records Retention Schedule" for approval
 - Appraisal criteria to use when developing
 - Legal
 - Fiscal
 - Administrative
 - Historical
- Public records may be destroyed or otherwise disposed of only in accordance with approved retention schedules

Electronic records disposition requirements

Chapter 1B-24, Florida Administrative Code

- “Agencies shall ensure that all destruction of records is conducted in a manner that safeguards the interests of the state and the safety, security, and privacy of individuals. In destroying records containing information that is confidential or exempt from disclosure, agencies shall employ destruction methods that prevent unauthorized access to or use of the information and ensure that the information cannot practicably be read, reconstructed, or recovered. The agency shall specify the manner of destruction of such records when documenting disposition.”
- For electronic records containing information that is confidential or exempt from disclosure, appropriate destruction methods include physical destruction of storage media such as by shredding, crushing, or incineration; high-level overwriting that renders the data unrecoverable; or degaussing/demagnetizing.

Electronic records management requirements

Chapter 1B-26.003, Florida Administrative Code

- “Electronic record means any information that is recorded in machine readable form.”
 - Each agency shall “Develop and implement a program for the management of electronic records.”
- “Provide an appropriate level of security to ensure the integrity of the records, in accordance with the requirements of Chapter 282, F.S. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users. Automated methods for integrity checking should be incorporated in all systems that generate and use official file copies of records.”
- “Agencies shall implement the following procedures to enhance the legal admissibility of electronic records.”
- “Each agency is responsible for ensuring the continued accessibility and readability of public records throughout their entire life cycle regardless of the format or media in which the records are maintained”....“Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained and accessible as long as needed.”

Federal Rules of Civil Procedure

Electronically stored information (ESI)

- Parties must address electronically stored information (ESI) earlier in the discovery process
 - ESI types and locations to be included in a party's initial disclosures
- ESI must be noted as being either easily searchable ("accessible") or not ("inaccessible")
 - Responding party must disclose all sources of potentially responsive information, even those not being searched or produced, and provide details of those sources
- Organizations should have in place internal processes and technology tools/ services to allow for a complete internal review before data is turned over to an opposing party
- Article summarizing impact of these ESI requirements are on:
<http://dlis.dos.state.fl.us/newsletter/article.aspx?articleID=1073&newsID=1019>, Florida State Library and Archives

Florida Attorney General Opinions

Electronic records related opinions

- Public Records - E-mail - Number: Informal Date: June 8, 2007
- Sunshine and Public Records Laws, private website - Number: AGO 2008-07: February 26, 2008
- Sunshine Law, use of online bulletin board - Number: AGO 2008-65: December 10, 2008
- Subject: Records, municipal facebook page - Number: AGO 2009-19: April 23, 2009
- Available at <http://www.myflsunshine.com/ago.nsf/sunopinions>

Web 2.0 technology use - areas to consider

Records retention and disposition

- What records types are being created on Web 2.0 provider sites?
 - Are all record types on these sites covered by your agency retention schedule?
 - Are drafts and previous versions of these records being retained and for how long?
 - Who is responsible for keeping the official record throughout its retention period?
 - How is this being monitored?
- What procedures are in place for downloading for public access requests?
 - Can the downloaded information be certified as official copies of your agency's records?
 - Do they have a history of service interruptions they may impact accessing records in a timely fashion to meet public requests?
- Who controls records disposition?
 - In a collaborative environment, which user controls disposition?
 - Does the system provider keep all information regardless?
- How do you know a record has been destroyed?
 - Is the record back-up and kept off-line by the provider?

Web 2.0 technology use - areas to consider

Privacy-protected information

- Can your agency personnel place confidential and privacy protected information on Web 2.0 provider sites?
 - Are your users being trained on appropriate levels of security required to ensure the integrity of the records?
- How is monitoring done to determine who is using what, where, how, and why?
 - Is file encryption and public key infrastructure being used to help meet state privacy requirements?
- Is your agency's data in a shared storage environment along with that of other users of the provider's services?
 - What internal firewalls are provided to ensure other users cannot access this data?

Web 2.0 technology use - areas to consider

E-discovery and court admissibility

- Has all of your agency's records on Web 2.0 provider sites been identified to help meet federal and state requirements concerning ESI?
- Will the provider allow their systems to be searched or used for e-discovery forensics purposes?
 - Are procedures in place with the provider to allow for preservation and collection of relevant records contained on their sites?
- What steps are you taking to authenticate the records taken from these sites to prove they are reliable, their integrity is intact, and no alteration has occurred?
 - Do they have procedures in place to show the records were created and stored in a standardized method each time?
 - Is security in place to prevent unauthorized addition, modification, or deletion of a record?
 - Is required system documentation being retained by the vendor to help authenticate the record to court admissibility purposes?

Summary

Key points to consider before using Web 2.0 providers

- Review your records governance requirements and decided how they are to be addressed in any Web 2.0 environment
 - Are these public records
 - How can they be accessed
 - How long do they need to be retained
 - How does disposition occur
 - Is confidential information protected
 - What steps are being taken to authenticate the record
 - What steps have been taken in case the information is needed for discovery
- Make your agency users aware of these requirements
 - Awareness training and/or written guidance on use of these technologies
- Discuss requirements and concerns with your Web 2.0 providers, including monitoring
 - Estimated there are now over 10,000 Web 2.0 tools, some multi-generational that are attempting to address security and other governance issues

Deloitte.