THE LEGAL REPORT

Thomas C. Michaud

VanOverbeke, Michaud & Timmony, P.C.

RECORD RETENTION

ELECTRONIC INFORMATION IN THE PUBLIC SECTOR

While the prediction that "by the turn of this century, we will live in a paperless society" may have been overly optimistic, the technological advances in this century alone have greatly increased the use and means to share and retain information electronically. This has created both an opportunity for public retirement systems to manage information more efficiently and a challenge to properly administer the information within the complexities of an ever changing technological and legal environment.

Records are retained for a myriad of operational, historical and legal purposes including: consistency in operations, resource of information, statutory requirements, audit requirements and protection from legal challenges. Although the law has yet to reach a consensus on the term "electronic record," most definitions are broad and written in such a way to encompass new and unforeseen technologies. Michigan's Freedom of Information Act, Act 442 of 1976, as amended (MCL 15.231 et seq.) ("FOIA"), which was enacted to provide public access to certain public records of public bodies and to establish procedures and guidelines for the dissemination of information, defines a "record" to include, "handwriting, typewriting, printing, photostating, photographing, photocopying, and every other means of recording and includes letters, words, pictures, sounds, or symbols, or combination thereof, and papers, maps, magnetic or paper tapes, photographic films or prints, microfilm, microfiche, magnetic or punched cards, discs, drums, or other means of recording or retaining meaningful content."

Given the broad definition of records, public retirement systems must recognize that records are not limited to paper documents, but include: e-mails, floppy disks, CD-ROMs, hard drives, DAT files, photographs, videotapes, audio recordings, personal digital assistants, cell phone memory and voicemail, as well as a public employee's "personal" files. As such, electronic information "prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function from the time it is created" is a record which must be managed.

Recent legal developments in the field of information management and electronic discovery have reinforced the importance of retirement systems establishing a record retention policy to efficiently and systematically control the creation, receipt, maintenance, use, and disposition of records including, the processes for capturing and maintaining evidence of and information about retirement system activities and transactions in the form of records. Courts continue to expect entities to preserve electronic data upon reasonable expectation of litigation, and continue to penalize entities where there has been a failure to place a hold on their records retention and destruction program, or failed to investigate and produce electronic information.

Electronic archaeologists now mine for data in search of gold (and mud) for litigation or political purposes. E-mail messages have specifically proved to be a fertile source of information and as more public retirement system business is conducted through e-mail, individuals should recognize that statements made in e-mails, messages saved in voicemail, notes contained on mobile divices, etc. may constitute public records. This includes "deleted" e-mails which are often retrieved on back-up tapes.

While the U.S. Supreme Court decision in Arthur Anderson LLP v. United States, 125 S. Ct. 2129 (May 31, 2005) (which involved the destruction of Enron business records) overturned Arthur Andersen's criminal conviction and upheld a business's legitimate right to destroy information pursuant to a valid record retention policy, other cases have found entities liable for the failure to protect or produce electronic records. In order to protect against claims of "spoliation" (i.e., the destruction, loss, or significant alteration of evidence, including documents, software, or tangible pieces of property or equipment), a record retention process should be designed, implemented and followed consistent with the requirements established by federal and state law, including a mechanism to halt the destruction of records.

While not all records are public records, public retirement systems are increasingly being faced with pressure from the legislature and courts to make more information a matter of public record in the belief that access will foster greater accountability. As custodian of the records, a retirement system must ensure that records are retained in a secure manner that allows not only for relative ease of retrieval and accessibility, but also protects the confidentiality of its members and the operations of a retirement system.

Information that is confidential, such as medical or proprietary records, must be protected from public disclosure. Electronic information presents unique security challenges. Simply locking the file cabinet is no longer an option where digital records are concerned. As many government and corporate entities have discovered, computers can go "missing" and hard drives/voice mails can be "hacked." Technological safeguards such as passwords and encryption must be implemented to ensure that the storage and transmission of information is protected. Retirement systems should explore the costs and benefits of securing electronic information and may need to enlist the services of outside information management professionals.

The decision as to the manner of record retention is unique to each retirement system and should be clearly understood and established by those entrusted to act in the best interest of the retirement system. A record retention policy should include consideration of the following elements:

1. All records are made and maintained in compliance with relevant laws and are retained for at least the minimum period stated in any applicable statutes or regulations.

2. All records concerning obligations of a retirement system (i.e., payment of benefits and expenses) are retained for a period of time necessary to fulfill the obligations.

3. Documents are destroyed pursuant to a standard policy developed for business reasons and procedures contain a mechanism to protect against destruction of documents upon receipt of legal processes.

4. Vital records are identified and safeguarded with the privacy and security of records appropriately assured.

A typical retention and disposal procedure would:

1. Inventory all records and documents.

2. Establish record categories within the filing system by function and content.

3. Set retention periods for each record category based upon specific criteria (i.e., statutorily required retention period, statute of limitations, audit requirements, administrative need, etc.).

4. Submit retention schedule to appropriate parties (i.e., auditor, actuary, legal counsel).

5. Approve schedule of disposal.

6. Implement, monitor and maintain the approved disposal schedule.

The proliferation of electronic documents and the legal obligations associated with maintaining such information has made it necessary for retirement systems to expend considerable resources in the management of retirement system records. While establishing a workable policy is difficult and time consuming, a systematic record retention and destruction program can vastly improve the overall operations of a retirement system and reduce costs and potential liability of administering electronic records.

As the public space has expanded into cyberspace, information received at your space should be treated as more than just a matter of record.