May 21, 2024

Alternative Storage Formats

Dear Reader:

The following document was created from the CTAS website (ctas.tennessee.edu). This website is maintained by CTAS staff and seeks to represent the most current information regarding issues relative to Tennessee county government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with county government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other CTAS website material.

Sincerely,

The University of Tennessee
County Technical Assistance Service
226 Anne Dallas Dudley Boulevard, Suite 400
Nashville, Tennessee 37219
615.532.3555 phone
615.532.3699 fax
www.ctas.tennessee.edu

Alternative Storage Formats

Reference Number: CTAS-205

Paper is not the only medium in which records can be stored. Many county offices are choosing to store records in either photographic (microfilm, microfiche, etc.) or electronic media for a variety of purposes and reasons. Each medium offers different advantages and disadvantages. Counties should thoroughly research either system before investing revenue and entrusting its vital records to a different storage media.

Alternative Formats and Temporary Records

Reference Number: CTAS-1198

Generally, if you are only keeping a record for five years or less, it is not cost-efficient to microfilm the original paper records or convert them to other media. But certain records that are "temporary" actually have a rather lengthy retention period. Many court records need to be kept 10 years and employee earning records that may be used for computing retirement benefits are kept for the approximate life of the employee. Even though these records do not have to be kept permanently, you may find it useful to convert them to other more compact formats for storage and destroy the paper originals shortly after they were created. Microfilming or electronic storage of these long-term temporary records can be ideal solutions to storage space problems. Once the records have been duplicated, apply to the County Public Records Commission for approval to destroy the original paper document. Approval of the records commission is necessary prior to the destruction of the original of any record that is still within its retention period.[1] It is not necessary to notify the Tennessee State Library and Archives of the destruction of original copies of temporary value records.[2]

Some local government offices are trying to do away with paper versions of some temporary records altogether, creating and storing the records solely in an electronic format. The law authorizes local governments officials to keep any records that the laws requires them to keep in electronic format rather than bound books or paper records.[3] However, certain stringent guidelines must be met in order to keep the records this way and local officials are strongly cautioned not to keep permanent records solely in an electronic format. Many officials have a dual system for some of their records. Using scanning or imaging technology, some offices create, then primarily use the electronic versions of their records even though paper or microfilm versions are also created and used as a security copy or for long term storage.

---

[1] T.C.A. § 10-7-404(a).

[2] T.C.A. § 10-7-413.

[3] T.C.A. § 10-7-121. But see T.C.A. § 49-2-301 that requires directors of schools to keep some records in both paper and electronic formats.

Microfilm

Reference Number: CTAS-1199

The process of microfilming[1] is more than 150 years old. "In 1839 the French began to use micro-photography, primarily for placing small portraits into lockets. During the Franco-Prussian War of 1870-1871, the French filmed documents and used carrier pigeons to transport the filmed information to unoccupied portions of France."[2] Comparatively, this makes the process of microfilming seem ancient compared to newer electronic formats for record keeping. There are several well-documented advantages of microfilm; control, convenience, space savings, protection, and the quick entry of full text.[3] Microfilming can offer as much as a 98 percent reduction in storage space over storing records in their original paper format.[4] By having a back-up copy of microfilm stored off-site, governments can almost immediately recover from any disaster or occurrence that damages its vital paper records. Produced correctly, microfilm is considered to be archival quality meaning it is a suitable format for storing permanent retention documents.

But microfilm also has its disadvantages. No alternative format is going to be a perfect solution for all your records management problems. Microfilming is not cheap. It is a labor intensive process that requires a level of expertise from the person doing the work. Additionally, if microfilm is not properly produced, developed and stored, it will not stand the test of time. It may be difficult to recognize deterioration of

microfilm records or mistakes in the filming process until it is too late to correct the problem. There is anecdotal evidence of some cases where a person filming records made the error of skipping over many pages of text which were subsequently lost forever when the paper originals were destroyed upon the completion of filming. For these reasons, it is vitally important that any county office relying on microfilm have a strict quality control procedure in place to make sure the film adequately captures the content of the paper records prior to their destruction.

---

[1] The term microfilm or microfilming will be used generally to discuss the various micro-photographic processes available.

[2] *Using Microfilm*, Julian L. Mims, CRM, issued by the National Association of Government Archives and Records Administrators (February, 1992), p. 1.

[3] *Using Microfilm*, p.1.

[4] *Using Microfilm*, p.1.

State Laws Regarding the Photographic Preservation of Records

Reference Number: CTAS-1200

County public records commissions may authorize the destruction of original records that have been reproduced through photocopying, photostating, filming, microfilming, or other micro-photographic process.[1] When doing so, the records must be reproduced in duplicate. The reproduction must result in permanent records of a quality at least as good as is prescribed by the minimum standards for permanent photographic records as established by the Bureau of Standards of the United States government (now the National Institute for Standards Testing). One copy of the reproduction shall be stored for safekeeping in a place selected by the county public records commission and concurred in by the county legislative body. If proper facilities are available, the location should be within Tennessee. The storage location should be selected based on the goal of preserving the records from fire and all other hazards. The other copy of the records must be kept in an office in the county accessible to the public and to county officers, together with the necessary equipment for examining the records whenever required and requested by the public during reasonable office hours. Microfilmed records may be kept in the office that generated the records, or, if the records commission determines, all such records of the county may be kept in one central microfilm repository for all microfilm records of the county.[2] The law specifically states that it is the intent of the General Assembly to provide for the original recording of any and all instruments by photograph, photostat, film, microfilm or other microphotographic process.[3] Other statutes also provide that county election commissions, with the approval of their county legislative bodies, may use a supplemental system for maintaining voter registration using microfilm.[4]

State Microfilming Program

Before embarking on their own microfilming program, county offices should consult with the Tennessee State Library and Archives to find out more about the services available from that agency and for its recommendations on working with private vendors. The office of Preservation Services, Tennessee State Library and Archives may be reached by phone at (615) 741-2764. The law provides that the Tennessee State Library and Archives is charged with providing trained staff and appropriate equipment necessary to produce and store microfilm reproductions of official, permanent value bound volume records created by county and municipal governments. To implement this security microfilming program, the Tennessee state librarian and archivist is authorized to develop a priority listing of essential records based on retention schedules developed by the County Technical Assistance Service and the Municipal Technical Advisory Service. This priority listing of essential records may be revised from time to time to accommodate critical needs in individual counties or municipalities or to reflect changes in retention schedules. The camera negative of the microfilmed records shall be stored in the security vault at the Tennessee State Library and Archives and duplicate rolls of these microfilmed records shall be made available to county and municipal governments on a cost basis.[5]

Budgetary constraints over recent years have forced the Tennessee State Library and Archives to scale back some of the microfilming services it offers. However, the agency still performs limited microfilming services free for local governments and remains the best objective source of information and advice about microfilming for Tennessee counties.

---

[1] T.C.A. § 10-7-404(a).
[2] T.C.A. § 10-7-406.
[3] T.C.A. § 10-7-406.
[4] T.C.A. § 2-2-137.
[5] Title 10, Chapter 7, Part 5.

Technical Guidelines

Reference Number: CTAS-1201

The following guidelines for producing and storing microfilm are considered crucial by the Tennessee State Library and Archives.[1]For more information on microfilming, contact the Tennessee State Library and Archives.

- Microfilm must conform to national archival processing and storage standards if it is to survive.

  Tennessee law requires that "photographic film shall comply with the minimum standards of quality approved for permanent photographic records by the national bureau of standards [now the NIST]and the device used to reproduce such records on film shall be one which accurately reproduces the original thereof in all details.[2]

- Good preparation of records to be filmed is crucial to success.

  If they need it, you should clean and flatten the records before filming. You must film the records in their correct order and arrangement. At the beginning of each group, series, and sub-series, identify the records by filming descriptive "targets" that also include notes on physical condition and arrangement of the records.

- All records in a group or series, regardless of condition, must be filmed in proper orientation, order and focus.

  If a page is omitted or improperly filmed and the original destroyed after filming, there is no way to recover the permanent record that should have been preserved.

- Archival quality silver-gelatin film must be used for the camera-image negative film, and it must be processed according to archival standards.

  Diazo film and other inexpensive process films will not endure. Residual chemicals on film from poor processing will destroy film.

  However, reference copies may be on any sort of commercial film that is convenient and affordable. It will have to be replaced from time to time, since heavy use in readers will wear out the film.

- The original negative (camera-image) film must be reserved in archival storage conditions and should be kept in a site removed from the main archives.

  Only positive copies of the original negative should be used for reference, otherwise the original may be destroyed. High humidity and changes in temperature that are wide or frequent tend to hasten the destruction of film.

  The original negative (camera image) film must be used only to produce reference copies as needed. Indeed, it is still better to have a second negative copy, from which to produce reference-use positives, so that the camera-image negative original is itself preserved.

  Off-site storage, under archival conditions offers the best chance for survival or the original negative film. The Tennessee State Library and Archives is a good storage option for counties and municipalities that wish to preserve their original camera-image, negative film.

---

[1] Tennessee Archives Management Advisory 99-005, Microfilming Permanent Records, January 11, 1999.
[2] T.C.A. § 10-7-501.

Electronic Records

Reference Number: CTAS-1202

County governments can now use computers both as a format for creating and maintaining records originally as well as for reproducing existing paper records onto other storage media. There are a host of issues related to electronic record keeping from security and access to migration and preservation. In some cases, the laws that govern record keeping have not kept pace with the technology that is available. In other cases, the law authorizes some actions to encourage the use of electronic records even though current technology has yet to generate a reliable answer to some concerns of long-term records management.

Creating Records in an Electronic Format

Reference Number: CTAS-1203

Any records required to be kept by a government official in Tennessee may be maintained on a computer, removable computer storage media, or in any appropriate electronic medium, instead of bound books or paper records.[1] But in order to do so, the following standards must be met:

1. The information must be available for public inspection, unless it is required by law to be a confidential record;
2. Due care must be taken to maintain any information that is a public record for the entire time it is required by law to be retained;
3. All daily data generated and stored within the computer system must be copied to computer storage media daily, and the computer storage media that is more than one week old must be stored off-site (at a location other than where the original is maintained); and
4. The official with custody of the information must be able to provide a paper copy of the information to a member of the public requesting a copy.[2]

These standards, however, do not require the government official to sell or provide the computer media upon which the information is stored or maintained.

---

[1] T.C.A. § 10-7-121.

[2] T.C.A. § 10-7-121.

Electronic Conversion of Paper Records

Reference Number: CTAS-1204

The County Public Records Commission may also, upon the request of any office or department of county government, authorize the destruction of original public records which have been reproduced onto computer or removable computer storage media, including CD ROM disks. [1] Despite the fact that copying of permanent records to electronic media is authorized by the law, be aware that the Tennessee State Library and Archives does not consider any existing format for electronic records to be of permanent archival quality.[2]Once the records have been duplicated, the official with custody of the records must apply to the County Public Records Commission for authority to destroy them. An original paper version of a record required by law to be permanently retained must not be destroyed once reproduced without a majority vote of the county public records commission.

Prior to the destruction of any records reproduced onto electronic storage media, the County Public Records Commission is also required to advertise its intent to do so in a newspaper of general circulation in the county, and, in those counties with a population in excess of 200,000, in a weekly newspaper.[3]The notice should describe the records by title and year, indicate that the records have been electronically stored, reproduced and protected, and indicate that the county office or department has requested permission to destroy the original record.

See Electronic Records are Not Permanent Archival Records; Tennessee State Library and Archives.

---

[1] T.C.A. § 10-7-404(d)(1).

[2] See Tennessee Archives Management Advisory 99-006.

[3] T.C.A. § 10-7-404(d)(1).

Why Electronic Formats May Not Be Well Suited for Perma-

nent Records

Reference Number: CTAS-1205

New technologies bring our offices new capabilities and wonderful conveniences. Computers can make the task of searching for and finding a specific record, or all records related to a specific topic, as simple as the push of a button. They were designed and intended for the compact storage of massive amounts of information and rapid processing of that information; they were not designed for permanence and therefore present new problems and dangers to the county official managing public records. Be aware that many of the best state and national records authorities do not consider any electronic format currently available, including CDs or computer hard drives, to be viable for data storage longer than 10 to 15 years.

> Therefore, electronic records may not be suitable as the sole format for keeping long-term or permanent records.

As the statutory provisions authorizing remote access or electronic creation and duplication of records indicate, extra safeguards are necessary with electronic records. If you consider for a moment the true nature of electronic records, you can see why precautions are necessary.

Fragility

Computer records are nothing more than magnetic impulses embedded in a chemical medium. Does not sound like something that is going to last through the ages, does it? The truth is, electronic records are much more convenient to use, but they are also more fragile than paper records. Like paper records, fire and water can destroy them, but so can magnetic impulses, power surges, heat and moisture. Unlike paper records, a little bit of damage goes a long way. A spilled cup of coffee may ruin a few papers on your desk before you can clean up the mess. Spill the same cup onto your computer, and the equivalent of volumes and volumes of information can be destroyed in a moment. Another manner in which computer records are unlike paper records is the possibility of damaging the records through use. Continuous use over a long period of time may cause the deterioration of a bound volume, but that in no way compares to the amount of damage that can be done to a disk of computer records by a negligent or malicious user. Damage to paper records is generally more readily apparent and more easily remedied than damage to electronic files.

Computer Records Are Not "Human-Readable"

When you use computer records, you need a third party involved namely, a computer. If something happens to your computer system, you cannot access the records until it is replaced. If the problem is a lightning strike that knocked out a few PC's in your office, it is no big deal. They may be expensive, but they are definitely replaceable. If the problem is a bug in a proprietary record-keeping software package and the company that wrote your software is out of business, you may have an insurmountable problem. No matter how well you preserve the computer media with the data on it, without a program you cannot read it.

Data Migration

If you still think computer records are safe and reliable for long term usage, consider this: even if you have your magnetic tapes and computer disks and CD-ROMS in 10 or 20 years' time and they have been perfectly preserved in pristine condition, will you still be running the same computer? This is a problem which may prove to be the most serious technological issue of this century. The retention schedules provide an ironic example of the problem. The previous CTAS records manuals produced in the 1980s were recorded onto 5.25 inch floppy disks. When work began on the 1999 edition of the records manual, only one ancient computer remained in the office that had a disk drive that could read the old files. Luckily we were able to copy the files onto the network and preserve the information before it was lost. It does not take 15 or 20 years for compatibility issues to arise. Replacing five-year-old computers may create difficulties in transferring data due to changes in the types of media read and written by the computer or changes in operating systems which create incompatibilities.

These examples highlight significant data management problems that arose in less than a generation—merely five or 10 years. Imagine the difficulty finding a way to access computer records that are 30, 40 or, in the not too distant future, 100 years old. To avoid falling victim to the rapid changes in technology, you must have a system of data migration. Whether you use a computer for keeping the current financial records of your office or you are using an imaging system to capture information on old records, you must anticipate and plan on being able to transfer that information from one computer system to the next as you upgrade your equipment and software. Failing to recognize this need will lead to a disaster. To be on the safe side and to ensure long-term preservation of permanent records, such records should be kept as paper or microfilm, in addition to the electronic systems used for access.

See Electronic Records are Not Permanent Archival Records; Tennessee State Library and Archives

Other Issues Relative to Electronic Records

Reference Number: CTAS-1206

Remote Electronic Access to County Records

Each county official has the authority to provide computer access and remote electronic access for inquiry only to information contained in the records of the office that are maintained on computer storage media in that office, during and after regular business hours. However, remote electronic access to confidential records is prohibited. The official may charge a fee to users of information provided through remote electronic access, but the fees must be in a reasonable amount determined to recover the cost of providing this service and no more. The cost to be recovered must not include the cost of electronic storage or maintenance of the records. Any such fee must be uniformly applied. The official offering remote electronic access must file with the comptroller of the treasury a statement describing the equipment, software, and procedures used to ensure that this access will not allow a user to alter or impair the records. This statement must be filed 30 days before offering the service unless the official has implemented such a system before June 28, 1997. T.C.A. § 10-7-123.

Records Management and E-Mail

Reference Number: CTAS-1207

Many county officials have raised questions about how to handle e-mail or how long e-mail should be kept. You will not find an entry in the retention schedules specifically for e-mail. E-mail is more of a format for records than a type of record itself. An inter-office memorandum may be typed and distributed on paper or it may be sent to all staff via e-mail. Either way, the retention period or procedures for managing the record should be determined based on the content of the memo, not its method of delivery. Much of the volume of e-mail that passes through our computers does not reach the level of an official "record." Recall the general definition of "public record."

> Public record ... means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency.[1]

This general definition is not as specific as the definition of county public records,[2] but it highlights the fact that the record may take many different forms. The definition also makes clear that a public record is something created pursuant to law or in connection with the transaction of official business. E-mails unrelated to county business are generally not considered to be public records. Additionally, most email communications that do relate to county business are in the nature of working papers - something which serves as input for final reporting documents and becomes obsolete immediately after use. We recommend the county public records commission establish a policy which authorizes the destruction of working papers as freely and easily as possible so they do not become overly burdensome. But suppose you send someone a notice of a promotion solely via e-mail. According to the listing in the retention schedule for Promotion Records of Notices (see item 16-031), this record should be kept for one year from the date the record is made or the action is taken, whichever is later. A copy of this e-mail should therefore be retained at least that long.

Network administrators or information technology specialists will tell you that it is highly complex or expensive to manage electronic correspondence on an individual e-mail basis. Some e-mail programs have archiving features or a means of designating for preservation. But most likely, your office has a policy of backing up all the data in an e-mail server for a limited period of time. Eventually, the back up tapes or disks will be discarded or over-written. Many e-mails will be deleted by the person receiving them and possibly never make it to a back-up tape. Of course, every copy of a public record does not have to be kept. If you have electronic correspondence that would be considered a public record based on its content, it is recommended that you print that out and preserve it as a paper record or that you institute some means of designating certain e-mail files for preservation. You may want to particularly keep this in mind for e-mails which consist of correspondence with members of the public regarding the official business of your office. The retention schedule entry for Correspondence Files (see entry 15-010) recommends keeping correspondence with citizens or government officials regarding policy and procedures or program administration for five years. This standard should apply whether the correspondence is by traditional "snail mail" or e-mail.

E-Mail and Privacy

If your office uses e-mail and the Internet, hopefully you have some policy in place stating whether or not personal use of e-mail or the Internet is allowed and whether or not all e-mail correspondence remains the

property of the county. Such policies at least put employees on notice as to whether or not they have any expectation of privacy in their e-mails. If it has not happened yet in your county, you may expect that at some point in the future you will receive a public records request from the media or from citizens to get a copy of e-mail correspondence of the office. At the time this was written there were no reported appellate cases to date in Tennessee regarding e-mail as a public record, however there have been cases considering this issue in other jurisdictions. In the Florida case of *Times Publishing Company v. City of Clearwater*[3] a newspaper reporter demanded copies of all e-mail of two city employees. The city allowed the employees to segregate their e-mail into two classes: public and personal. The city turned over the public e-mails, but refused to release the personal e-mails pending a determination by the court. Ultimately, the court ruled that personal e-mails which were not created or received in connection with the official business of the city did not qualify as "public records" subject to disclosure under Florida law and that it was proper for the city to remove them from the e-mails which were released.[4] Whether or not a Tennessee court would reach the same conclusion under our public records statutes is unknown at this time. What is relatively clear is that the e-mails which related to the business of the city were considered public records and were subject to disclosure. Any county offices using e-mail correspondence to conduct the business of the office should keep this in mind.

---

[1] T.C.A. § 10-7-301.

[2] See T.C.A. § 10-7-403.

[3] *Times Publishing Company v. City of Clearwater*, 830 So.2d 844 (District Court of Appeal of Florida, Second District, 2002).

[4] Times Publishing Company, at 847.

Electronic Signatures and Transactions

Reference Number: CTAS-1208

County officials should also be aware of recent state and federal laws which have been passed to authorize and encourage electronic transactions and the acceptance of electronic signatures. In 2000, the U.S. Congress passed the Electronic Signatures in Global and National Commerce Act ("E-Sign").[1] That same year, Tennessee passed its own Electronic Commerce Act of 2000. This law was superceded and replaced the next year, when the Tennessee General Assembly then enacted the Uniform Electronic Transactions Act (UETA),[2] which was a model law crafted by the National Conference of Commissioners on Uniform State Laws in 1999 and adopted by many states. These laws were all intended to facilitate and validate electronic transactions, but they do not replace existing laws or require the use of electronic signatures.

Electronic Signatures in Global and National Commerce Act (E-Sign)

The E-Sign Act did not amend or pre-empt existing laws specifically, but provided that notwithstanding any statute, regulation, or other rule of law, with respect to any transaction in or affecting interstate or foreign commerce (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[3] Therefore, if a state law requires a transaction or signature to be "in writing," the federal E-Sign Act requires that you interpret the term "in writing" to include electronic files and signatures. E-Sign specifically exempts certain transactions from its provisions, including—

1. a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;
2. a state statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or
3. the Uniform Commercial Code, as in effect in any state, other than sections 1-107 and 1-206 and Articles 2 and 2A.[4]

Additionally, E-Sign does not apply to—

1. court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;
2. any notice of the following—
   -Cancellation or termination of utility services (including water, heat, and power);

-Default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
-Cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or
-Recall of a product, or material failure of a product, that risks endangering health or safety; or

3. any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials, wills, family law matters, court orders, most matters governed by the Uniform Commercial Code, notices of cancellation of utilities and notices of foreclosure.[5]

Uniform Electronic Transactions Act (UETA)

As with E-Sign, this act does not require a record or signature to be created or sent in electronic format and only applies to transactions where all parties have agreed to conduct the transaction electronically but it does provide broad authorization for the use of electronic records and signatures. It also more directly controls the creation or receipt of such records and signatures by state and local government offices. The act provides that if the law requires a record or signature to be in writing, an electronic record or signature satisfies the requirement; however, the law also provides that if a law other than this act requires a record to be posted or displayed in a certain manner, to be sent, communicated or transmitted by a specified method, or to contain information that is formatted in a certain manner, then the record must be posted, displayed, sent, communicated or transmitted in accordance with that law. Similarly, if a law requires a record to be retained, the requirement is satisfied by keeping it electronically if the electronic record accurately reflects the information in the record and if the electronic record remains accessible for later reference. One provision of the act notably states however that the act does not preclude a governmental agency of this state (which is defined to include county governments) from specifying additional requirements for the retention of a record subject to the agency's jurisdiction. Therefore, even though two parties to a transaction may agree to perform that transaction electronically, if a county office must receive and retain a copy of that transaction, the county could require that copy to be in paper format.

Another section of the UETA specifically governs the creation and retention of electronic records and the conversion of written records to electronic form by governmental agencies in Tennessee. It provides for the Information Systems Council (ISC) to determine whether and the extent to which the state or any of its agencies create and retain electronic records and convert written records to electronic records. Officials of counties and municipalities and other political subdivisions are authorized to determine for themselves whether they will create and retain electronic records and convert written records to electronic records. Those officials can also determine whether the governmental agency will send and accept electronic records and signatures to and from other persons. To the extent that any governmental agency chooses to do this, the Information Systems Council may establish certain rules and regulations governing the process. Local government officials that choose to send and receive electronic records that contain electronic signatures, must file certain documentation with the comptroller prior to offering such service as well as providing a post-implementation review.

In 2003, the General Assembly amended state law to clarify that the Tennessee Uniform Electronic Transactions Act does not supersede the federal E-Sign Act in regard to the following: (1) The consumer disclosure requirement (when a written record of contract terms is required by law an electronic record can be used instead, if the consumer consents to such); (2) The accuracy and accessibility requirement (when a law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record); and (3) Denial of electronic record requirement (if an electronic record is not in a form that can be retained and accurately reproduced for later reference by all parties, such electronic record's legal effect, validity, or enforceability may be denied). This legislature also clarified that the Uniform Electronic Transactions Act does not authorize the electronic delivery of any of the following (consistent with the E-Sign Act):

1. Court orders or notices or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;
2. Any notice of: cancellation or termination of utility services; default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual; the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or recall of a product, or material failure of a product, that risks endangering health or safety; or

3. Any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

So far, the impact of these laws on the daily operation of local government offices has not been significantly burdensome. However, they are a clear indication that in the future local government offices will have to adapt to a private sector that is moving further and further away from traditional paper transactions and relying more on electronic commerce and communications.

---

[1] 15 U.S.C. §§ 7001,*et seq.*

[2] 2001 Public Chapter 72, codified primarily in T.C.A. §§ 47-10-101, *et seq.*

[3] 15 U.S.C. § 7001(a)(1) and (2).

[4] 15 U.S.C.A. § 7003(a).

[5] 15 U.S.C.A. § 7003(b).

Geographic Information Systems Records

Reference Number: CTAS-1215

In 2000, the General Assembly also passed Public Chapter 868 to authorize counties to charge increased fees to people purchasing copies of a certain type of record for commercial purposes. Under the new law all state and local governments maintaining geographic information systems (GIS) are authorized to charge enhanced fees for reproductions of public records that have commercial value and include a computer generated map or similar geographic data. Prior to the passage of this act, local governments could charge only for the actual costs of reproduction of such data (usually a minimal charge for the costs of the computer disk or other copying media) unless they were in one (1) of five (5) counties designated by narrow population classes that had specific authorization to charge higher fees under the law. Under T.C.A. § 10-7- 506(c), local government entities that have the primary responsibility for maintaining a GIS can also include annual maintenance costs and a portion of the overall development costs of the GIS in the fees charged to users who want to purchase a copy of the information for commercial use. If the system is maintained by the county, the county legislative body establishes the fees. If GIS is maintained by a utility, the board of directors establishes the fees. Two groups are exempt from the higher fees: individuals who request a copy of the information for nonbusiness purposes and members of the news media who request the information for news-gathering purposes. These exempt parties will be charged only the actual costs for reproducing the data. Development costs that may be recovered by the fees charged to commercial users are capped at ten percent (10%) of the total development costs unless some additional steps are taken. For local governments, the local legislative body and the state ISC must approve a business plan that explains and justifies the need for additional cost recovery above ten percent (10%). Even with the approval of such a plan, development cost recovery cannot exceed twenty percent (20%). However, these limits do not apply to annual maintenance costs, which may be fully recovered in the fees charged to commercial users. The recovery of development costs of a system is subject to audit by the comptroller of the treasury. Once the allowable portion of the development costs of the system have been recovered by the additional fees charged to commercial users, then the fees must be reduced to cover only the costs of maintaining the data and ensuring that it is accurate, complete, and current for the life of the system.

Identity Theft and Unauthorized Access to Electronic Records

Reference Number: CTAS-1209

Faced with growing concerns about identify theft, the General Assembly has begun to take steps to protect consumer information in business and government data bases that could be used for fraudulent purposes. Effective July 1, 2005, new provisions enacted in Title 47, Chapter 18, Part 21 of the *Tennessee Code Annotated* by 2005 Public Chapter 473 require county governments to notify affected parties when there has been unauthorized access to certain personal consumer information in the county's computers. The law applies broadly to any business doing business in the state of Tennessee and all agencies of the state of Tennessee and its political subdivisions. These entities must disclose, to any residents whose information has been compromised, any breach of a computer system which allows unauthorized disclosure of an individual's name in combination with any of the following: social security number, driver license number, financial account numbers, or credit or debit card numbers. Personal information does not include publicly available information lawfully made available to the general public from federal, state,

or local government records. Notice may be provided by written notice or electronic notice. Substitute notice is allowed if the cost of providing notice would exceed $250,000 or requires notice to more than 500,000 individuals. Substitute notice is defined to consist of e-mail notice if the information holder has e-mails for the affected parties, conspicuous posting of the notice on any internet page of the information holder, and notice to major statewide media. If circumstances require notification to more than 1,000 persons at one time, notice to all consumer reporting agencies and credit bureaus of the breach is also required. Any person injured by a violation of this act may bring a civil action against business entities to recover damages or enjoin the violator from further actions violating these requirements; however, state agencies and political subdivisions are exempt from the civil damages provisions of the act.

Source URL: *https://www.ctas.tennessee.edu/eli/alternative-storage-formats*