

RECORDS MANAGEMENT

FOR

COUNTY GOVERNMENTS

*A reference guide for county officials and county public records commissions
published by*

**The University of Tennessee
County Technical Assistance Service**

Compiled and Edited by
David Connor, CTAS Legal Consultant

July
2005

Visit our Web site at
www.ctas.tennessee.edu

FOREWORD

July 2005

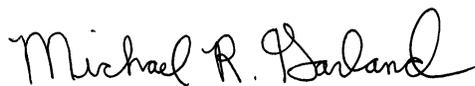
Dear County Official:

This manual is offered as a basic summary of laws, regulations and practices related to records management by county government offices. This 2005 edition is an update of the 1999 manual. The 1999 comprehensive manual replaced several previous publications of this office entitled *County Records Manuals*, which addressed records specific to one office. Instead of several individual publications with records disposition schedules which were geared toward a single office of the county, this larger manual contains more comprehensive information on records management, including new sections to address the many changes in technology in recent years, plus the disposition schedules for all county offices in one volume. In this way, we hope the manual is of more universal appeal, easier to update, and more useful to county public records commissions and state agencies that work with county governments. The 2005 edition did not make major revisions to the retention schedules, but does include a few new schedules and items. In addition, the text portion of this edition includes new, updated, or expanded material related to public access to records, electronic records and transactions, social security numbers and confidential records, expunging records, recent court cases and attorney general's opinions, and new statutes or regulations affecting records management for local government.

We have tried to make this publication as timely and accurate as possible. Please be aware however, that laws and regulations affecting local governments are in a constant state of change. When relying on information in this publication about a specific law or regulation, it is always best to consult the specific statute or regulation to make certain the law has not been amended or repealed. Consult with the county attorney or other legal counsel when necessary.

The CTAS staff hopes this manual will be useful to you and will help increase the efficiency and effectiveness of your office. Please feel free to contact us if you have questions or comments regarding this publication. As you will note in the Acknowledgments, many people have assisted us in the preparation of this document. All those involved have the gratitude of the CTAS staff for their invaluable help in producing this work.

Sincerely,



Michael Garland

CTAS Executive Director

Table of Contents

PREFACE	vii
PART ONE: INTRODUCTION	1
Introduction	3
Reasons for Records Management	3
Space	3
Records Serve as a Legal Foundation	3
Open Records Requirements	4
Historical Preservation of Documents	4
Purposes of this Manual	4
PART TWO: LEGAL ISSUES	5
Legal Issues: Introduction	7
Laws that Require Records to Be Kept	7
Federal Laws and Regulations	7
State Laws and Regulations	7
Laws that Govern How You Manage Your Records	8
Good Record Keeping as a Bedrock of Law and Government	8
Basic Record Keeping Statutes	8
The State Public Records Commission	9
County Public Records Commissions	11
Creation and Membership	11
Organization and Compensation	11
Jurisdiction and Authority of the Public Records Commission	12
Oversight Over the Disposal and Final Disposition of Records	12
Authorizing Transfer of Records	12
Miscellaneous Authority	13
Promulgating Rules and Regulations	13
Lamination	13
Establishing Copying Charges	13
Funding	13
Where to Begin—Establishing Procedures	14
Recommendations	14
Minimums	15
Progressive Steps	15
The Advantages of a Public Records Commission	16
Public Access to Records	17
The Freedom of Information Act (FOIA)	17
Tennessee Public Records Statutes	18
Who Has Access?	18
How Should Access Be Provided?	18
Limiting Risks	19

Providing Copies of Public Records	20
Charging for Copies	20
Records with Commercial Value	20
Special Issues in Providing Access to Court Records	21
Expunging Court Records	21
Providing Access to Records in Non-Paper Formats	23
Providing Access to Electronic or Computerized Records	23
Remote Access to Computerized Records	24
Denial of Access to Public Records—Liability	25
To What Records Is the Public Entitled Access?	25
Confidential Records	26
Maintenance of Confidentiality	28
Special Considerations and Specific Types of Confidential Records	28
Social Security Numbers	28
Motor Vehicle Registration Records	30
Vital Records	31
Law Enforcement Personnel Records	31
Domestic Violence Prevention and Protection Documents	31
County Hospital, Health Department Records and Ambulance Records	32
HIPAA	32
Credit Card Records and Credit Reports	34
Student Records	35
The Family Educational Rights and Privacy Act	35
Model Notification of Rights under FERPA for Elementary and Secondary Schools	37
Model Notice for Directory Information	38
Educational Records of Disabled Students	39
Tennessee Statutes Affecting Education Records	40
Confidentiality	40
Educational Records as Evidence in Judicial Proceedings	40
Non-Custodial Parents	41
Record Keeping Duties of the Director of Schools	41
Conclusion	41
 PART THREE: RECORDS MANAGEMENT	 43
The Basics	45
Step One: Evaluate	45
Inventory	45
Filing Systems	46
Filing Equipment	46
Step Two: Develop Records Disposition Authorizations (RDAs)	46
Step Three: Develop Written Policies and Procedures	48
Step Four: Continuing Maintenance	48
Appoint a Records Management Officer	48

Conclusion	49
Disposal of Records	51
Checks and Balances	51
What Kind of Record Is It?	51
Working Papers	51
Temporary Records	51
Continuing Authorization for Destruction of Temporary Records	52
Permanent Records	53
Duplication of Permanent Records	53
Notice Requirements in Destroying Original Copies of Permanent Records	53
Methods of Destruction	54
Special Considerations	54
Financial Records and Audits	54
Exhibits and Evidence in Court Cases	54
Documents	55
For Physical Evidence Other than Documents and Firearms ...	55
For Firearms	55
Other Miscellaneous Special Considerations	56
Conclusions	56
Alternative Storage Formats	57
Alternative Formats and Temporary Records	57
Microfilm	57
State Laws Regarding the Photographic Preservation of Records	58
State Microfilming Program	58
Technical Guidelines	59
Electronic Records	60
Creating Records in an Electronic Format	60
Electronic Conversion of Paper Records	60
Why Electronic Formats Are Not Well Suited for Permanent Records .	61
Fragility	61
Computer Records Are Not “Human-Readable”	61
Data Migration	62
Other Issues Relative to Electronic Records	62
Records Management and E-Mail	62
E-Mail and Privacy	63
Electronic Signatures and Transactions	64
Electronic Signatures in Global and National Commerce Act ..	64
Uniform Electronic Transactions Act (UETA)	65
Identity Theft and Unauthorized Access to Electronic Records	66
Proper Storage Conditions	67
Records Centers	67
More Information	68

Establishing Archives	68
Specifications	69
Archives Storage and Management Space	69
Technical Assistance	71
Disaster Preparedness	73
Contingency Plans	73
Vital Records Protection	74
Recovery of Stolen or Misappropriated Records	75
Conclusion	76
Endnotes	77
PART FOUR: RETENTION SCHEDULES	89
Assessor of Property Records	99
County Clerk Records	105
County Mayor Records	121
Circuit and Criminal Court Records	125
Clerk and Master Records	137
General Sessions Court Records	153
Juvenile Court Records	155
Department of Education Records	157
County Election Commission Records	169
Highway Department	173
Register of Deeds Records	177
Sheriff's Records	185
Solid Waste Departments and Landfill Records	191
Trustee's Records	195
Accounting and Purchasing Records and Other Miscellaneous Records	201
Employment Records	205
Animal Control Records	213
Fire Department Records	215
Planning and Zoning Records	219
APPENDICES	221
Appendix A: Statutory Provisions Governing County Public Records and the County Public Records Commission	223
Appendix B: Tennessee Archives Management Advisory 99-007	229
Appendix C: Sample Resolution to Establish the Membership of the County Public Records Commission	235
Appendix D: Sample Resolution to Establish a County Archives	237
Appendix E: Sources of Additional Information	239
Appendix F: Records Inventory Worksheet	243
Appendix G: Records Disposition Authorization Form and Instructions	247
Appendix H: Additional Disaster Recovery Resources	253

PREFACE

Prior to 1978, the Tennessee State Library and Archives published a single manual on records management for county offices entitled the *Tennessee County Records Manual*. In 1978, in response to a mandate of the 90th General Assembly, which enacted new laws regarding the county public records commission, the County Technical Assistance Service (CTAS), with the aid of the Tennessee State Library and Archives, the Division of Records Management of the Department of Finance and Administration, the County Audit Division of the Comptroller's Office and many county officials, revised the *Tennessee County Records Manual* and published the following series of new manuals in its place:

- County Records Manual for the Assessor of Property
- County Records Manual for the Chancery Court
- County Records Manual for the Circuit, Criminal, and General Sessions Courts
- County Records Manual for the County Clerk
- County Records Manual for the Department of Education
- County Records Manual for the Election Commission
- County Records Manual for the County Executive
- County Records Manual for the County Highway Department
- County Records Manual for the Register of Deeds
- County Records Manual for the Sheriff
- County Records Manual for the County Trustee

These office-specific manuals were geared toward the records of one particular county office and contained a disposition schedule related to those records. After the initial publication in 1978, these individual manuals were independently revised and republished throughout the mid-1980s as the need arose.

Significant legislative and technological changes have necessitated a new publication on this subject. With this single manual, we are replacing the series of office-specific manuals and returning to the original one-volume format. One of the reasons for abandoning the office-specific series of manuals was a legislative change in 1994 mandating the creation and operation of the County Public Records Commission. Since that organization is now required to be involved in records management for all county offices, we felt a comprehensive publication would be easier and less confusing to use than 11 separate manuals. Additionally, as this manual includes more chapters and information on technical issues related to records management, it was more efficient to publish one manual rather than reproduce that information in 11 separate documents. In Part Four of this manual you will still find office-specific disposition schedules for all county offices that were once covered in an individual manual. Certain records which are common to each county office (personnel and employment records, for example) are now organized under topic listings. It is our hope that this arrangement of materials will assist the reader in identifying the appropriate disposition for a particular record.

PART ONE
INTRODUCTION

I ntroduction

Records management is an often overlooked issue in both public and private sector offices; however, this task is becoming more vital everyday. In this information age, everyone—from the average citizen to the largest corporation or government—must find a way to preserve, manage, store, and organize their records. Whether it is a neighbor finding this month’s phone bill and getting it paid on time, or General Motors keeping accurate wage and hour records on its employees, everyone needs a system for tracking documents and the information in them. Good managers will expend significant time and effort in planning and making decisions about their labor force and their facilities. Few take the time to think about their records. The records of an office are often as essential to its operation as its employees, facilities, and equipment. New employees can be hired and trained to replace those who leave; new office space and equipment can be leased or purchased to replace anything that is lost, even in the worst disasters. If your records are lost or destroyed, however, there is nowhere to go to purchase a replacement, and they often cannot be recreated.

For certain county officials, like the register of deeds or the clerk of a court, record keeping is one of the central duties and purposes of the office. For others, like highway departments or sheriff’s offices, record keeping is incidental to the fundamental purpose of the office—maintaining roads or law enforcement. Nevertheless, these offices must still comply with federal and state statutes that require accurate records regarding the personnel, finances, and other aspects of the office. Good records management practices will benefit both types of offices.

Reasons for Records Management

Proper records management not only conveys organizational and managerial benefits to an office, but also—for local government offices—it is a vital task, necessary for fulfilling important legal requirements and duties. The following are just a few of the reasons your county should take records management seriously.

Space

In most counties, space is not the final frontier; it is the final battle. It is rare for a county office or courthouse to have all the space it needs. Most local officials would complain that the necessary records of the office are rapidly filling up all available space. Courthouses are bursting at the seams with old records stuffed into basements, storage closets, attics, and other creative locations. For this reason alone, it is important and cost effective for a county to implement a records management program.

Records Serve as a Legal Foundation

In a society of laws, local governments and the citizens they serve are both dependent upon good documentation to demonstrate their legal status. Court orders, marriage licenses, and the minutes of the county commission are just a few examples of important documents that create relationships, establish rights or liabilities, and authorize certain actions. When disputes arise over legal issues, it is important to have good documentation on which to rely. Local governments have an important responsibility to preserve these records. Proper records management will ensure these records are preserved and can be found when needed.

The records of an office are often as essential to its operation as its employees, facilities, and equipment.

Open Records Requirements

Since government records are generally open to public inspection, the task of managing records becomes even more important and more complicated. The principle of allowing public access to government records, combined with so-called “sunshine laws,” which require open meetings, is considered an important check on government and an important defense against corruption in public office and mismanagement of public resources. Unless there is a specific legal exemption that makes a record confidential, the public has the right to inspect and get a copy of the records of government agencies. So you must as a county official, not only preserve and keep records, you must also allow public access to these records for inspection. Unless your records are well organized and well protected, you may not be able to comply with public requests for information, undermining public confidence in government and hindering your office’s relationship with the citizens it serves.

Historical Preservation of Documents

Counties play a vital role in preserving our nation’s history. The documents and records of local governments give us insights into the lives of our ancestors and the circumstances of their times. Counties with too many records and too little space for the records end up putting them wherever they can. In many cases, these storage areas do not adequately protect the records from the elements. Heat, moisture, mildew, insects, and vermin can quickly render records useless. The county and its citizens may be losing important information as well as a part of their past and their heritage. With proper records management, the important records are preserved, the less essential records are destroyed when no longer useful so they do not take up all the available space, the records are catalogued and organized so officials and the public can access them, and records are stored under proper conditions to enable long-term preservation.

Purposes of This Manual

This manual is intended to be a resource to help county officials and members of the County Public Records Commission implement proper records management programs in county offices. In this manual you will find summaries of the basic laws regarding record keeping that affect county offices; a description of the county public records commission and its authority and responsibilities; a discussion of guidelines for storing records in alternative formats such as microfilm, microfiche, and the various electronic or computer storage media; instructions regarding the procedures to follow prior to destroying a record; suggestions about contingency planning for disaster recovery and records storage; as well as general information on records management and a listing of other sources of information on these topics. Although many of these issues are too complex to treat them fully in this publication, hopefully the manual will highlight the issues that should concern county officials and records commissions and give them a start in the right direction.

The vast majority of this manual consists of records retention schedules for all the major types of records and offices of the county. These schedules describe the standard records kept by offices, indicate whether these are permanent or temporary records, and establish the amount of time a temporary record must be kept before it can be destroyed. The County Technical Assistance Service is authorized by law to produce these schedules as “guides” for county public records commissions, county officials, and judges to use in determining the proper disposition of their records.¹

PART TWO
LEGAL ISSUES

L

egal Issues: Introduction

County governments, and all the secondary offices, boards, committees, and commissions of a county, are creations of the law. They find their origin in either the Tennessee Constitution or statutory law. It is a long established principal in Tennessee law that counties can only do those things that the law authorizes them to do.² Therefore it is vitally important to any operation of county government to know what the laws are that authorize the county to perform a function and to know what the laws are that place limitations around that authority. There are laws that require counties and county officials to keep records, and there are laws that govern how a county manages its records. Both of these topics will be examined in this part.

Laws that Require Records to Be Kept

Not every record in a government office has a corresponding statute or regulation requiring that record be kept. Many records are generated simply as an ordinary course of business without any legal authority mandating their creation. But the creation and preservation of certain other records are required by specific laws. Since these laws affecting individual records are referenced in the retention schedules at the end of this manual, this chapter will only discuss the sources of those laws more generally.

Federal Laws and Regulations

County officials should be aware that federal laws and regulations require them to keep certain records. This is particularly true of payroll information and other employment-related records. Most of the laws regarding how we hire, fire, compensate, and treat employees are generated at the federal level. The *Family and Medical Leave Act*, the *Fair Labor Standards Act*, the *Occupational Safety and Health Act* are just a few of the laws that place certain burdens on employers to keep records regarding their employees. (For more detail on these requirements, see the retention schedule for Personnel Records in Part Four of this manual.) These statutes also generate a whole other layer of federal regulations that govern the implementation and enforcement of the acts. In addition to personnel issues, federal laws and regulations also touch such diverse topics as student records and voter registration. Laws passed by the U.S. Congress are codified in the *United States Code* (U.S.C. or U.S.C.A. for *United States Code Annotated*). The massive amounts of rules and regulations generated by the different federal agencies are primarily found in the *Code of Federal Regulations* (C.F.R.).

State Laws and Regulations

Since county governments are instrumentalities of the state, most of the laws regarding what records need to be kept by county offices and how those records should be managed are found in the *Tennessee Code Annotated* (T.C.A.). As with the federal government, the state of Tennessee also has a set of rules and regulations promulgated by state agencies, boards, and commissions which are published by the secretary of state and known as the Official Compilation—Rules and Regulations of the State of Tennessee.

The duties of most county officials can be found spelled out in Title 8 of the *Tennessee Code Annotated*. For most offices, a requirement is included in the duties of the office to keep and preserve specific types of records. Certain county offices, such as the register of deeds, the clerks of the various courts of the county, and the county clerk, have a primary function of record keeping. The proper and efficient performance of these duties is necessary not only for the continued operation of the county

government, but also for the preservation of order in our society. Without them, our criminal justice system, our civil courts, and our rights of property ownership would be thrown into chaos. But even offices without a primary record keeping function are required to keep records.

Even though county officials may change with every election, the offices themselves must maintain a level of continuity. To ensure this, the responsibility for keeping and turning over the records of county offices was specifically addressed in the statutes requiring county officials to be bonded. Part of what is insured by the bond of an official is the fulfillment of a duty to “**...faithfully and safely keep all records required in such principal’s official capacity, and at the expiration of the term... turn over to the successor all records and property which have come into such principal’s hands...**”³ Failure to do so can result in recovery against the insurance company or sureties on the bond who may in turn proceed against the official in his or her individual capacity for subrogation of the claim. It is the solemn obligation of each county official to act as the legal custodian of the records of that office, to provide for their security and care, and to turn them over in good order to his or her successor.

Laws that Govern How You Manage Your Records

Good Record Keeping as a Bedrock of Law and Government

If you ever thought the way we do things seems to have come from the dark ages, you were right. Some practices of record keeping in government offices, particularly certain local government offices, are literally ancient. The importance of keeping accurate records of property transactions and legal proceedings is a bedrock of English law and goes back a thousand years. Laws that require the recording of documents in “well bound books,” the necessity of having a written record to show property ownership, the creation of specific offices to keep these records—all go back to the Middle Ages. Up until the advent of the computer, we had been doing things pretty much the same way they had been done since the 13th century. Even today, some of the laws in our Tennessee code regarding the records of the register’s office and the offices of the clerks of court retain elements of this language from more than 700 years ago. Something does not last that long without there being a good reason. Basic rights that we take for granted, such as the rule of law and the sanctity of private property, are impossible without a good, durable record keeping system. All this should impress the Tennessee county official that he or she is the inheritor of a great and solemn tradition of responsible record keeping. Generations of clerks, registers, and officials before them have discharged this public trust and, hopefully, passed the records on to you in good shape.

Basic Record Keeping Statutes

Both the older state laws on records management and their more modern counterparts are found primarily in Title 10, Chapter 7 of the Tennessee Code Annotated. Parts 1 and 2 of that chapter contain a number of statutes about preserving, transcribing, and indexing records. The statutes require the county to “procure for the register’s office well-bound books for the purpose of registering therein such instruments of writing as are required by law to be registered...”⁴ Among other things, the laws direct how to transcribe information from books that have been “damaged or mutilated by fire or otherwise,”⁵ require the county to appropriate money to rebind books when necessary,⁶ and designate how the clerks of courts and the register are to properly index the books.⁷ As was discussed earlier, the county official can be held liable for failure to safely keep the records of his or her office. An exemption is granted here relieving an official of liability during the time record books are out of the custody of the county clerk, clerk and master, circuit court clerk, or register for the purpose of having books rebound.⁸

Not all of our records statutes are steeped in the past. Although many of the laws found in these parts seem headed the way of the dinosaur, there are some that point to the future. One of these newer, more progressive statutes authorizes maintaining any information required to be kept by a government official on a computer or on removable computer storage media instead of bound books or paper if certain standards are met.⁹ Another authorizes county officials to provide computer access and remote electronic access to information maintained on computer media in the office.¹⁰ A third authorizes the register to maintain all indices required of the office on a computer instead of index books.¹¹ When granting new authority to adapt to modern technology, our state legislature has been cautious. All of these statutes condition the use of electronic media on a number of safeguards and restrictions. More information on these statutes and other laws regarding electronic records can be found in detail in Part Three of this manual in the chapter on Alternative Storage Formats.

The State Public Records Commission

Part 3 of Chapter 7 of the Tennessee Code, Title 10, establishes the State Public Records Commission and designates the Records Management Division of the Department of General Services as the primary records manager for all state government records.¹² Currently, these entities do not take jurisdiction over county government records, but they can be looked to as examples for proper records management and preservation. There are similarities between the responsibilities and powers of the State Public Records Commission and the county public records commissions that have jurisdiction over county records. The county public records commission is vital to any records management program for county governments. Its creation, membership, powers, and operation are discussed in detail in the next chapter.

C

ounty Public Records Commissions

In 1959, the Tennessee General Assembly first made provision in the Tennessee Code for the creation of a county public records commission.¹³ Although the creation of the commission was optional at the time, the organization and responsibilities of the commission under the 1959 law were very similar to what one finds in the state law today. The express purpose of the commission is “to provide for the orderly disposition of public records created by agencies of county government.”¹⁴ While minor revisions and additions to the statutes regarding this commission have occurred over the last few decades, the most significant change in the county public records commission occurred in the mid-1990s, when the legislature amended the law to mandate the creation of this body.¹⁵ Ever since 1994, every county in Tennessee has been required by law to have a County Public Records Commission.

Creation and Membership

The commission is required to be composed of at least six members. Three of the members are appointed by the county mayor subject to the confirmation of the county legislative body. Of those three, one appointee is to be a member of the county legislative body, one is to be a judge of one of the courts of record in the county, and one is to be a genealogist. In addition to these appointees, certain county officers automatically become members of the county public records commission by nature of the office they hold. These *ex officio* members include the county clerk (or the designee of the county clerk pursuant to a 2002 amendment to the law), county register, county historian and, in those counties with a duly appointed archivist, the county archivist. The *ex officio* members remain on the commission for as long as they hold their office. The appointed members of the commission serve until they vacate office, at which time the county mayor appoints a replacement in the same manner as provided above.¹⁶ Since the state statute mandating the records commission places no limitations on the *ex officio* members, there are no distinctions between the *ex officio* members and appointed members. **All members of the County Public Records Commission have the same rights and privileges, including voting rights.**¹⁷ If your county does not have a public records commission or if your records commission has become inactive, it is strongly recommended that you begin taking steps to comply with the law and establish the commission. A sample resolution for creating a public records commission is included in the appendices to this manual.

Since 1994, every county in Tennessee has been mandated to have a County Public Records Commission.

Organization and Compensation

The commission is directed to elect a chairperson and a secretary and to keep minutes of all its proceedings and transactions.¹⁸ Members of the commission are not paid a salary except that any member of the commission who does not already receive a fixed annual salary from the state or the county may receive a per diem of \$25 for each day of actual meeting. All members may be reimbursed for actual necessary expenses incurred in performing the duties of the records commission.¹⁹ Although active commissions may meet more regularly, the state law requires that the County Public Records Commission meet at least twice each year.²⁰

Jurisdiction and Authority of the Public Records Commission

The county public records commission is granted the power to oversee the preservation and authorize the destruction of any and all public records as defined by the law to be within the jurisdiction of the commission.

Those records within the jurisdiction of the county public records commission include

- All documents, papers, records, books, and books of account in all county offices;
- The pleadings, documents, and other papers filed with the clerks of all courts including the courts of record, general sessions courts, and former courts of justices of the peace and the minute books and other records of these courts; and
- The minutes and records of the county legislative body.²¹

Note: Prior to 1999, the County Public Records Commission also technically had jurisdiction over municipal records. As a practical matter, few municipalities were working with the county public records commission to manage their records. Since a legislative change in 1999,²² municipal records are no longer within the purview of the County Public Records Commission.

Oversight Over the Disposal and Final Disposition of Records

The most important role of the County Public Records Commission is to provide oversight and make determinations regarding the ultimate disposition of the records of county offices. County governments in Tennessee are not highly centralized. Individual elected officials have a great deal of independence in the management of their own offices. Recognizing this, and realizing the danger of a single official having the sole discretion regarding whether to keep important public records, the state legislature created the county public records commission and provided it with the authority to decide whether county records should be retained or destroyed.²³ It is the responsibility of the commission to ensure that no county records that need to be preserved are destroyed prematurely and to ensure that original records which have been reproduced into other storage media have been properly duplicated before the originals are destroyed. In working with county officials, the commission should strive to balance this responsibility to protect records against the need to manage records efficiently. Since destroying records is absolutely necessary for keeping the records of an office manageable, the commission should encourage and cooperate with local officials in culling the obsolete and unnecessary records from their offices. There are two primary circumstances where the public records commission may authorize destruction of records. First, the records commission may authorize the destruction of temporary value records and working papers that are no longer needed by county offices and departments through its rules and regulations.²⁴ Second, the commission may authorize the destruction of original paper records that must be retained permanently once those records have been successfully preserved in another format.²⁵ The full procedures that should be followed in making determinations about records disposition and destroying and duplicating records are discussed in more detail in part of this manual.

Authorizing Transfer of Records

For records commissions that place a premium on the historical preservation of county records, the law provides an alternative to destruction. Once the County Public Records Commission determines that a county office, department, or court no longer needs to retain a record, the commission may provide for transferring the record to another institution instead of destroying it. The records may be placed into the custody of a local or regional public library, a local, regional or state college library, or the county archives, to be preserved for historical purposes.²⁶ The transfer of the records should be approved by a majority vote of the commission. At any time after the records are transferred to one of

the entities listed above, the commission may, after giving one month's notice to the institution holding the record, transfer the records to another institution. If appropriated by the county legislative body, county funds may be expended by the records commission for the purpose of transferring records to an institution or for the maintenance and preservation of the records.²⁷ If your county chooses to transfer records to another institution for storage and preservation, it is recommended that the county enter into a contractual agreement with that entity specifying that it is only keeping them on behalf of the county and that ownership of the records is not being transferred. Rather than transferring the records to a private library or archives, the Tennessee State Library and Archives recommends that a county should establish its own archives or enter into an interlocal agreement with other local governments for the creation of a regional archives. More information about this subject is available in Part Three of this manual in the section entitled Establishing Archives.

Miscellaneous Authority

Promulgating Rules and Regulations

In conjunction with its general oversight authority the county public records commission is authorized to promulgate rules and regulations over certain matters under its jurisdiction. Pursuant to state law, the records commission has the authority to establish rules and regulations regarding the making, filing, storage, exhibiting, and copying of reproductions of records.²⁸ Such rules and regulations must be approved by the majority of the voting members of the records commission and must be signed by the chair of the commission.²⁹ The rules and regulations should include, but need not be limited to, the following:

- Standards and procedures for the reproduction of records for security or for disposal of original records in all county offices;
- Procedures for compiling and submitting to all county offices lists, schedules, or time tables for disposition of particular records within the county; and
- Procedures for the physical destruction or other disposition of public records.

Lamination

The law also expressly authorizes the records commission to provide for the lamination of permanent records.³⁰ This, however, is one of those cases where the law was too quick to embrace a technology. Instead of protecting documents, the lamination process too often destroys the very documents it is intended to preserve. For this reason, **the Tennessee State Library and Archives strongly recommends that permanent records not be laminated** but rather encapsulated in mylar sleeves.³¹

Establishing Copying Charges

The records commission has the power to establish charges and to collect such charges for making and furnishing or enlarging copies of records.³² (This authority applies usually to records in county archives. Often, office specific statutes govern the fees charged for copies of records in particular offices such as the register of deeds or court clerk.) While it will be up to the county legislative body to determine how to allocate these revenues, counties may want to consider “re-investing” them in equipment, supplies, or personnel expenses related to records management and records preservation.

Funding

The county legislative body may appropriate such funds as may be required for carrying out the purposes of the County Public Records Commission. This includes, but is not limited to, funding for purchasing or leasing equipment, the equipping of an office and related expenses, hiring administrative assistants, and the employment of expert advice and assistance.³³

Where to Begin—Establishing Procedures

To help find direction and some basic first steps to take, public records commission members should finish reading the information in this section on the records commission itself, then skip over and read the beginning of Part Three of the manual. Those sections provide basic instruction and guidance to public officials on how to manage their records and they outline the steps that the official and the records commission should go through in inventorying, evaluating, and disposing of records. If there are officials in your county who are actively working to manage their records, they are probably following a strategy similar to the one described in Part Three. If your officials are not doing anything, you can direct them to those materials for a road map to follow.

After reviewing Part Three, flip through some of the retention schedules in part of this manual. Those schedules actually make up the bulk of the book. They may not make a lot of sense to you at first, but when you begin to work with a local official on the records of his or her office, the usefulness of the schedules should become apparent. As a records commission, you do not have to look through pages and pages of records yourself and decide what to do with each one from scratch. What you should do is work in cooperation with county officials and department heads to ensure that records of those offices are being destroyed in accordance with an acceptable retention schedule that was thoughtfully developed.

The County Technical Assistance Service, in cooperation with the Tennessee State Library and Archives and the Division of Records Management, is authorized to publish schedules which are to be used as guides by all county public records commissions, county offices, and judges of courts of record in determining which records should, can, and may not be destroyed.³⁴ Those schedules are the ones found in Part Four of this manual. The retention schedules describe more than 650 different records series for multiple county offices. This material is organized by county office and by subject. Obviously CTAS recommends that all county public record commissions adopt these schedules as the basis for determining the disposition of county records in their county. When the schedules were developed, they were reviewed and revised by the legal and technical staff of CTAS, by the Division of County Audit in the office of the comptroller, by representatives of the Tennessee State Library and Archives and the Division of Records Management in the State Department of General Services, and by committees and groups of numerous county officials. The language of the statute says that county officials and records commissions shall use these schedules as “guides” in determining whether a record should be kept or destroyed. This does not mean that a County Public Records Commission can never deviate from the CTAS schedules. However, any decision to use a different retention period should be thoughtfully considered and the reasons well documented by the records commission. Any decision to destroy a record sooner than is recommended by the schedules certainly needs to be taken seriously. If your records commission decides that there is a significant reason why a record should be destroyed before the recommended retention period has elapsed, I suggest contacting CTAS first to discuss the retention period and see if there is a reason why the recommended retention period in the manual should be shortened.

Recommendations

The Tennessee State Library and Archives (TSLA) has been extremely helpful in the development of this manual and its retention schedules. It has employees on its staff who have the task of working with local officials and records commissions to ensure good county records management and the preservation of important historical documents from Tennessee’s history (those from days gone by as well as those we are creating each day). TSLA offers the following list of basic minimum actions that county public records commissions should be taking in order to fulfill their function of basic records

management and oversight. For those records commissions that desire and have the resources to be more progressive, there are further recommended courses of action that follow.

Minimums

- Meet at least twice a year. (This is the statutory minimum.)
- Set a schedule for regular meetings so that county officials can plan ahead for their interactions with the records commission.
- Elect officers (at least a chairman and a secretary).
- Keep minutes and records of decisions and transactions.
- Oversee the preservation and authorize the destruction of any and all public records as defined by the law.
 - ▶ Request offices to conduct an inventory of their records and submit that inventory to the PRC.
 - ▶ Use records inventories to gauge need for the destruction of temporary records and the sufficiency of storage space for permanent records.
 - ▶ Encourage records-keeping officers and PRC members to familiarize themselves with the CTAS manual, especially the records retention schedules.
 - ▶ Require county offices to begin using a standard Records Disposition Authorization form (see a sample in the appendices) to document requests for records destruction.
 - ▶ Review the request, then authorize or disapprove requests from county offices to destroy original records, using the retention schedules in this manual for guidance.
 - ▶ Assure that authorizations for destruction of public records are forwarded to TSLA for review within 90 days of the PRC authorization.
 - ▶ Follow-up on requests sent to TSLA before destroying any records to make sure that approval of the destruction has been given.
- Establish rules and regulations regarding the making, filing, storage, exhibiting, and copying of reproductions of records.
- Establish procedures for compiling and submitting to all county offices lists, schedules, or time tables for disposition of particular records within the county.
- Establish procedures for the physical destruction or other disposition of public records.

Progressive Steps

TSLA suggests the following further measures that a PRC can take to strengthen its records management function.

- Hold meetings more than twice a year. (If your county is just beginning an effort to get records management going, meeting more often will be necessary. Also, if all the offices of a county begin actively participating in records management, two meetings will probably not be sufficient to thoroughly review all requests.)
- Report at least once a year to the county mayor and legislative body on commission activities and the state of records and archives management in the county.
- Review records keeping practices in county offices and recommend to the offices and to the county mayor and legislative body remedies to correct faults and improvements to deal with emerging information and records needs.

- Work with county offices, CTAS, TSLA, and the Records Management Division of the state Department of General Services to draft, review, revise, and issue realistic records management schedules for local government records.
- Encourage the development of disaster recovery and vital records protection plans for all county offices.
- Review and approve all plans by county offices for electronic imaging or data processing systems to assure that
 - (a) the system employed will protect and preserve records designated as permanent by CTAS retention schedules, and
 - (b) a permanent, archival-standard microfilm of permanent records is produced.
- Encourage a regular program of microfilming to protect and preserve permanent records of the county. Send a copy of any microfilm produced to TSLA for quality control testing and storage in the vault.
- Become more familiar with any records you intend to destroy so that you can recognize any that may have historical value or are good candidates for transfer to a county archives or outside institute that can preserve the record for historical purposes.
- Propose to the county cooperative arrangements with other counties or cultural institutions such as libraries and universities for keeping, managing, and allowing for the public inspection of historically valuable records, including permanent public records of the county.
- Advise and propose to the county mayor and the legislative body the planning, development, site selection, establishment, funding, budget, regulation, and operation of a local archives and records office.
- Advise and recommend to the county mayor and legislative body the appointment and removal of personnel, including an archivist as director, for the central records office and archives.
- Review operations of any existing county records offices and archives to assure the county legislative body that they meet records management and archives management standards and satisfy the needs of the county and its citizens.

The Advantages of a Public Records Commission

Although the law requires that every county create a public records commission, there are more advantages to creating the commission than simply fulfilling the legal requirement. An active records commission helps to manage the records that your county generates efficiently and legally. Destroying out of date, temporary records alleviates records storage problems and frees up space in offices, possibly postponing the need for renovation or expansion of offices. If the records commission takes the additional measures suggested and works with the county to create an archives, the county has ensured that it has fulfilled its duty to provide long term access to public records as mandated by the Tennessee Code. Additionally, having an active PRC also demonstrates to the citizens of your county that its government is meeting its legal and custodial responsibilities of caring for public records.

For more information on how to get your PRC up and running, contact the Archives Development Program at the Tennessee State Library and Archives

Jaime Awalt (615) 253-3471
Wayne Moore (615) 253-3458

P Public Access to Records

Modern laws requiring public access to government records began to surface in the United States in the 1950s. But the concept of openness in government goes back to the start of our nation. Certain of the founding fathers placed a great deal of importance on the need for citizens to be informed about the activities of their government. However, even the most visionary of the founding fathers probably did not anticipate the depth and breadth of information held by the government today. The struggle to balance the right of the public to access government records with the increasing desire to protect privacy and confidentiality gets more difficult each year. While new technologies have enhanced our ability to manage data and information, they have also created new fears about abuse of personal and confidential information. The sword of liability can cut both ways. There are potential liability concerns for refusing access to records that are public and for disclosing confidential information. For these reasons, it is important for the custodian of public records to have a good understanding of the public's right to access government records and the limitations on that right.

“A popular government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy—or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors must arm themselves with the power which knowledge gives.”

James Madison

The Freedom of Information Act (FOIA)

During the “atomic age” following WWII, a strong movement began on the state and federal level to allow the public access to information about what the government was doing and to files that the government had collected about individual citizens. This push resulted in the passage of “open records” laws in many states during the 1950s and culminated in the passage of the Freedom of Information Act at the federal government level³⁵. Tennessee was among those states passing an open records law in the 1950s.³⁶ The specifics of our state laws will be discussed shortly, but first it is useful to make a few brief points about the Freedom of Information Act. “The Freedom of Information Act (FOIA)³⁷ was passed by Congress in 1966 and amended in 1974. Based on the premise argued by Madison and Hamilton that openness in government will assist citizens in making the informed choices necessary to a democracy, FOIA creates procedures whereby any member of the public may obtain the records of the agencies of the federal government.”³⁸

The main thing county officials need to know about the FOIA is that it applies to *agencies of the federal government*.³⁹ The Freedom of Information Act does NOT apply to county governments. As a county records custodian, you need to be aware of the FOIA because citizens may try to assert their rights to county government records under that act due to confusion as to which laws apply. Different policies and procedures apply to federal offices under the Freedom of Information Act that are not included in the Tennessee public records statutes that apply to your office. Under the FOIA, citizens may request a federal agency covered by the act to perform searches of its records to locate certain information and then disclose the information, providing copies to the person making the request (subject to certain fees). As will be seen, Tennessee statutes allow broad access to public records, but they do not

generally require local officials to perform searches or create new reports or responses to requests if those reports are not already a part of the office records.

Tennessee Public Records Statutes

The public records statutes that do apply to county offices are found in Title 10, Chapter 7, Part 5 of the *Tennessee Code Annotated*. The starting point for a discussion of the law in this area is the declaration found in T.C.A. § 10-7-503, that government records are open to public inspection. It reads as follows:

... [A]ll state, county and municipal records ... except any public documents authorized to be destroyed by the county public records commission in accordance with § 10-7-404, shall at all times, during business hours, be open for personal inspection by any citizen of Tennessee, and those in charge of such records shall not refuse such right of inspection to any citizen, unless otherwise provided by state law.⁴⁰

This statute has been construed broadly by the both the state attorney general and the Tennessee judiciary.⁴¹ The legislature made it clear that its intent in passing this law was to “...give the fullest possible public access to public records” and it instructed the courts to exercise whatever remedies are necessary to ensure that purpose is fulfilled.⁴² The courts have ruled that a “presumption of openness” exists with government documents.⁴³ That is not to say that public access is totally without limitation however.

Who Has Access?

The statute states that records must be open for inspection by any “citizen” of Tennessee. In keeping with the legislative intent to provide for liberal public access to government records, the Tennessee Supreme Court has determined that the word “citizen” includes convicted felons incarcerated as inmates within the Tennessee prison system.⁴⁴ Although certain rights are stripped from individuals when they are convicted of a felony (i.e. voting, ability to hold public office), the court concluded that neither the Tennessee Public Records Act nor any other statute prevented a convicted felon from seeking access to public records. Neither should access be denied to anyone else who appears to be a citizen of this state. (See more about providing copies of records to inmates in the next section.)

The law is not as generous with non-residents. Since the statute states that it grants public access to “any citizen of Tennessee,” the Tennessee attorney general has opined that public officials may deny requests for copies of public records based on the lack of state citizenship.⁴⁵ Since there is no fundamental federal right to access of government records and since Tennessee’s laws provide access only to state citizens, the attorney general reached the conclusion that it is not a violation of the privileges and immunities clause of the United States Constitution to deny access to persons making requests from other states for Tennessee records. Keep in mind that although the act does not affirmatively require disclosure of public records to non-citizens, neither does it prohibit the release of public records to non-citizens.⁴⁶ It is within the discretion of the official who has custody of the records to determine whether or not access will be provided to non-citizens. It is the recommendation of CTAS that offices should develop a written policy in that regard and enforce it consistently.

How Should Access Be Provided?

The law states that records shall be open to inspection “during business hours.” Every effort should be made to provide reasonable accommodation to parties requesting access to records; however, providing this service need not prevent the performance of other duties of the office. A request to see

every record of an office and make a photocopy of each of them could obviously bring the entire operation of an office to a halt. For this reason, the official who has custody of the records is also authorized by law to adopt and enforce reasonable rules governing the making of extracts, copies, photographs or photostats of the records.⁴⁷ These regulations should be reasonable and not interfere with the intent of the legislature to provide broad public access to records. The official with custody of the record should strive to balance the right to access records with his or her responsibility to preserve and protect the records. Regulations should be tailored to accommodate requests in a timely manner while allowing for the continued efficient functioning of the office and for the preservation and security of the records. Regulations that are intended to frustrate the ability of a citizen to access records will likely be found unreasonable and struck down by the courts. The county public records commission may serve as a valuable resource in developing and drafting these regulations.

Although there is little legal authority in this area, the following are some examples of regulations that would likely be found reasonable by a court:

- Establishing that copies of records would be provided within a reasonable time period (for example: the next business day for small requests and within five business days for larger requests);
- Prohibiting the inspection and copying of records by citizens without supervision of the official or an employee of the office; and
- Prohibiting the handling of older bound volumes or other fragile records by anyone other than an employee of the office so long as the information in the records is still provided in a usable format.

The 1999 edition of this manual suggested that another possible regulation could provide that requests for inspection of a large number of records would be accommodated only by appointment pursuant to a written request. In a 2001 opinion, the attorney general was asked to consider a very similar requirement. In opinion 01-021, the attorney general found that there was no clear answer to the question. While the public records laws are to be interpreted to allow the fullest possible access, this should not lead to absurd results. The attorney general opined that if a citizen challenged a requirement to set an appointment to view records, a court might not find this requirement to be tantamount to a denial of access if the agency could articulate a reasonable basis for requiring the appointment. Absent a legitimate reason, the court may conclude the requirement of an appointment was merely being used to delay access to the records.⁴⁸ This opinion therefore appears to support the idea that local officials can implement reasonable regulations so long as there is a clear, articulated reason for the regulation that relates to goals of records management. .

Limiting Risks

Be aware that there is a danger of theft, vandalism, or damage by negligence inherent in allowing a member of the public access to government records. There is a profitable market out there for certain historical manuscripts. Across the country, government records are disappearing from government offices and reappearing for sale in antique stores, flea markets, speciality shops, or Internet auction sites. To prevent theft or vandalism, someone from your office should supervise the person accessing the records or, at a minimum, the person accessing the records should be required to examine them in an open area where abuse of the records or attempted thefts will be noticed. If county records have been lost in the past and are discovered in someone's possession, the Tennessee Code, in Section 39-16-504, grants statutory authority to counties to initiate judicial proceedings to reclaim lost, stolen, or otherwise misappropriated records.

Providing Copies of Public Records

Also note that, in all cases in which a person has the right to inspect public records, he or she also has the right to take extracts or make copies of the record, or to make photographs or photostats of the record while it remains in the possession, custody, and control of the official who has lawful custody of the record.⁴⁹ In 1999, the attorney general interpreted this to mean that the Tennessee Public Records Act does not require a public official to make copies and send them to anyone regardless of whether or not they are a citizen of Tennessee.⁵⁰ However, this opinion is limited by a subsequent court decision. In the case of *Waller v. Bryan*,⁵¹ the Tennessee Court of Appeals required public officials to make public records available to members of the public who could not visit the official's office under certain circumstances. In that case, an inmate appealed the ruling of a chancellor that he was not entitled to requested records which were in the possession of a police department. The local government refused to make copies of the requested records and mail them to the inmate. Obviously, his circumstances did not allow him to appear in person to inspect the records and make a copy. The Court of Appeals held that as long as a citizen can sufficiently identify the requested records so that the government office knows which records to copy, the official should comply with the records request. To refuse to do so merely because the citizen could not appear in person would, in the words of the court, "place form over substance and not be consistent with the clear intent of the Legislature."⁵² The court observed that a requirement to appear in person would not only limit access to records by inmates, but also all those Tennessee citizens who were prevented by health problems or other physical limitations from appearing at the government office.

Charging for Copies

Tennessee courts and the attorney general have found that the authority to make and enforce reasonable rules and regulations regarding copying public records includes within it the ability to recover actual costs incurred by the governmental agency in making the records.⁵³ However, this ability to recover costs is limited to the context in which copies of records are produced and is limited to allow a charge only for a cost that reasonably approximates the actual costs of copying the record.⁵⁴ In 2001, the attorney general was asked whether local governments could charge a fee to recoup costs of providing access to records or for researching or locating non-public records for review by the public. The attorney general concluded that T.C.A. § 10-7-503(a) does not authorize a local government body to charge a fee for allowing inspection of a public record.⁵⁵ Neither was there any general statutory authority that would allow a local agency to charge a research or location fee *per se*. (Note however, that there is very limited authorization discussed in the next section.) Furthermore, conditioning the right to inspect records on the payment of a fee that was not authorized in state law would be tantamount to denying the right to inspect records. However, the attorney general did note that research fees or location fees may be chargeable if they involve recovery of actual costs of staff time that was spent compiling the records in order to make copies.⁵⁶ Therefore, the best legal authority we have to date indicates that costs related to finding and providing access to records are not recoverable if the citizen merely wishes to review or inspect the record. If staff time is spent locating and collecting records in order to provide copies of the records, this cost most likely is recoverable. Furthermore, because of these limitations, the attorney general has opined that agreements or contracts between a local government and a private entity to sell public records probably violates the Tennessee Public Records Act.⁵⁷ See more about this issue under the section regarding remote access to records below.

Records with Commercial Value

The legislature has recognized that in certain circumstances, a governmental agency may expend a great deal of money developing a record with great commercial value. That record in turn may then be

requested by a company who only has to pay a small fee for a reproduction of the information which may be used to generate significant amounts of revenue. Therefore, the legislature in 2000 amended T.C.A. § 10-7-506 to add provisions that protect the investment of government resources specifically in computer generated maps or geographic information systems. These systems are expensive to develop and have numerous profitable commercial applications once the data is developed. Private entities could acquire a copy of the data and regular updates for practically no cost then profit greatly by selling subscriptions to the data. For this reason, the legislature allowed governments to also recover a portion of the actual development and maintenance costs when providing copies of computerized mapping systems or data to persons other than the news media or individuals for non-business use. While this general statute is limited to electronic geographic records, an additional statute applicable only to court clerks offices in Knox and Shelby counties allows those officials to charge a fee not to exceed \$5 for computer searches for any public record having a commercial value.⁵⁸

Special Issues in Providing Access to Court Records

Court records can be a little different from most of the records in other county offices in that they are created by parties of the case who need access to the records on an on-going basis during litigation. The evidence and discovery materials in the cases are not created by the clerk, but merely held for use by the parties. For this reason, though case files are technically public records, special provisions may apply. The United States Supreme Court has stated that “every court has supervisory power over its own records and files.”⁵⁹ In Tennessee, the Court of Criminal Appeals has similarly ruled that “a trial court has the inherent authority to determine the custody and control of evidence held in the clerk’s office.”⁶⁰ These case files, while in the court clerk’s office, will usually be open to the public.⁶¹ This public right of access is rooted in the First Amendment and in the common law, but is a qualified right.⁶² Since this right is qualified and not absolute, it is subject to the court’s discretion on a particular matter.⁶³ Therefore, unless there is a statute making a record confidential or a clear court directive sealing records or prohibiting public access to the records, the public may access case files. If the court seals a record, it becomes confidential and free from public scrutiny.⁶⁴ This power is not unlimited. The records may only be sealed when “interests of privacy outweigh the public’s right to know.”⁶⁵ If parties to litigation approach a clerk with concerns about public access to materials included in case files, the clerk should direct the parties to petition the judge to order such records sealed from public access. Additionally, as parties to litigation may need extended access to and use of case records, courts may also adopt rules to authorize that pleadings and exhibits may be withdrawn by parties to the case or their legal representatives.⁶⁶

Expunging Court Records

Several statutes in Tennessee law provide for parties to have records of judicial proceedings involving them expunged from the records of the court and certain other offices. The basic statute for expunction of criminal offense records is found in T.C.A. § 40-32-101(a)(1).

All public records of a person who has been charged with a misdemeanor or a felony, and which charge has been dismissed, or a no true bill returned by a grand jury, or a verdict of not guilty returned by a jury, and all public records of a person who was arrested and released without being charged, shall, upon petition by that person to the court having jurisdiction in such previous action, be removed and destroyed without cost to such person; however, the cost for destruction of records shall apply where the charge or warrant was dismissed in any court as a result of the successful completion of diversion program according to §§ 40-15-102--40-15-105; provided, that the records of a person who successfully completes a diversion program pursuant to §§ 40-15-102

— 40-15-105 shall not be removed and destroyed pursuant to this section if the offense for which prosecution was suspended was a sexual offense as defined by Section 40-39-102(3) provided, however, that when a defendant in a case has been convicted of any offense or charge, including a lesser included offense or charge, the defendant shall not be entitled to expungement of the records or charges in such case pursuant to this part..

The law provides that the record to be expunged “does not include arrest histories, investigative reports, intelligence information of law enforcement agencies, or files of district attorneys general that are maintained as confidential records for law enforcement purposes and are not open for inspection by members of the public and shall also not include records of the department of children's services or department of human services which are confidential under state or federal law and which are required to be maintained by state or federal law for audit or other purposes. . .”⁶⁷ Court cases have also determined that physical evidence is not addressed by the expungement statutes; and therefore, cannot be expunged.⁶⁸

In cases of judicial diversion, there is separate statutory authority for expunging records.⁶⁹ In those circumstances, a person who had charges dismissed through judicial diversion may apply to the court to expunge all official records other than certain non-public records that are kept solely to determine whether the person is eligible for diversion in the future. Once again, sexual offenders are not eligible to have their records expunged. The application for expungement shall contain a notation by the clerk evidencing that all court costs are paid in full, prior to the entry of an order of expungement.⁷⁰ If the court determines, after hearing, that the charges against such person were dismissed and the proceedings discharged, it shall enter such order. The effect of such order is to restore the person, in the contemplation of the law, to the status the person occupied before such arrest or indictment or information. Other statutes authorize expunction in cases that were dismissed through pre-trial diversion under a memoranda of understanding⁷¹ or in cases where the governor declares the defendant exonerated.⁷²

The Administrative Office of the Courts is mandated to develop a standard uniform judgement document to be used when judges order expungement. In cases where the criminal record is expunged, certain information must be reported to the Tennessee Bureau of Investigation (TBI) to be maintained in its expunged criminal offender and pretrial diversion database.⁷³

In addition to courts with criminal jurisdiction, the primary statute on expunging criminal offenses explicitly states that it applies to juvenile courts.⁷⁴ Also related to younger offenders, the statute goes on to provide that all public records of a person who has been convicted of an offense that was committed prior to such person's 21st birthday shall, upon petition by such person to the court having jurisdiction over the original conviction, be removed and destroyed if such person has not been convicted of an offense except for the offense to which the petition pertains; was not convicted of a sexual offense; and pays a fee to be established by the court for the destruction of such public records (not to exceed \$25).⁷⁵ Juveniles who have their driving record suspended can apply to have that record expunged once they reach 18 years of age and have their license reinstated.⁷⁶ There are also some very specific rules related to expunction of records of certain offenses by juveniles related to the transportation of liquor or beer. Persons under 21 years of age convicted of violations of these statutes have the right to have the records of such violation destroyed after the passage of six months from the date of the violation upon motion of the person to the court which heard the violation and without cost to such person.⁷⁷

Outside of the criminal setting, parties to any divorce proceeding, who have reconciled and dismissed their cause of action, may file an agreed sworn petition signed by both parties and notarized, requesting expungement of their divorce records.⁷⁸ Upon the filing of such petition, the judge shall issue an order directing the clerk to expunge all records pertaining to such divorce proceedings, once all court costs have been paid. The clerk shall receive a fee of \$50 for performing such clerk's duties under this section. Other less commonly used statutory provisions allow for the expunction of affidavits of heirship from the register of deeds office⁷⁹ and records of proceedings related to the appointment of a fiduciary where none was appointed.⁸⁰ Also, records of military discharge may be expunged by registers of deeds from their records upon application by proper parties.⁸¹

Providing Access to Records in Non-Paper Formats

The records of governmental offices are no longer only paper documents or bound books. Records may now be found in a diverse mixture of media. If your office stores records in various formats, such as audiotape or videotape, you may need to make sure some means of accessing the record is readily available to the public. Since the definition of a public record includes records of many formats (including various audio and video records and electronic files), the attorney general has opined that it may violate the Public Records Act if the custodian of the records stored in these other formats could not provide a means for the public to inspect these records.⁸² This may require you to have a VCR and television or tape player available for use in your office or somewhere in the courthouse. Separate statutes specifically related to electronic records and microfilm records also require that equipment be available to allow viewing of records stored in these other media.⁸³ These mandates may be of particular concern to an archives facility which may store records of many different formats in one location. Allowing continued access to these records may prove difficult for both the office that created the records and the archives. More information about managing and protecting electronic and microfilm records may be found below and in Part Three of this manual.

Providing Access to Electronic or Computerized Records

The advent of computers in government record keeping has created legal issues regarding not only the question of “what is a public record?” but also “what is the record itself.” If the assessment rolls in the assessor of property’s office are stored in computers, is the record only a standard report of that information or is it the raw data itself? If the public requests that the data be organized and produced in a format other than standard reports generated routinely by the office, is it entitled to that information in a format of its own choosing?

These questions were first examined in detail by the Tennessee Supreme Court in 1998 in the case of *The Tennessean v. Electric Power Board of Nashville*.⁸⁴ In that case, the newspaper sought a computerized listing of names, addresses, and telephone numbers of customers from the Nashville Electric Service (NES) electrical utility. While NES admitted that the requested information was present in its computer system, NES refused the request on the ground that it did not possess a list or data compilation that contained only the specific information requested by the newspaper. In other words, it had the information, but such information was not organized into a “record” and therefore was not under the provisions of the public records act. Additionally, some of the phone numbers collected by NES were unlisted and raised confidentiality issues. Also, NES estimated that it would cost \$4,500 to develop a computer program to compile the information requested by the newspaper. Finally, due to an internal policy of NES to notify a customer of any requests for information about their account, the utility estimated that it would cost an additional \$86,400 to send first class mail notices to its entire customer group that the newspaper sought information about them.

The trial court ruled that NES had to produce the record because Tennessee's Public Records laws did not distinguish between records based on the format in which they were stored. However, the trial court decision was not pleasing to the newspaper because it allowed NES to recover all costs of producing the records including the \$86,400 required to notify customers of the access to the records.⁸⁵ Both parties in the case appealed the decision. Looking to cases from other jurisdictions,⁸⁶ the Tennessee Court of Appeals ruled that a records custodian did not have to collect or compile materials or create a record that did not previously exist for the benefit of a requestor.⁸⁷ The appellate court believed to rule otherwise could tax the resources of governmental agencies. The Tennessee Supreme Court however disagreed. It recognized the competing interests of the public's right to access and the government agency's burden of complying with requests; but, ultimately, the Supreme Court found that the Court of Appeals paid too much attention to the physical format in which the record is stored. It stated as follows:

...[O]nce information is entered into a computer, a distinction between information and record becomes to a large degree impractical. In our view, it makes little sense to implement computer systems that are faster and have massive capacity for storage, yet limit access to and dissemination of the material by emphasizing the physical format of a record.⁸⁸

Ultimately, the court also ruled that, although NES could recover actual costs incurred in producing and disclosing the requested records, it had no statutory authorization to require payment of costs to implement its own customer notification policy. To do so would inhibit the disclosure of public records.⁸⁹

This case is likely to become a landmark decision in Tennessee law. It significantly enhances the rights of the public in the computer era to access government information. It altered the prior understanding of the law which was that local governments did not have to create records that did not exist simply because someone asked for them. Now, if the data is computerized, the answer to the question of what records do and do not exist is less clear.

Remote Access to Computerized Records

Another development that has arisen with the advent of electronic records and the development of the Internet is the ability of citizens to access information remotely. County offices are authorized under Tennessee law to provide computer access and remote electronic access (for inquiry only) to information contained in the records of the office which are stored on computer.⁹⁰ Access may be provided both during and after regular business hours. The official who has custody of the records may charge persons using remote electronic access a reasonable amount to recover the costs of providing such services and no other services. The fee must be uniformly applied and must be limited to the actual costs of providing access. It can not include the cost of storage and maintenance of the records or the costs of the electronic record storage system.⁹¹ Any officials providing remote access to their computer records must implement procedures and utilize a system that does not allow records of the office to be altered, deleted or impaired in any manner. Any official choosing to provide this service must file a statement with the office of the Comptroller of the Treasury at least 30 days prior to implementing the system. The statement must describe the computer equipment, software and procedures that are used to provide access and to maintain security and preservation of the computer records. The state of Tennessee will not bear any of the costs of providing access.⁹² Once a system for providing access is in place, any member of the public willing to pay the fees must be allowed to have access to the records, including anyone desiring to use the information for proprietary purposes.⁹³

Similar provisions specific to electronic files of voter registration systems can be found elsewhere in the code.⁹⁴

A recent attorney general's opinion examined the question of whether a county official could provide remote access to public records through a private vendor.⁹⁵ In the circumstances described in the opinion, a vendor was allowed to upload a copy of the data stored on the computers in the office of the register of deeds in exchange for certain services provided by the vendor. The vendor then had the right to provide public access to the data via a subscription service. The attorney general opined that this agreement violated T.C.A. § 10-7-123. Specifically, subsection (a)(4) of that statute provides that once a remote access system is in place, access must be given uniformly to all members of the public who desire access so long as they pay the reasonable fees to the county official to cover the cost of actually providing the service. In this case, remote access was being provided by the county official only to one entity, the vendor, and denied to the rest of the public. The law does not prohibit a private vendor from selling subscriptions to the information which has been acquired from county offices.⁹⁶ But it does require the county official to provide equal access to the data to anyone willing to pay the access fee.

The attorney general has also been asked whether there was a problem with the criminal court clerk's office making records, including information about arrests, charges and disposition of cases, available on the Internet. The attorney general opined that the clerk could make such records available in that fashion, so long as the clerk still complied with orders to expunge records and insured they were removed from the Internet as well as the files of the clerk's office once an order compelling expungement was issued by the judge.⁹⁷ This standard applied whether a case led to a conviction or was disposed of through judicial diversion.⁹⁸

Denial of Access to Public Records—Liability

Any citizen of Tennessee who is denied the right to personal inspection of a public record in whole, or in part, is entitled to petition the court to review the actions that were taken to deny access and to grant access to the record.⁹⁹ Petitions may be filed in the chancery court for the county where the records are located or in any other court exercising equity jurisdiction in the county.¹⁰⁰ Upon the filing of the petition, the court shall, at the request of the petitioning party, issue an order requiring the defendant to appear and show cause why the petitioner should not be granted access to the record. No formal written response to the petition is required. The burden of proof rests on the person having custody of the records to show why public access should not be allowed.¹⁰¹ If the court determines that the petitioner has a right to inspect the records, they shall be made available unless the defendant timely files for appeal or the court certifies a question with respect to disclosure of the records to an appellate court.¹⁰² If a public official is required to disclose records pursuant to these procedures, he or she can not be held civilly or criminally liable for any damages caused by the release of the information.¹⁰³ If, however, the court determines that the government entity knowingly and willfully refused to disclose a public record, it may, in the discretion of the judge, assess all reasonable costs involved in obtaining the record, including attorney's fees, against the governmental entity.¹⁰⁴

To What Records Is the Public Entitled Access?

It has already been noted that the legislature intended the fullest possible public access to public records. But what are public records? Generally speaking, the courts have ruled that “[i]n those instances where documents have been made or received in connection with the transaction of official business by any governmental agency, then a presumption of openness exists, and the documents are public records within the meaning of T.C.A. § 10-7-503.”¹⁰⁵ As we have seen in the discussion above, access is not limited by the format in which the record or information is kept. However, the

presumption of openness is overcome whenever state law provides that a record shall be kept confidential.

Confidential Records

A lengthy statute in the Tennessee Public Records Act provides a laundry list of government records that must be kept confidential.¹⁰⁶ This statute is amended and added to on a regular basis by the General Assembly. The following list reflects the records designated as confidential by T.C.A. § 10-7-504 at the time of publication (current through the 2004 legislative session).

- Medical records of patients in state, county, and municipal hospitals and medical facilities;
- Any records concerning the source of body parts for transplantation or any information concerning persons donating body parts;
- All investigative records of the TBI, the office of the TennCare inspector general, all criminal investigative files of the motor vehicle enforcement division of the department of safety relating to stolen vehicles or parts, all files of the drivers' license issuance division and the handgun carry permit division of the department of safety relating to bogus drivers' licenses and handgun carry permits issued to undercover law enforcement agents;
- Records, documents, and papers in the possession of the military department that involve national or state security, including national guard personnel records;
- Records of students in public educational institutions (for more discussion of these records, see the following chapter on Student Records);
- Certain books, records, and other materials in the possession of the office of the attorney general relating to any pending or contemplated legal or administrative proceeding;
- State agency records containing opinions of value or real and personal property intended to be acquired for a public purpose;
- Proposals received pursuant to personal service, professional service and consultant service contract regulations, sealed bids, and related records before the state has finished its complete evaluation (note that an opinion of the attorney general has extended this confidentiality to similar records of local governments although they are not expressly mentioned in the statute¹⁰⁷);
- Investigative records and reports of the internal affairs division of the department of correction or the department of children's services;
- Official health certificates, collected and maintained by the state veterinarian;
- The capital plans, marketing information, proprietary information, and trade secrets submitted to the Tennessee venture capital network;
- Records of historical research value which are given or sold to public archival institutions, public libraries, or libraries of a unit of the board of regents or the University of Tennessee, when the owner or donor wishes to require that the records are kept confidential;
- Personal information contained in motor vehicle records;
- All memoranda, work notes or products, case files, and communications related to mental health intervention techniques conducted by professionals in a group setting to provide job-related critical incident counseling and therapy to law enforcement officers, EMTs, paramedics, and firefighters;
- All riot, escape, and emergency transport plans incorporated in a policy and procedures manual of county jails and workhouses or prisons operated by the department of correction or under private contract;
- In order of protection cases, any documents required for filing other than certain forms promulgated by the Tennessee Supreme Court;

- Computer software and manuals sold to state boards, agencies, or higher educational institutions;
- Credit card numbers of persons doing business with the state or a political subdivision and related identification numbers or authorization codes (see more on this topic at the end of this chapter);
- Credit card numbers, social security numbers, tax ID numbers, financial institution account numbers, burglar alarm codes, security codes, and access codes of any utility;
- Records that would allow a person to identify areas of structural or operational vulnerability of a utility service provider or that would permit disruption or interference with service;
- Contingency plans of governmental entities for response to violent incidents, bomb threats, ongoing acts of violence, threats related to weapons of mass destruction, or terrorist incidents;
- Records of any employee's identity, diagnosis, treatment, or referral for treatment by a state or local government employee assistance program;
- Unpublished telephone numbers in the possession of emergency communications districts;
- Employment records of state, county, municipal, or other public employees that contain unpublished telephone numbers, bank account information, social security numbers, and drivers' license information (except where driving or operating a vehicle is part of the employee's job duties) of the employee or an immediate family or household member (note that under the law, this information in employment records should be redacted whenever possible and not be used to limit or deny access to otherwise public information);
- Personnel information of undercover police officers;
- Records identifying a person as being directly involved in the process of executing a sentence of death; and
- Information that would allow a person to obtain unauthorized access to confidential information or to government property¹⁰⁸

This list of confidential records found in T.C.A. § 10-7-504 is not exclusive, however, and other statutes, rules, and the common law dealing with a subject matter can also make a specific record confidential.¹⁰⁹ While the following list is not exhaustive, these statutes are other legal sources that designate certain records that may be in the possession of a county office as confidential:

- All memoranda, work products or notes and case files of victim-offender mediation centers (T.C.A. § 16-20-103);
- Adoption records and related records (T.C.A. §§ 36-1-102 and following);
- Many records regarding juveniles (see T.C.A. §§ 37-1-153, 37-1-154, 37-1-155, 37-1-409, 37-1-612, 37-1-615 and 37-2-408);
- Certain records regarding the granting of consent to abortion for a minor and other records regarding abortion (T.C.A. §§ 37-10-304, 39-15-201 ff);
- Pursuant to T.C.A. § 38-7-110, all or a portion of a county medical examiner's report, toxicological report or autopsy maybe declared confidential upon petition by the district attorney on the grounds that release of such record could impair the investigation of a homicide or felony. Additionally, 2005 Public Chapter 216 made it a criminal offense for certain audio and video materials related to an autopsy to be release to an unauthorized person.
- Certain student information (see following chapter) ;
- Whistleblowing reports of violations the Education Trust in Reporting Act (T.C.A. §§ 49-50-1408);
- Certain records of an employer's drug testing program (T.C.A. § 50-9-109);
- Accident reports (T.C.A. § 55-10-114);

- Tax returns and tax information (T.C.A. § 67-1-1702);
- Business tax statements, reports, and returns as well as some information on business license applications¹¹⁰ (T.C.A. § 67-4-722);
- Information or records held by a local health department regarding sexually transmitted diseases (T.C.A. § 68-10-113);
- Patient medical records of hospitals and local or regional health departments (T.C.A. § 68-11-305); and
- Nursing home patient records (T.C.A. § 68-11-804).

Please note that this list only highlights some of the other provisions of the Tennessee Code that make records confidential. Additionally, the Tennessee Supreme Court has ruled that sources of legal authority other than statutes may make a record confidential. For example, the Tennessee Supreme Court has ruled that the Tennessee Rules of Criminal Procedure and Civil Procedure may also designate certain records as confidential.¹¹¹ Other records may be sealed by a court order or made confidential by a federal statute or regulation. If you have a question regarding the confidentiality of a specific record not listed above, contact your county attorney or CTAS county government consultant for assistance.

Maintenance of Confidentiality

Any record that is designated as confidential must be treated as confidential by the agency with custody of the record throughout the maintenance, storage, and disposition of the record. This includes destroying the record (if it is eligible for destruction) in such a manner that the record cannot be read, interpreted, or reconstructed¹¹². However, once a confidential record has been in existence more than 70 years, it shall be open for public inspection by any person unless disclosure of the record is specifically prohibited or restricted by federal law or unless the record is a record of services for mental illness or retardation.¹¹³ This “70-year rule” also does not apply to adoption records, records maintained by the office of vital records, and records of the TBI that are confidential.¹¹⁴

Special Considerations and Specific Types of Confidential Records

Social Security Numbers

Social Security Numbers (SSNs) have been a cause of concern and difficulty for many local government records custodians. The difficulty with SSNs is that they are confidential when held by certain government officials for certain purposes, but may not be confidential when part of a different record or kept by a different office, or collected in a different manner. There is a common public perception that SSNs should be kept confidential; but the public is also aware that this number is used by public and private entities for innumerable purposes. A local government official may possess social security numbers in the personnel records of his or her own employees; in license applications; voter registration forms; court petitions and evidence files; and in publically recorded documents. Sorting out when and how these records may be accessed by the public is, to say the least, confusing. The Tennessee attorney general summed this conundrum up nicely:

The federal and state laws involving social security numbers are as numerous and varied as the pieces of a patchwork quilt. There are laws requiring that SSNs be collected; laws that make SSNs public record; laws that make them confidential; even laws that make unauthorized disclosure of some records with SSNs punishable as a crime.¹¹⁵

The Federal Privacy Act of 1974, 5 U.S.C. § 552a; the Internal Revenue Code, 26 U.S.C. §§ 1402(g) and 7213; the Social Security Act, 42 U.S.C. § 405; and federal statutes on child and spousal support, 42 U.S.C. §§ 654a and 666(a)(13); as well as the Tennessee Public Records Act, T.C.A. §§ 10-7-503 and 10-7-504; a recent enactment regarding SSNs in the possession of state agencies found in T.C.A. § 4-4-125; and dozens of other provisions of the Tennessee Code all impact the recording and dissemination of SSNs. While this manual can provide some guidance and direction about how to treat SSNs, many questions about specific records will likely have to be addressed on a case by case basis by your county attorney or in a question to a CTAS consultant.

The Federal Privacy Act of 1974 generally prohibits federal agencies from disclosing a record without the consent of the individual to whom the record pertains.¹¹⁶ But this law applies to federal agencies and does not place such restrictions on state and local government officials. The act does, however, restrain state and local governments from denying an individual a right, benefit, or privilege simply because the individual refuses to disclose his or her SSN.¹¹⁷ There are two exceptions to this limitation. First, the number may be required if a federal statute so directs. This exemption allows the collection of SSNs on marriage, driver, and professional license applications as the federal statutes on child support enforcement mandate such disclosure.¹¹⁸ The second exemption applies in cases where the required disclosure was part of a record keeping system in place prior to January 1, 1975. This exemption allows Tennessee administrators of election to continue to require a SSN on a voter registration form since our voter registration statutes required that number for identification verification prior to that date. The act also requires federal, state, and local government agencies requesting disclosure of SSNs to indicate whether the disclosure is mandatory or voluntary, the legal authority under which the SSN is solicited, and the uses that will be made of it. Therefore, the Federal Privacy Act does not make SSNs in local government records confidential, but it determines when and how local governments may collect the number.

The Federal Internal Revenue Code prohibits the unauthorized disclosure of tax returns and tax return information (which would encompass the SSN) by officers and employees of the United State and by state and local officials who receive such information for certain specified statutory reasons.¹¹⁹ Basically, these purposes relate to income tax collection, certain law enforcement activities, and child support enforcement. Therefore, if a county official receives an individual's SSN specifically for one of these purposes, the official should not disclose the number or use that information for any purpose other than the one for which the official received it. The federal laws provides both civil and criminal penalties for doing so.¹²⁰

Still, these federal laws do not provide guidance for the accessibility of the majority of SSNs held by county officials. A state law enacted in 2001 and amended in 2002 established a rule that no state entity shall publicly disclose the SSN of any citizen of the state unless permission is given by the citizen, distribution is authorized under state or federal law, or the distribution is made to certain consumer reporting agencies or financial institutions specifically named in the statute.¹²¹ The attorney general has opined that this prohibition does not distinguish between internal and external dissemination, and that the statute requires express permission before dissemination even if the citizen voluntarily provided the SSN. If this statute applied to county governments, it would give a clear answer to the question of confidentiality, but it is limited in application to the state. There has been no indication to date that the term "state entity" should be interpreted to include local governments.

Two provisions that do clearly affect the status of SSNs in the possession of county officials are found in T.C.A. § 10-7-504(a)(16) and (f). The first provision relates to the ability of certain persons who are victims of domestic violence to request that government records which could be used to locate them

be kept confidential. This issue is discussed in detail below in a specific section related to these requests. The other provision makes the SSNs and other identifying information of county government employees confidential when it is held by the county in its capacity as an employer. This item is discussed above. A third statute related to the office of the register of deeds passed in 2003 to address problems arising from SSNs appearing in publically recorded documents. Under T.C.A. § 10-7-513, veterans and certain other persons may request that SSNs appearing in military discharge records in the register's office be redacted.

Because of the difficulty caused in managing records with SSNs and due to concerns over identity theft and fraud, the General Assembly has begun to remove requirements in the law that the number be included on documents where it is not essential. For instance, in 2003 the legislature amended T.C.A. §§ 34-3-104 and 34-2-104 to delete requirements for SSNs in petitions for appointing a conservator or in petitions for guardianship.¹²² That same year, the legislature enacted T.C.A. § 10-7-515, which prohibits preparers of any documents to be recorded in the register of deeds' office from including SSNs on any such documents except in the case of a power of attorney.

These legislative changes may ease the difficulties in dealing with SSNs or provide a clear answer for the confidentiality of these numbers in the future. For now, the local custodian of records should do his or her best to examine the type of record that contains the SSN and determine what it is and how it was collected. If it does not fall under one of the specific statutes discussed above and the record containing the number is otherwise a public record, there is probably no authority to keep the SSN confidential. However, a safe practice would be, whenever practical, to redact SSNs from copies of public records or records made available for inspection by the public unless the citizen expressly requests to see the SSN. If the requestor desires to specifically see the record with the SSN, you may need to consult legal counsel at that point whether or not to comply with the request. If legal counsel is unsure whether the record is confidential, it is a safer course to protect confidentiality and allow the requestor to petition the chancery court for access to the record. If the court orders disclosure, the records custodian is protected from liability for disclosure. Even if the court determines that the record should be disclosed, it is likely that a judge will find that the records custodian was acting in good faith by trying to protect the SSN. If you are aware that there are SSNs in your office in records that do not clearly fall within specific statutes making them confidential and it is not feasible to redact them all (for example SSNs that appear commonly in court case files and petitions), it is highly unlikely that any court will find that a county official has a duty to actively search out and redact such numbers. If citizens approach a county official with a request to make such records confidential, they may be directed to a judge to petition to have such documents placed under seal.

Motor Vehicle Registration Records

Access to motor vehicle registration records held by the Department of Safety, the Department of Revenue, or in the office of the county clerk when acting as an agent of those departments is restricted by both state and federal law. The federal Drivers Privacy Protection Act places restrictions on access to these records.¹²³ In addition, in 1996, our state legislature adopted the Uniform Motor Vehicle Records Disclosure Act that closely parallels the language of the federal act.¹²⁴ Under the provisions of these laws, personal information obtained by those government offices in connection with a motor vehicle record can not be disclosed except for specific purposes to certain authorized individuals or with the consent of the driver.¹²⁵ Personal information is defined to include information that identifies a person, including an individual's photograph, computerized image, social security number, driver identification number, name, address, telephone number, and medical or disability information.¹²⁶ Use of the information is generally allowed for governmental agencies in carrying out their functions.¹²⁷ Additionally, the statutes include about a dozen other authorized uses whereby certain private parties

have rights to access the records for those specified purposes.¹²⁸ If a county clerk is presented with a request for personal information from motor vehicle records from a private citizen or a company, he or she should compare the request to the restrictions and authorizations found in T.C.A. §§ 55-25-103 through 55-25-112 and 18 U.S.C. § 2721 through 18 U.S.C. § 2725 to determine whether the release of such information is lawful. The Tennessee Department of Safety, Division of Title and Registration may be able to provide county clerks with further guidance regarding these records if necessary.

Vital Records

To protect the integrity of vital records and to insure their proper use and the proper administration of those records, the General Assembly made it unlawful for a custodian of these records to permit inspection of, or to disclose information contained in vital records, or to copy or issue a copy of all or part of any such records except in strict accordance with procedures found in the law or in accordance with a court order.¹²⁹ But the law goes on to state that an application for a marriage license and the authenticating documentation for the events of birth, death, marriage, divorce or annulment of a marriage, in the possession of a county clerk, court clerk, state registrar, or other authorized custodian are public records and that verified information from such documents may be provided upon request. However, the information contained in the “Information for Medical and Health Use Only” section of a birth certificate and the “Confidential Information” section of marriage, divorce, or annulment certificates remains confidential.¹³⁰

Law Enforcement Personnel Records

A couple of specific statutory provisions provide extra protection to personnel records of law enforcement personnel. Under T.C.A. § 10-7-503(c), there are requirements that when personnel records of law enforcement officers are inspected, the custodian of the records must make a record of the inspection and inform the officer. The person wishing to inspect the records must provide his or her name, address, business telephone number, home telephone number, driver license number, or other appropriate identification prior to receiving access to the records. Within three days after the inspection, the officer whose files have been examined should be informed that the inspection has taken place; the name, address, and telephone number of the person making the inspection; for whom the inspection was made; and the date of the inspection.¹³¹

In addition to these notice provisions, T.C.A. § 10-7-504(g) provides that the personnel information of undercover officers may be segregated and maintained in the office of the chief law enforcement officer. Once segregated, the information is treated as confidential. The information to be segregated includes the address and home telephone number of the officer as well as the address or addresses and home telephone number or numbers of the members of the officer’s household and/or immediate family. Information in the file that has the potential, if released, to threaten the safety of the officer or the officer’s immediate family or household may be redacted if the chief law enforcement officer determines that it poses such a risk. Anyone denied access to the information may have the decision reviewed in a show cause hearing before the chancery court. These provisions are not to be used to limit or deny access to otherwise public information. This statute also does not limit access to personnel records by law enforcement agencies, courts, or other governmental agencies performing official functions.¹³²

Domestic Violence Prevention and Protection Documents

In addition to the large group of records made strictly confidential by state laws, there is another class of records that *may* be made confidential by a 1999 law. Chapter 344 of the public acts of 1999 amends T.C.A. § 10-7-504 to allow persons who have obtained a “valid protection document” to request certain information that could be used to locate them be kept confidential. Protection documents are

defined by the act and include such things as orders of protection and affidavits of directors of a rape crisis center or domestic violence shelter. If the individual desiring confidentiality presents one of these documents to the records custodian for the governmental entity and requests confidentiality, the custodian of the records may choose to comply with the request or reject it. If the request is rejected, the custodian must state the reason for denying the request. If the request is granted, the records custodian must place a copy of the protection document in a separate confidential file with any other similar requests, indexed alphabetically by the names of the persons requesting confidentiality. From that point on until the custodian is notified otherwise, any time someone requests to see records of the office, the records custodian must consult the file and ensure that any identifying information about anyone covered by a protection document filed with the office is kept confidential before allowing any record to be open for public inspection. "Identifying information" includes any record of the home and work addresses, telephone numbers, social security number and "any other information" regarding the person that could reasonably be used to locate an individual. That information must be redacted from the records of the office before anyone can be allowed to inspect the records of the office. Since it is difficult to ascertain what information could possibly be used to locate an individual, you are strongly cautioned against complying with such requests. Unless you are certain your office can redact all identifying information regarding an individual from all files of your office should probably reject such requests for confidentiality, citing the administrative difficulty in redacting the records. It is not mandatory for your office to comply with these requests. However, if you do comply and then fail to protect all such information, you may create liability for your office. .

County Hospital and Health Department Records and Ambulance Records

Special rules apply to medical records. They are governed primarily by T.C.A. §§ 68-11-301 and following. The definition of hospital used in those provisions is broad enough to include county health departments.¹³³ Certain hospital records are not public records.¹³⁴ Generally, the law requires that a hospital or health department is required to retain and preserve records which relate directly to the care and treatment of a patient for 10 years following the discharge of the patient or such patient's death during the period of treatment within the hospital.¹³⁵ Mental health records are treated differently. Hospitals and health departments are given the option of retaining records for a longer period of time if they wish.¹³⁶ As noted above, records held by a local health department related to sexually transmitted diseases are strictly confidential.¹³⁷

Records of ambulance services are similar in some respects to hospital records. There are a handful of statutes and regulations that specifically mandate the creation and retention of certain records related to the operation of ambulance services.¹³⁸ The information in run records that relates to the medical condition and treatment of the patient is specifically declared confidential.¹³⁹ Although the statutes and regulations do not establish retention period for all ambulance records, it is recommended that ambulance services should follow the general standard of a 10-year retention period for records that are medical in nature. Additionally, the rules of the Emergency Medical Services Division specifically require that ambulance dispatch logs should be retain for at least 10 years.¹⁴⁰

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, is a federal law that instituted dramatic reforms regarding the use of information in the health care and insurance industry. It created a great deal of apprehension among many private and public entities that were uncertain about whether the act impacted them as well. The Act required the Secretary of Health and Human Services to issue privacy regulations governing individual health care information. The privacy provisions of HIPAA are found in the ironically named "administrative simplification" provisions of the act. The goal of the privacy rule is to safeguard protected health information (PHI) while allowing

the free flow of health care information in the world of electronic commerce and transactions.¹⁴¹ Protected health information includes all individually identifiable health information held by a covered entity or its business associate in any form or media.¹⁴² In other words, it is made up of health and medical records that identify the individual to whom the record relates. The privacy rules apply to three types of entities: health plans, health care providers, and health care clearinghouses.¹⁴³ The easiest category to consider from the local government standpoint is the health care clearinghouse. This category deals with entities that process and re-format information being transmitted between entities. Counties will not fall under this category.

Health plans are individual and group health care plans that provide or pay the cost of medical care.¹⁴⁴ If your county provides health insurance for its employees through private insurance, the insurance carrier would be the health plan. If your county is self-insured, it is likely that in administering the self-insured health care plan, the county will have to comply with the privacy rules and may be covered by HIPAA. If you have a third party administrator, that entity may be handling most compliance issues for the county, but you should still evaluate your requirements under HIPAA. Technically your third party administrator is merely a “business associate” under the terms of HIPAA who falls under provisions of the law due to its relationship with the county’s health plan. Responsibility for compliance ultimately lies with the plan itself and not with its business associates.

Health care providers are also be covered by HIPAA if the provider electronically transmits health information in connection with certain types of transactions.¹⁴⁵ These include claims, benefit eligibility inquiries, referral authorization requests, or certain other transactions listed under the HIPAA Transactions Rule.¹⁴⁶ For example, the fact that your county may employ a nurse or doctor for the jail may make the county a health care provider; however, the county will only be a *covered* health care provider under HIPAA if those employees are electronically transmitting health information in conjunction with one of the listed transactions. If your sheriff does not employ personnel to provide medical services to the jail but merely contracts with another entity to provide the service, then the sheriff’s office would not be a covered entity.

Even if it appears that some aspects of county government may be considered covered functions under certain circumstances, it is possible for the county to declare itself a hybrid entity. Under the HIPAA regulations, a hybrid entity is a single legal entity that is covered, but whose covered functions are not its primary functions.¹⁴⁷ By being declared a hybrid entity, the county limits the application of the HIPAA requirements to only those county operations that are acting as a health care provider. For instance, a county operated ambulance service or hospital would need to comply with HIPAA as a health care provider if it transmits PHI electronically, but the register of deeds and county clerk’s offices, and other non-health care operations would not be covered.

Covered entities are required to provide notices and disclosures to individuals who have PHI held by the entity. If you have been to a doctor’s office in the last couple of years, you have probably seen these standard forms. Offices that are covered by HIPAA are also required to adopt privacy policies and procedures that are consistent with the privacy rule, must designate a privacy official responsible for implementing these policies, must conduct workforce training and management, must mitigate any harmful disclosures of PHI, must maintain reasonable appropriate safeguards to protect against improper disclosure of PHI, must have procedures for receiving complaints about privacy issues, and must meet certain documentation and record keeping standards.¹⁴⁸

The HIPAA rules and regulations are extremely complex and filled with exceptions, limitations, and modifications for various entities and transactions and will only apply to limited operations of local

governments if at all. For this reason, they are not discussed in depth in this manual. If you think your office or your county may be covered by HIPAA, you should discuss the requirements of the law with your county attorney and with any third party administrators or other health care consultants with which your county may contract. For more information about the law and associated rules, see the Web site for the HHS, Office for Civil Rights at <http://www.hhs.gov/ocr/hipaa>. A recent opinion of the Tennessee attorney general also gives instructions with regard to the release of health information under HIPAA for law enforcement purposes.¹⁴⁹

Credit Card Numbers and Credit Reports

As county governments have begun allowing citizens to use credit cards for payment of taxes and fees, government records keepers encounter some new regulations and challenges in managing records that contain information related to those credit accounts. As was noted above, credit card numbers of persons using an account to make payments to the government are confidential under T.C.A. § 10-7-504(a)(19). Additionally, there is information in the section of this manual dealing with electronic records that describes notification requirements that apply when a breach of security has allowed improper access to account information or other personal information that could be used for identity theft purposes.

Finally, local governments that use credit reports as a part of background checks must comply with the Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act (FACTA) and related rules and regulations of the Federal Trade Commission¹⁵⁰. The FCRA requires employers that use private agencies to perform background checks (whether related to credit history, criminal background or driving record checks) on job applicants to comply with notice, consent, and disclosure requirements related to such checks and reports. FACTA added the requirement that entities possessing consumer information related to these reports must properly dispose of such information in a manner that preserves confidentiality and requires those possessing such information to take reasonable measures to ensure against unauthorized access or use of the information. Therefore, if your county uses private reporting agencies for background checks during the employment process or for other purposes, make sure anyone in your county possessing this information properly protects this sensitive consumer information.

Student Records

There is another important group of records made confidential by a federal statute known as the Family Educational Rights and Privacy Act. Due to the intricacies of that law and the procedures regarding student records generally, those records are discussed in more detail in the following chapter.

S

Student Records

Both federal and state laws include special provisions to protect the confidentiality of records of students in Tennessee schools. Tennessee's public records statutes specifically provide for the confidentiality of such records.¹⁵¹ But more significant than our state statutes is a complex set of federal law that provides extensive regulations controlling the inspection, amendment, and disclosure of educational records. The primary federal statute addressing student records is the "Family Educational Rights and Privacy Act" (FERPA).¹⁵² This law outlines who can and cannot access student education records and establishes rights for both parents and students in regard to these records. The following outline of the requirements of FERPA is adapted from a January 2004 memo to superintendents of local school systems from the Family Policy Compliance Office of the U.S. Department of Education. Before relying on this information, local education officials should check with the attorney for their school board or county to make certain these regulations have not been amended. A copy of the full memo and additional material regarding FERPA and other federal laws and regulations can be found at the U.S. Department of Education Web site on the Internet at <http://www.ed.gov/policy/gen/guid/fpc/index.html>

The Family Educational Rights and Privacy Act

Statute: 20 U.S.C. § 1232g. Regulations: 34 C.F.R. Part 99.

The Family Educational Rights and Privacy Act (FERPA) provides that a local educational agency (LEA) that receives U.S. Department of Education funds may not have a policy or practice of denying parents the right to

- Inspect and review education records (34 C.F.R. § 99.10).
- Seek to amend education records (34 C.F.R. §§ 99.20 through 99.22).
- Consent to the disclosure of personally identifiable information from education records except as specified by law (34 C.F.R. §§ 99.30 and 99.31).

These rights transfer to the student when he or she turns 18 years of age or enters a post-secondary educational institution at any age ("eligible student").

Local education agencies (LEAs) must annually notify parents and eligible students of their rights under FERPA. 34 C.F.R. § 99.7. The annual notification must also include

- The procedure to inspect and review education records;
- The procedure to request amendment of education records;
- A specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest if the agency or institution discloses or intends to disclose personally identifiable information to school officials without consent; and
- The right of parents to file a complaint with the Family Policy Compliance Office (FPCO) in the Department. (A model FERPA notification follows this outline and is also available on FPCO's Web site, www.ed.gov/policy/gen/guid/fpc.)

If the LEA or educational institution under the LEA discloses directory information from education records without consent, it is required by 34 C.F.R. § 99.37 to notify parents and eligible students of

- The types of information the LEA (or institution) has designated as directory information (see 34 C.F.R. § 99.3 “Directory information” for definition);
- The right to opt out of disclosure of directory information. (A model “directory information” notice also follows this outline and is available on FPCO’s Web site www.ed.gov/policy/gen/guid/fpcoc.)

LEAs must also comply with FERPA’s redisclosure and recordation provisions, set forth in 34 C.F.R. §§ 99.32 and 99.33, except for disclosures that are specifically exempted.

Outlined below are changes in the No Child Left Behind Act (NCLB) that do not amend FERPA, but relate to the disclosure of personally identifiable information from students’ education records.

Suspension and expulsion disciplinary records:

- Section 4155 of the Elementary and Secondary Education Act of 1965 (ESEA), 20 U.S.C. § 7165, as amended by the NCLB, requires that each state have “a procedure in place to facilitate the transfer of disciplinary records, with respect to a suspension or expulsion, by local educational agencies to any private or public elementary school or secondary school for any student who is enrolled or seeks, intends, or is instructed to enroll, on a full- or part-time basis, in the school” no later than January 8, 2004. LEAs should include a notice in their annual notification of rights under FERPA that they forward education records to other schools that have requested the records and in which the student seeks or intends to enroll (34 C.F.R. §§ 99.7 and 99.34(a)(ii)). (See enclosed model notification of rights.)
- Section 9528 of the ESEA, 20 U.S.C. § 7908, as amended by the NCLB, and 10 U.S.C. 503, as amended by § 544 of the *National Defense Authorization Act for Fiscal Year 2002* (Pub.L. No. 107-107), require LEAs to
 - give military recruiters the same access to secondary school students as provided to postsecondary institutions or to prospective employers; and
 - provide students’ names, addresses, and telephone listings to military recruiters, when requested, unless a parent has opted out of providing such information. (Military Recruiter Guidance is on FPCO Web site.)

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students over 18 years of age ("eligible students") certain rights with respect to the student's education records. These rights are:

(1) The right to inspect and review the student's education records within 45 days of the day the School receives a request for access.

Parents or eligible students should submit to the School principal [or appropriate school official] a written request that identifies the record(s) they wish to inspect. The School official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

(2) The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate.

Parents or eligible students may ask the School to amend a record that they believe is inaccurate. They should write the School principal [or appropriate school official], clearly identify the part of the record they want changed, and specify why it is inaccurate. If the School decides not to amend the record as requested by the parent or eligible student, the School will notify the parent or eligible student of the decision and advise them of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

(3) The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.

One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the School as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the School Board; a person or company with whom the School has contracted to perform a special task (such as an attorney, auditor, medical consultant, or therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

[Optional] Upon request, the School discloses education records without consent to officials of another school district in which a student seeks or intends to enroll. [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]

(4) The right to file a complaint with the U.S. Department of Education concerning alleged failures by the *School District* to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-5901

[NOTE: In addition, a school may want to include its directory information public notice, as required by § 99.37 of the regulations, with its annual notification of rights under FERPA. A sample directory information public notice can be found on the following page.]

Model Notice for Directory Information

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that [School District], with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, [School District] may disclose appropriately designated "directory information" without written consent, unless you have advised the District to the contrary in accordance with District procedures. The primary purpose of directory information is to allow the [School District] to include this type of information from your child's education records in certain school publications. Examples include:

- ▶ A playbill, showing your student's role in a drama production;
- ▶ The annual yearbook;
- ▶ Honor roll or other recognition lists [Note: Under Tennessee law, you may not want to treat these lists as directory information. See material below relative to Tennessee statutes];
- ▶ Graduation programs; and
- ▶ Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, upon request, with three directory information categories - names, addresses and telephone listings - unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.⁽¹⁾

If you do not want [School District] to disclose directory information from your child's education records without your prior written consent, you must notify the District in writing by [insert date]. [School District] has designated the following information as directory information; [Note: an LEA may, but does not have to, include all the information listed below.]

- ▶ Student's name
- ▶ Participation in officially recognized activities and sports
- ▶ Address
- ▶ Telephone listing
- ▶ Weight and height of members of athletic teams
- ▶ Electronic mail address
- ▶ Photograph
- ▶ Degrees, honors, and awards received
- ▶ Date and place of birth
- ▶ Major field of study
- ▶ Dates of attendance
- ▶ Grade level
- ▶ The most recent educational agency or institution attended

Footnotes:

1. These laws are: Section 9528 of the ESEA (20 U.S.C. 7908), as amended by the No Child Left Behind Act of 2001 (P.L. 107-110), the education bill, and 10 U.S.C. 503, as amended by section 544, the National Defense Authorization Act for Fiscal Year 2002 (P.L. 107-107), the legislation that provides funding for the Nation's armed forces.

Educational Records of Disabled Students

Certain students in the care of a local education agency have medical conditions, physical or mental disabilities or other special needs that affect and determine the educational services rendered to the child. With such children, significant amounts of medical records may be included in the educational records of the student. Specific requirements and regulations control the management of these records. The Tennessee Department of Education offers the following information in regard to these records.

When must a school district destroy a disabled student's records?

This is an important administrative question because student records may contain test results, evaluations, past Individualized Education Program (IEPs), correspondence, due process hearing transcripts, IEP meeting minutes, and teacher-produced anecdotal records, etc.

The governing authority is found at 34 C.F.R. Section 300.573.

300.573 Destruction of information.

(a) The public agency shall inform parents when personally identifiable information collected, maintained, or used under this part is no longer needed to provide educational services to the child.

(b) The information must be destroyed at the request of the parents. However, a permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation.

Subpart (a) requires schools to notify parents when materials in the student's record are deemed no longer necessary to provide appropriate services. In other words, schools may begin the removal of surplus materials any time that the information is judged to be of no value to the design or implementation of the child's educational program.

Subpart (b) requires that schools destroy such personally identifying but unnecessary records upon the parents' request. In short, when records are declared surplus, they must be destroyed when the child's parents ask that this be done. However, school districts may retain a permanent record of the "student's name address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed..." even if the parents request that the entire student record be destroyed. Best practice would be to retain the above listed information in perpetuity.

34 C.F.R. 300.560 defines destruction as "physical destruction or removal of personal identifiers from the information so that the information is no longer personally identifiable."

Must a school district keep student records for a specific time period?

Schools receiving federal funds are required to keep for three years records necessary to show their compliance with federal and state mandates, (34 C.F.R. Section 76.730, financial records, and Section 76.731, program compliance requirement, Section 80.42, retention and access requirements for records).

Under previous law, (34 C.F.R. Section 76.734 abrogated) the required retention period was five years. This regulation was the basis of several OSEP policy letters contributing to a continued confusion about the required retention period.

How may a school district keep records for three years, as stated above, and still comply with a parent's request to destroy personally identifiable information that is no longer needed to provide educational services to their child?

The school district may remove any reference, which makes the information personally identifiable while still maintaining the records proving compliance with state and federal programs, 34 C.F.R. 300.560.

Tennessee Statutes Affecting Education Records

Confidentiality

While the federal act provides a much more comprehensive treatment of the law on student records, Tennessee's public records act also classifies student records as confidential. T.C.A. § 10-7-504(a)(4) reads:

“The records of students in public educational institutions shall be treated as confidential. Information in such records relating to academic performance, financial status of a student or the student's parent or guardian, medical or psychological treatment or testing shall not be made available to unauthorized personnel of the institution or to the public or any agency, except those agencies authorized by the educational institution to conduct specific research or otherwise authorized by the governing board of the institution, without the consent of the student involved or the parent or guardian of a minor student attending any institution of elementary or secondary education, except as otherwise provided by law or regulation pursuant thereto and except in consequence of due legal process or in cases when the safety of persons or property is involved. The governing board of the institution, the department of education, and the Tennessee higher education commission shall have access on a confidential basis to such records as are required to fulfill their lawful functions. Statistical information not identified with a particular student may be released to any person, agency, or the public; and information relating only to an individual student's name, age, address, dates of attendance, grade levels completed, class placement and academic degrees awarded may likewise be disclosed.”

Like FERPA, this statute requires parental consent for disclosure of records except for the case of directory information. It allows access in cases where there is a danger to person or property on in accordance with legal process. Because the language in our state statute appears more restrictive than FERPA with regard to academic performance information, most attorneys in Tennessee are advising LEAs to get prior consent before publishing honor rolls or anything else regarding a student's academic performance. This is the one exception to the definition and examples of directory info under FERPA that you may want to keep in mind.

Educational Records as Evidence in Judicial Proceedings

In 2002, the General Assembly passed a comprehensive law entitled the Educational Records as Evidence Act to establish detailed procedures governing the production of subpoenaed student educational records.¹⁵³ The act provides that it is sufficient to comply with a subpoena requesting educational records for the custodian of the records to furnish a true and correct copy of the records within five days of the subpoena in cases where the school is neither a party to the action nor the place where any cause of action is alleged to have arisen.¹⁵⁴ The act requires that the records be enclosed in a separate sealed inner envelope and addressed to the appropriate court clerk, deposition officer, or

party.¹⁵⁵ The envelope remains sealed until opened at trial or other appropriate time in the presence of all required parties. Prior to the opening of the envelope, the act requires that the judge or presiding individual first determine that either (1) the records have been subpoenaed at the instance of an involved student, parent, or the student or parent's counsel; (2) the involved student or parent has consented and waived confidentiality; or (3) the records have been subpoenaed in a criminal proceeding.¹⁵⁶ The act requires the custodian of records to submit an affidavit with a copy of the records certifying the authenticity of the records, providing that the records were prepared by the personnel of the school or persons acting under their control and certifying the reasonable charges of the school for furnishing such copies.¹⁵⁷ The act provides that the furnished copies and the affidavit of the custodian of the records are admissible into evidence as though the original records were produced and the custodian were present to testify.¹⁵⁸ Multiple affidavits may be filed where more than one person has knowledge of the facts.¹⁵⁹ The act requires a subpoena to contain a clause stating that a copy of the records and an affidavit are not sufficient if the original school records or the personal attendance of the custodian of records is required.¹⁶⁰ Where original records are introduced, the act permits the substitution of copies thereof and the return of the original records after their introduction.¹⁶¹ Charges for copies and production of the records are allowed as a court cost.¹⁶²

Non-Custodial Parents

Any parent who does not have custody of a child, or if the parents have joint custody, the parent not residing with the child, may request in writing that a copy of the child's report card, notice of school attendance, names of teachers, class schedules, standardized test scores and any other records customarily available to parents be furnished directly to the non-custodial or non-resident parent.¹⁶³ However, a judge with jurisdiction over the custody of the child may, upon showing of good cause, deny any information concerning the residence of the child to the non-custodial or non-resident parent.¹⁶⁴

Record Keeping Duties of the Director of Schools

The director of a local board of education is given specific responsibility under the statutes that spell out his or her duties to keep certain records in specific formats and under certain conditions.¹⁶⁵ The director is charged with keeping a complete and accurate record of the proceedings of all meetings of the school board and the director's official acts and a detailed and accurate account of all receipts and disbursement of the public school funds in both well bound books and in electronic disks. These records must be kept in a location that is secure from the effects of natural disasters, to include fires, earthquakes, tornadoes and other catastrophic events.¹⁶⁶ The law also provides that the director must deliver to his or her successor all records and official papers belong to the position. A failure to do so is a separate Class C misdemeanor for each month during which the director withholds the records.¹⁶⁷

Conclusion

Both federal and state laws place extensive restrictions on access to student records. It is possible that violations of these regulations could result in legal action under federal civil rights laws. Therefore, the privacy concerns of students and parents should be taken most seriously. The sample notices provided in this section should help local education officials comply with applicable regulations and keep parents informed regarding the rights of their children. Due to the breadth of this publication, these issues cannot be addressed more thoroughly in this manual. The Tennessee Department of Education and the U.S. Department of Education are a good source for additional information. These agencies both provide significant amounts of relevant information on their Internet sites. It is suggested that local education personnel needing further guidance contact these agencies.

PART THREE
RECORDS
MANAGEMENT

The Basics

Whether or not you realize it, you already have a records management program. The problem is, it may be doing more harm than good. If your records are filed in a haphazard manner, if you don't know exactly what you have and where you have it, if it takes you too long to find what you need, if your office space is packed to the ceiling with file cabinets and boxes, if records are stored in unsuitable locations, if you throw away records too soon, or if you don't destroy records often enough, you could benefit from spending a little time, effort, and resources on implementing a beneficial records management program for your office. The information in the following pages should assist you by providing a crash course in basic records management. While earlier parts of this manual were designed to provide direction and information to members of the county public records commission, this part is primarily intended to help the elected or appointed county official or department head learn how to get a good grasp on records management for his or her individual office.

Step One: Evaluate

The first thing to do is find out exactly where you are. Begin with an evaluation of the current state of the records of your office. Performing an inventory of your stored records is fundamental to efficient records management and gives you some hard data with which to make sound decisions. It is virtually impossible for a county office to get any sort of handle on its records situation unless it knows, with some degree of exactness, what records are in storage, how much of them there are, and how old they are.

Inventory

Once you have selected someone to do the inventory, make sure they understand the information you need and the goals of the inventory. Your office may wish to use the sample Records Inventory Worksheet located in Appendix F to this manual as a guide for performing an inventory. "The general goals of the inventory should include

- ▶ Identifying the various records series in each office,
- ▶ Describing all record locations and storage conditions,
- ▶ Providing dates and other useful information,
- ▶ Measuring space and equipment occupied by records, and
- ▶ Providing a basis for writing records retention schedules."¹⁶⁸

The inventory will be beneficial to your office in a number of ways.

1. Obviously, it will tell you exactly what records you have and where to find them. This alone will increase the efficiency of your office.
2. It will help locate records that you can get rid of. Using the inventory and the records retention schedules for your office that are located in Part Four of this manual, you will probably discover a number of records that are unnecessarily taking up space in your office or your storage area.
3. It will identify records that are in danger. Paper records can be easily damaged by water or even excessive humidity or other environmental problems. If your inventory finds evidence of water damage to records, mold and mildew, or signs of damage from vermin, insects or other pests, take steps to remedy these problems before your office loses vital information. See the chapters in this part on *Proper Storage Conditions* and *Disaster Preparedness* for advice about dealing with these problems and establishing a safe environment for storing records long term.

Filing Systems

After you have evaluated the inventory of the records your office keeps, spend some time evaluating your filing system as well. If improvements can be made to the way you file records, you will improve administrative efficiency in your office and reduce costs. “If every employee of an agency of local governments spends even 5 percent of the time searching for hard-to-find information, that time translates into very substantial sums of money, and quality of services is sure to suffer.”¹⁶⁹ A good filing system will provide two major benefits to the people using it: *precise* retrieval and *timely* retrieval.¹⁷⁰ Another way of thinking about these issues is to ask “Can I find *what* I want *when* I want it?” If your filing system results in records retrieval that takes too long, that only gives you part of what you want, or gives you back much more than you needed, it is inefficient. Poor filing system performance is generally attributed to seven major factors.

- (1) Inadequate management attention;
- (2) Poor organization and structure of files;
- (3) Poor labeling and indexing procedures;
- (4) Uncontrolled growth of records;
- (5) A high incidence of missing, misfiled, or lost records;¹⁷¹
- (6) Inadequate and/or poorly trained files personnel; and
- (7) Inadequate or no formal record-keeping procedures.¹⁷²

If your employees spend even 5 percent of their time searching for files or information, that translates into substantial sums of money on an annual basis.

Filing Equipment

You may think all filing cabinets are alike, but that is just not true. Do not simply assume the storage system you have cannot be improved upon. You have options to consider. Movable-shelving, color-coded open-shelving systems and even bar-coding have become common in many offices that handle a large volume of records. The old standard vertical-drawer filing cabinet first came into use in the late 19th century and many records managers consider these cabinets to be functionally obsolete for most modern office applications. “[The vertical-drawer file cabinet] is the most costly of all filing equipment, since it requires more floor space and more physical time and effort to access the folders. It also does not provide the full benefit of visual retrieval aids, such as special labeling and color coding.”¹⁷³ If you know your filing system is inefficient, consider checking into more modern equipment. Although it will cost money initially, it may save money in the long run by saving floor space in your office, thereby postponing the need for expansion or relocation, and by reducing staff time that is wasted on an inefficient filing system with cumbersome storage units.

Step Two: Develop Records Disposition Authorizations (RDAs)

Your first question is probably “what is an RDA?” The acronym RDA stands for Records Disposition Authorization. An RDA provides a formal statement of when a record can be destroyed and what authority serves as the basis for its destruction. This document can, however, be much more. A comprehensive RDA becomes a plan for the entire life of a record series from creation to final disposition. Among other things, a comprehensive RDA should include

- a basic description of a record series;
- information about how the record is created;
- how it is used;
- where it needs to be stored;

- what format it needs to be kept in;
- who should have access to the record;
- how long it is in active use by an office;
- when to move a record into inactive storage;
- whether a record is vital or confidential; and
- whether or not the record can be destroyed.

RDAs and the retention schedules found in Part Four of this manual differ in a number of ways. The retention schedules describe the various records of an office, state if a record is permanent, identify the minimum amount of time a temporary record must be kept and state a legal authority or rationale for

RDAs are fundamental to an efficiently operating records management program in any office with a large volume of records.

that retention period. They generally do not tell you where to keep a record, how long the record may be in active use, and when a record can be moved to inactive storage or an archive. Those determinations are office-specific based on the resources available to you and the operating procedures of your office. The Retention Schedules will provide you with the foundation for writing your RDAs; but you are encouraged to consider them only a starting point. If your office handles a large number of records and a lot of people deal

with them, consider putting more than the minimum into your RDAs.

RDAs are fundamental to an efficiently operating records management program in any office with a large volume of records. RDAs allow an official to summarize on a single form what records are outdated and eligible for disposal, and then use that form to request permission from the County Public Records Commission to destroy. Such authorizations may be *continuing*, i.e. ready to use whenever records of a particular type have reached the end of their life-cycle and may be destroyed or placed in an archive. Once created, the RDA would only need periodic review to ensure that the plan you laid out for a group of records still makes sense and complies with your needs and any applicable legal requirements. Each office should have a set of RDAs that covers all the records it creates as well as older ones it inherits. (See the sample RDA Form developed by the Tennessee State Library and Archives which is located in Appendix G of the manual. This form may be copied and used to submit RDA's to the records commission.)

The following general principles and considerations may be helpful in making decisions about how to manage your records. They are quoted verbatim from the Tennessee State Library and Archives Tennessee Archives Management Advisory entitled *Appraisal and Disposition of Records*.

- If a legislative mandate requires permanent or temporary retention of any record, set of records, or class of records, then the record(s) specified in the mandate must be kept at public expense for at least so long as the mandate requires.
- A record or set of records should be retained by an agency so long as it is useful to performance of its routine functions.
- A decision to retain records beyond such active usefulness or legislative mandate is a decision to maintain them in such condition that they can be examined readily by the public. Such a decision requires a commensurate commitment of resources to continuous care and custody for the entire term of retention.
- A decision for permanent retention is a decision for perpetual care.

- Records should not be kept beyond their useful life in the public interest.
- No record that is necessary to the public interest should be destroyed.
- Records that are retained beyond their active usefulness to the routine functions of an agency must be of sufficient public interest to justify the expense of keeping and administering them, and the justification should be clearly stated, understood, and agreed to before accepting the responsibility and paying the cost to retain the record(s).
- The following kinds of records may all be appraised as having archival value for permanent retention:
 - (1) essential records that are needed to resume or continue operations or to recreate legal and financial status after disaster, or that are needed to protect or fulfill obligations;
 - (2) records that have lasting value as legal and fiscal evidence to account for responsible government; and
 - (3) records that are of such high evidential and historical value that they should be retained at public expense for the sake of a sound, reliable, and comprehensive understanding of the political, social, economic, and historical context of government and culture.

Step Three: Develop Written Policies and Procedures

Both large and small offices can benefit from having written records management policies on certain issues. The policies should adopt the Records Retention Schedules in this manual, incorporate any Records Disposition Authorizations developed by your office, and include policies for dealing with inactive records, for allowing public access to records and making copies, for responding to emergencies that threaten records, for maintaining confidential records, for keeping records in alternative storage media, and for interacting with the county public records commission, the Tennessee State Library and Archives, and a records center or archive if one is in existence in your county. If you think your office has had or may have a problem with files being lost, stolen, or misplaced, develop a policy and procedures for tracking files as well. Require anyone removing a file from its storage space to fill out a “sign-out” sheet indicating who they are, what record they are taking, and the date of its removal. This procedure should help your office track down misplaced records and cut down on losses. If you have an active records commission in your county, it may have already used its authority to develop policies on some of these issues. In that case, you could simply incorporate the commission’s policies into your office procedures.

Step Four: Continuing Maintenance

The best records management program will quickly fall into obsolescence if the office does not make efforts to stay on top of things. Records, particularly government records, grow at an astronomical rate. If you do not take steps to regularly move inactive records to other storage and destroy temporary records when they become eligible for destruction, they will soon begin to fill up your filing equipment, then your office, and bring clutter and disorganization to all operations. Consider implementing a “records clean-up day” for annually re-assessing the records of the office to identify what can be moved or destroyed. Select a time that is not in the middle of your busy season (perhaps around the holidays) and designate a day for everyone to identify records that can be destroyed and collect them.

Appoint a Records Management Officer

You may want to appoint one person within the office to be a records management officer. Having a single person responsible for records management efforts made within your office and to coordinate communication about your records with entities outside your office (the county public records commission, a records center, or an archives) can be a key to achieving success. The person should have good organizational skills, but should obviously not already be overwhelmed with too many other

duties to be able to devote any time to records management. It may surprise you to hear that almost one-fourth of local governments have a full time records officer.¹⁷⁴ Having an appointed records management officer who can designate part of his or her time year-round to keeping the office files current will go a long way toward insuring that your records management program succeeds.

Conclusion

Performing an inventory and putting workable RDAs in place are crucial to a smoothly operating records office. They provide a 'paper trail' and documentation on how an office manages the records it holds in trust. RDAs also provide a useful bridge from one office holder or administration to the next—a clear set of instructions regarding the care and disposition of the records that are the main product of that office's work. They help avoid congestion and inefficiency. This introductory information on records management hopefully has given you some ideas for addressing problems in your office and improving your system of record-keeping. Next this manual will discuss related records management issues in more detail, such as the steps you follow to dispose of a record, how the official interacts with the public records commission, proper environmental storage conditions for records, developing records centers and archives, the use of alternative storage media such as microfilm and electronic formats, preparing for disasters and protecting your vital records.

D

isposal of Records

Even the best planned and operated records program will fail miserably if it never gets rid of records. Simply keeping and storing away every record—in short, the “out of sight, out of mind” version of records management—is not a viable or responsible option. In order to find what you need and preserve what you need to keep, you have to eliminate records that no longer have any value. That is where disposal comes in.

Checks and Balances

Disposing of the records of a county office is not as simple as hauling them out to the trash when you get tired of them. Because these records can be of great importance to so many people, there are a number of procedural checks and balances to go through in order to lawfully dispose of records, whether the disposition is by destruction or transfer of the records to another institution. For many records, the official who has custody of the record, the county public records commission, the Tennessee State Library and Archives, and, for court records, a judge, all need to be involved in determining the final disposition of the record.

What Kind of Record Is It?

When trying to decide what to do with records, the first step is to identify them and classify them. The retention schedules found in Part Four of this manual will tell you how long a record needs to be kept. Find the description in the schedule that matches the record you are considering and see what the table indicates. For disposition purposes, records will fall into one of three classes: working papers, temporary records, and permanent records. The procedures for disposing of each of these classes are different.

Working Papers

Working papers are defined as “those records created to serve as input for final reporting documents, including electronic processed records, and/or computer output microfilm, and those records which become obsolete immediately after agency use or publication.”¹⁷⁵ This class of records comprises all those little records that come and go in the course of a day that we usually do not even think about as records. Whether it’s notes for a meeting or a rough draft of a report, if the record becomes obsolete after you use it, consider it a working paper. The good news about working papers is that they are easy to get rid of. Any public record defined as a working paper may be destroyed in accordance with the rules and regulations adopted by the public records commission without retaining the originals of such record and without further review by other agencies.¹⁷⁶ Any rules and regulations of a public records commission regarding working papers should be liberal, allowing county officials to eliminate these records as easily as possible before they become burdensome. Many working papers generated by county offices are extremely informal types of records. Because of that officials may not find anything in the retention schedules that describes them. Consider whether the record matches the definition above when trying to determine if it is a working paper.

Temporary Records

If a record needs to be kept around for some reason after its initial use, then it is at least a temporary record. Temporary records are officially defined as “...material which can be disposed of in a short period of time as being without value in documenting the functions of an agency.”¹⁷⁷ Financial and payroll records are good examples. Payroll records have fulfilled their immediate purpose once your employees receive their checks. But those records also must be kept in order to comply with federal

statutes and regulations and are important documents in the case of an audit. (See the discussion entitled “Special Considerations,” later in this section for more information records and audits.) Most of these retention periods are fairly short (three to five years) and therefore it is simplest to keep most temporary records in their original paper format during this retention period. For a few classes of temporary records, the retention period is long enough or the class of records is so voluminous that it may be helpful and cost effective to transfer the record to a different format for storage during the retention period. This will be discussed in the section on *Alternative Storage Formats* later in this part. Additionally, some temporary records may only exist in electronic format and will never be printed on paper. The law allows this practice as long as certain conditions are met (again, see the section on *Alternative Storage Formats* for more details). Regardless of what form the record is in (paper, computer disc, microfilm) the period of retention is determined by the *content* of the record and not its *format*. Although they take up less space, electronic records also need to be managed and preserved or destroyed in accordance with retention schedules and RDAs.

Once a temporary record has been retained for the period described in the schedule, then, like a working paper, it may be destroyed in accordance with the rules and regulations of the county public records commission.¹⁷⁸ The rules of the records commission should require the official wishing to destroy temporary records to notify the commission of the kind of record to be destroyed and cite an authority for its destruction. An easy way to do this is to use the five-digit code number that appears with each listing in the retention schedules in Part Four of this manual as a reference for the authorization to destroy the record. Although your county public records commission may wish to individually review each request to destroy temporary records before approving destruction, it may also provide for a less cumbersome procedure.

Continuing Authorization for Destruction of Temporary Records

The Tennessee State Library and Archives has agreed that county public records commissions can provide “continuing authorization” to destroy records so long as the official is complying with the schedules in this manual. (See the policy statement from that agency that precedes the records retention schedules in Part Four of this manual.) If your records commission adopts the retention schedules in this manual and adopts rules that allow for continuing authorization, it is recommended that all officials request continuing authorization from the commission. Once granted, they would only need to notify the commission when records are being destroyed in compliance with the schedule, identifying the type, age, and quantity of the records, and would not have to wait for further authorization or approval to proceed.

For example, many payroll-related records need to be kept for three years. The retention schedule for *Employment Records* in Part Four of this manual describes those records and cites the federal regulations that establishes that retention period. To use continuing authorization to dispose of these records, use the following steps:

1. The public records commission should adopt the retention schedules in this manual.
2. The official who has custody of the records should develop an RDA that describes the records he or she believes fall into these records classes.
3. The public records commission should review the RDA to make sure it describes records which appropriately fall under the chosen retention period and then approve the RDA.
4. Once the RDA is approved, the official can begin destroying all records that are covered by the RDA which have been kept for the length of time designated in the retention schedule. As time passes and more records pass the threshold for destruction (in this case three years), the official can automatically destroy the records and send a brief notice to the records commission informing it of this action.

This process can continue indefinitely, without the need to make formal requests or wait on approvals, until such time as the official or the records commission determines that the RDA needs to be revised or reconsidered.

Permanent Records

Permanent records are records of such value that they must always be retained in some kind of permanent format. Examples of permanent records are the deeds filed in a registers office, the minutes of the county commission, and the original process in a civil or criminal proceeding. Some records, like deeds, are kept permanently because the record continues to have legal significance in perpetuity. Other records are permanent because they preserve certain information about the way we live and conduct government and are therefore valuable historically. Still others are useful for statistical or planning purposes. Then there are those that are permanent simply because there are laws that have declared them to be so. All of these need to be kept in such a manner as to preserve them indefinitely. So, you may be wondering why permanent records are mentioned at all in this chapter on *Disposal of Records*. This is because, while the information in the record must be preserved, you do not necessarily have to keep the original paper copy of these records.

No permanent public record may be destroyed unless a majority of the public records commission agrees.

Duplication of Permanent Records

If you can safely and successfully convert paper records into another permanent media that is easier to store, the original paper version of the records can be destroyed although this is not recommended as a general practice.¹⁷⁹ This is where the checks and balances are extremely important. No original permanent public record may be destroyed under the law unless a majority of the county public records commission agrees.¹⁸⁰ The records commission should take this review seriously and make certain that the original records were completely and accurately reproduced into a durable medium by the official or his or her contractor before giving approval to destroy the paper. Before destruction, there are also notice requirements that must be complied with which will be discussed below. There are two major types of alternative storage formats for records that are recognized in the law: photographic and electronic. These formats will both be discussed in more detail in the next chapter. In addition, that chapter will review the legal authority and proper procedures to follow in copying permanent records into these formats and destroying the originals.

Notice Requirements in Destroying Original Copies of Permanent Records

Even after authorization for destruction of original paper records has been granted by the county public records commission, no *permanent value* record may be destroyed until notice is given to the Tennessee State Library and Archives of the intent to do so. Notice is to be given at least 90 days prior to destroying the records.¹⁸¹ Upon receiving notice, the staff of the state archives is directed to examine the records approved for destruction and take into its possession any records believed by the state archivist to be of historical value for permanent preservation. If the records commission receives no reply after nine months from the date of providing notice to the Tennessee State Library and Archives of the intent to destroy records copied onto computer media, it may proceed with the destruction of the records described in the notice.¹⁸² However, county officials should note that the Tennessee State Library and Archives considers the wisdom of this practice to be very questionable and should only be used in rare cases if ever.

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.¹⁸³ 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.

Methods of Destruction

This may seem to be a simple question, but officials often ask “how should I destroy a record?” For many working papers and some temporary records of an office, tossing them in the trash, or better yet, recycling them, is appropriate. However, if there is a possibility that confidential information is included in the records, they should be disposed of in a manner that obliterates this information such as shredding or burning.¹⁸⁴ The employees of your office would probably prefer that old temporary payroll records of your office which may contain their social security numbers not be put into a trash bin where someone could sift through them. Similarly, even though the information may be public while it is in your custody, many citizens would prefer that taxpayer records, vehicle registrations and other county records are obliterated when they leave your custody and don’t end up blowing around in a landfill for anyone to find. Computer records that are eligible for destruction should be fully deleted with storage disks destroyed, reformatted or over-written with new information to eliminate traces of the old files.

Special Considerations

Various law provides for some special considerations for certain records or types of records. These requirements should be considered when an official or the public records commission is making decisions about how to manage or dispose of these records

Financial Records and Audits

One important group of such records are those financial records that are needed for an audit. Most financial records of county offices are temporary records that must always be kept at least as long as is required for audit purposes. Regardless of whether or not an official thinks a financial or accounting record has served its useful purpose, it cannot be destroyed if the office of the comptroller deems it necessary for audit purposes.¹⁸⁵ You will notice that most financial records listed in the retention schedules in Part Four of the manual have a five-year retention period. This standard is based on the recommendation of the Division of County Audit in the Office of the Comptroller. Records that are important for audits need to be maintained through the time of the audit plus about three years afterwards in case any problems turn up. Formerly, the retention period for these records was based on keeping them for three years after the audit is complete. Since it was often difficult for a local official to know when an audit became final, the retention period was changed to five years from the date of creation of the record. This gives the official a definite time period to work from and also allows continuous destruction of financial records rather than lumping all records from a fiscal year together with a single retention date. Generally, this five-year period should suffice; however, if directed by the comptroller’s office to preserve records for a longer period due to an ongoing audit investigation or some other unusual circumstance, the local official should comply.¹⁸⁶

Exhibits and Evidence in Court Cases

The law includes a number of special considerations for materials which have become evidence and exhibits in judicial proceedings. Although some of these materials are technically not “records” this information is related to records management for court clerks and is included in this manual for those

reasons. Some of this information also appears in the retention schedules for court clerks. Exhibits are treated differently depending on whether they are documents or some other kind of physical evidence or firearms.

Documents

Unless local rules of court provide otherwise, the clerk can destroy certain records under the direction and order of the judge once the case has been finally disposed of for a period of 10 years. "Finally disposed of" means judgment has been entered and the appeal times have lapsed for all parties. The clerk has to retain the pleadings, original process and original opinion, original rules, appearance and execution dockets, minute books, and plat or plan books as permanent records. But all other records, dockets, books, ledgers and documents can be destroyed pursuant to a court order.¹⁸⁷ In civil cases, the 10-year period is shortened for certain types of records. A judge may order the clerk to destroy discovery materials, briefs, cost bonds, subpoenas and other temporary records in civil cases three years after the final disposition of the case.¹⁸⁸

In addition to these procedures, clerks need to comply with T.C.A. § 18-1-204. That statute requires them to notify the Tennessee State Library and Archives of the records they intend to destroy and give them 90 days to examine and remove any significant historical records if they so choose. Also, once they get an order for destruction of records from their judge, the clerks should take the order to the records commission for approval prior to destruction pursuant to T.C.A. § 10-7-406.

For Physical Evidence Other than Documents and Firearms

Physical evidence has a more complicated set of procedures, but the good news is that you can destroy it sooner. If evidence is used in a case, once the case comes to judgment or conclusion and once all appeals have been settled, the clerk is to give 30 days notice to the attorneys of record in the case that they can come pick up any thing that belongs to them or their clients. After 30 days, the clerk can dispose of the evidence by following the procedures in T.C.A. § 18-1-206(a)(2)–(7). This statute requires the clerk to make an inventory of the evidence to be destroyed with references to the case involved and the term of court in which the evidence was used. The clerk then publishes the inventory for three consecutive weeks in a newspaper of general circulation. Parties who want to object to the disposition of the property or make a claim for it have 30 days to file a petition with the court. Once that time passes, the clerk gives the inventory (and any petitions people may have filed) to the court for the judge to approve or reject each item on the list and decide if it should be

1. Returned to the owner or the owner's attorney;
2. Preserved by an organization for historical purposes;
3. Sold; or
4. Destroyed.

The clerk then gives the court order and the items to be disposed of to the sheriff. Depending on the disposition ordered for the item, the sheriff then delivers the items to their owners or to historical organizations or advertizes and sells the items or destroys them and files an affidavit concerning the destruction of the items with the court.

For Firearms

If a court clerk has exhibits in his or her possession that are firearms they should be disposed of in accordance with the procedures spelled out in T.C.A. §§ 39-17-1317 and 39-17-1318.

Other Miscellaneous Special Considerations

Records and documents of proceedings in a court of record can only be destroyed after a judge has issued an order authorizing their destruction.¹⁸⁹ Regardless of who approves it however, the law explicitly prohibits the destruction of any original process in a civil action or criminal proceeding.¹⁹⁰ Records pertaining to mortgages and deeds of trust on personal property and chattel mortgages can only be destroyed after the term of the mortgage has expired and all conditions have been met and the register approves the destruction of the record.¹⁹¹ Finally, no record of a county office or a court of record can be destroyed if the county official or judge who has custody of the record objects to its destruction.¹⁹² Court case files commonly contain material that is rich in historical and genealogical significance. If the county has an archive or is considering establishing one, these records are excellent candidates to be preserved for their historical value.

Conclusions

Whether by transfer or destruction, county officials, department heads, and records commissions must actively work to get rid of temporary records. There is so much emphasis placed on proper preservation of records that many officials keep everything out of fear of making a mistake. But there are checks and balances that are in place help prevent such mistakes and take the pressure of one individual making the decision whether or not a box of records can be destroyed. Unfortunately, since counties do not have unlimited storage space, keeping too many records usually results in a bigger mistake because it means that somewhere down the line the official cannot keep all of the records properly organized, accessible to the public and protected from environmental dangers. Taking steps to pro-actively manage the records as they are being created is much easier than waiting for the volume of records to reach a crisis level and then sorting out what can be destroyed.

A lternative Storage Formats

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

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. For that reason, much of this chapter will focus on storing permanent records in alternative formats. 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.¹⁹³ It is not necessary to notify the Tennessee State Library and Archives of the destruction of original copies of temporary value records.¹⁹⁴

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.¹⁹⁵ 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. These issues will be discussed in more detail in the section that follows regarding electronic records.

Microfilm¹⁹⁶

The process of microfilming is more than 150 years old. “In 1839 the French began to use micro-photography, primarily for placing small portraits into locketts. 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.”¹⁹⁷ 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.¹⁹⁸ Microfilming can offer as much as a 98 percent reduction in storage space over storing records in their original paper format.¹⁹⁹ 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.

State Laws Regarding the Photographic Preservation of Records

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.²⁰⁰ 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.²⁰¹ 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.²⁰² 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.²⁰³

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) 741-2997. 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.²⁰⁴

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.

Technical Guidelines

The following guidelines for producing and storing microfilm are considered crucial by the Tennessee State Library and Archives.²⁰⁵ For more information on microfilming, contact Carol Roberts or Bob Freeland with the Tennessee State Library and Archives at (615) 741-2997 or (615) 253-6445.

- 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.”²⁰⁶
- 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 of 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.

Electronic Records

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

Any records required to be kept by a government official in Tennessee may be maintained on a computer or removable computer storage media, including CD ROM disks, instead of bound books or paper records.²⁰⁷ 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.²⁰⁸

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

Electronic Conversion of Paper Records

Under a law that became effective on July 1, 1999, 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. The transfer of the records must be in accordance with regulations promulgated by the secretary of state in regards to the technology and the standards and procedures used.²⁰⁹ A copy of

the guidelines of the Tennessee State Library and Archives regarding digital imaging for permanent records is found in Appendix B of this manual. 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.²¹⁰ 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. If the official does not receive a response from the records commission within six months, he or she may forward the request to the Tennessee State

Be aware that the Tennessee State Library and Archives does not consider any existing format for electronic records to be of permanent archival quality.

Library and Archives for review. If the Tennessee State Library and Archives does not respond within nine months of receiving the request, the county official or department head may destroy the records in accordance with the regulations promulgated by the secretary of state.

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.²¹¹ 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.

Why Electronic Formats Are Not Well Suited for Permanent Records

All of these 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 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 are NOT 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 in this manual 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 this 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.

These issues and others are discussed and addressed in the guidelines found in Appendix B of this manual. Consider them seriously, seek technical assistance for working with technology, and question any vendors thoroughly about these problems when considering any technology purchase.

Other Issues Relative to Electronic Records

In the section of this manual related to public access to records, one can find additional information about providing remote access to government records via information technology. That chapter also discusses some of the other challenges specifically related to allowing public access to computerized or electronic records. The following subjects may also be of interest to records custodians with electronic records.

Records Management and E-Mail

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 of this manual 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.²¹²

This general definition is not as specific as the definition of county public records,²¹³ 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 that say “Send me a copy of that report when you get it finished;” “ By the way, George is out at a doctor’s appointment this afternoon;” or “Don’t forget the staff meeting this afternoon at 2:00” would not be a public record. These communications are more in the nature of working papers, something which becomes obsolete immediately after use. They should be disposed of in accordance with your general policy for working papers. 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. While I am aware of no reported appellate cases to date in Tennessee regarding e-mail as a public record, there have been cases considering this issue in other jurisdictions. In the Florida case of *Times Publishing Company v. City of Clearwater*²¹⁴ 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.²¹⁵ 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.

Electronic Signatures and Transactions

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”).²¹⁶ 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),²¹⁷ 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.²¹⁸ 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.²¹⁹

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
 - (A) Cancellation or termination of utility services (including water, heat, and power);
 - (B) 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;
 - (C) Cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or
 - (D) 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.²²⁰

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.

Identity Theft and Unauthorized Access to Electronic Records

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 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.

P

roper Storage Conditions

Like everything else on this planet, records need to be surrounded by the proper environment in order to survive. Most of the time, the records your office uses on a regular basis are kept in the same area that people work. This is good, because generally, the conditions that are comfortable for humans are also acceptable for storage of records of most formats.

Unless conditions are very severe, temperature and humidity are not factors affecting records scheduled for destruction in a few years. ... Wide fluctuation in temperature and high humidity can result in severe damage to these records. Ideally, the temperature range should be 65 to 75 degrees, and the humidity should be kept at 45 to 55 percent.²²¹

These conditions, at least the temperature ranges, are similar to those in the typical office environment. Unfortunately, the records we use most regularly and keep close around us in our offices are often those that we only need temporarily. Concerns about storage conditions become more important the longer you plan to keep a record. The problem is, those long-term or permanent retention records that need better care are often the ones we access less often, so they get moved out of the way into conditions that are less hospitable.

City halls and county courthouses, with their attics and basements, were never designed to accommodate this ever-increasing volume of semi-active and inactive records. This records growth, plus inadequate records programs, has resulted in the misuse of existing office and storage areas and the use of unimproved warehouses, jail cells, fire stations, abandoned school buildings, and hospital rooms as inactive records storage sites, including storage of records of archival value. The undesirable features of these kinds of storage facilities and inadequate programs become apparent once it is necessary to obtain information from records in storage. It takes only a few unsuccessful attempts to locate records in poorly maintained areas to discourage further use. Time, neglect, and lack of maintenance will take their toll on records stored there.²²²

For these reasons, counties should consider setting up facilities specifically designed for storing records on a long term basis. Rather than using basements, attics, or whatever space is available, the county may want to establish a records center for its inactive temporary records and an archives for its permanent value records.

Records Centers

A records center is essentially a centralized area for storing records. It is a place where all county officials can send their inactive records as an alternative to keeping them in their own offices where they take up valuable space and get in the way of operations. By default, the basement or bell tower of the courthouse may have become an ersatz records center, but the county should considering investing in a true one. A well-run records center can result in significant savings of both time and money while it protects and preserves records. "The effectiveness of a records center is based upon (a) its use of low-cost equipment which makes maximum use of space, (b) its ability to provide an orderly arrangement and control of records, and (c) its ability to employ procedures which assure prompt and efficient handling of records."²²³ Setting up a records center may sound like a project that only large counties might try to tackle. But small- and medium-sized governments can also benefit from saving

money. One federal government study on cost avoidance estimated that “...for every cubic foot of records stored in a records center, there is a savings of \$16.08.”²²⁴ When you consider the reams and reams of records in local government offices, including the school system and the court system, the savings can add up quickly.

A records center does not have to be a separate building. “A small government can usually convert an existing room quite easily since less space is required. There are many cities, towns, or counties that need no more than 1,000 cubic feet of records storage space. A records center of that capacity can be placed in a room about the size of a two-car garage.”²²⁵ If your county likes the idea but still thinks it does not have a great enough need to justify the expense of a records center, consider doing something radical— co-operate with other local governments. If the county, the school system, and all the municipalities within a county worked together through an inter-local agreement to establish a records center, costs would be spread among them and enough inactive records should be found to justify establishing the records center.

The Rome/Floyd County Records Program (population 81,250) is an excellent example of a cooperative venture supported by four Georgia local governments. This innovative records management program serves Floyd County, the city of Rome, and two school districts (Rome city schools and Floyd County schools). Each government partially funds the program. Service features included a records center with a capacity for 18,000 cubic feet (providing for records transfer, reference, selected microfilming, and records disposal) and technical assistance (a records management officer) on the proper management of records. These four local governments—by combining resources to create a professional program which none could individually afford—achieve most of their essential records management goals. All records placed in the records center still remain the property of the respective originating governments, however. The program has received the National Association of Counties achievement award, and it saved more than \$68,000 for the four local governments in 1990.²²⁶

More Information

If your county wants more information about starting a records center, including exactly what sort of space, equipment and organizational procedures are recommended for operating the center, contact the Archives Development Program at the Tennessee State Library and Archives or consult a publication that has been quoted throughout this chapter entitled *A Guide for the Selection and Development of Local Government Records Storage Facilities*, published by the National Association of Government Archives and Records Administrators. Contact information for that organization is located in the appendices to this manual under Sources of Additional Information. Also, you will find below, under the section regarding archive facilities, detailed recommendations on environmental conditions that can affect records storage. While concerns regarding improper storage conditions are magnified the longer a record is kept and are therefore more crucial in an archive than a temporary records storage center, environmental concerns should not be ignored for records centers. These recommendations are a useful resource for considering both the creation of a records center facility and evaluating any current storage space you are using for records. The idea of setting up a records center is closely connected to setting up a local archives. Many of the same concerns apply to both, but they serve different functions and tend to be frequented by different groups. A comprehensive records management program will benefit from planning that considers and incorporates both concepts.

Establishing Archives

In addition to, or in conjunction with setting up a records center, your county should consider establishing a county archives if one is not already in existence. An archives differs from a records center in that the records center generally keeps inactive records for a temporary time period before their final disposition. A records center will primarily be used by the officials and employees who created the records that are stored in the center as some need requires them to retrieve older inactive records. An archives is usually dedicated to preserving records of such historical value that they should be maintained permanently. The two may be located in the same facility and virtually indistinguishable to the public, or they may be separately located and operated facilities. An archives provides many of the same benefits as a records center, namely, removing records that are not regularly used by an office from expensive and cluttered office space and providing proper storage conditions for the records. An archives also serves an important role in preserving the history of our country and our communities and provides a valuable resource for members of the community researching our past. More likely, these private researchers will access the records of a county archives more often than county employees. By providing another location for this research, the archives indirectly helps county officials by allowing them to refer genealogists, students, and other researchers to another office rather than diverting time and effort from their daily tasks to assist those people in accessing the older, historical records of the county.

Specifications

Since the primary purpose of the archives is to preserve records permanently, the environmental conditions for the archives are even more important than those for a record center. The following considerations for archival space are recommended by the Tennessee State Library and Archives.²²⁷

Archives Storage and Management Space

Archival standards should be met so as to preserve local archives for future use. The closer local archives come to meeting these standards, the more likely it is that the records will survive.²²⁸

Distinctly exclusive space

An entirely separate building is desirable, but not essential, and some counties may not be able to afford it. In an existing building, a separate, exclusive space that can be secured from unauthorized entry and that meets the following general specifications is the minimal requirement to assure proper maintenance. The space should not be combined or confused with any other use.²²⁹

A strong, durable building that is earthquake-resistant and storm-resistant

Heavy (e.g. masonry and steel) construction is desirable, not only to resist storm and earthquake damage, but also to help meet the other standards, below with greater economy of operating costs.

Secure against theft and other hostile intrusion

A safe and secure locking system for the space is highly desirable. Entry to and exit from the space should be controlled by official staff so that patrons are not free to come and go without surveillance, so as to assure that documents will not be stolen or removed inadvertently without proper authorization.

As damp-proof as possible with a consistently moderate relative humidity

The best relative humidity for archival materials is a constant RH of 45–55 percent; excessive ranges and changes in humidity tend to speed up deterioration of archives materials. Leaky roofs, walls, and foundations that invite seepage and mold are natural enemies of archives. The site of the archives space should be chosen to protect it from flooding, either from nearby rivers or from excessive ground-water during heavy rains. Care should be taken to see that water pipe systems that serve the space are sound and leak-free.

Consistently moderate temperature

The best temperature for archival materials is a constant temperature between 65 and 70 degrees Fahrenheit. Excessive ranges and swings of temperature tend to speed up deterioration of archival materials.²³⁰

Free of pollutants

As much as possible, air circulation systems should be filtered to remove contaminating acids, dust, and other air-borne dangers to archives materials.

Free of biological pests

As much as possible, the archives should be protected against and free from insects, rodents, mold, and other biological dangers to records.

Free from ultra-violet light

As much as possible, sunlight and other sources of ultra-violet light, such as fluorescent tubes, that tend to damage film and paper documents must be excluded from the archives by shielding and filtration.²³¹

Fire-proof

To the greatest extent possible, construction materials should be of masonry, steel, and other fire-retardant or fire-resistant materials. Care should be taken to see that heating and electrical systems that serve the space are not likely to cause accidental fires.

Protected by a reliably-tested fire suppressant system

The most commonly-advised system is a reliable water sprinkler system with proper drainage for the water to be eliminated readily. Desirable fire protection includes rapid response by local fire fighting teams and briefing and orientation of local fire departments by local government officials on the nature of the archives and the need to preserve the content materials.²³²

Shelves and other containers should meet archival specifications

Shelving should be of strong, baked enamel steel construction.²³³ Enough space should be left between shelves, for convenient access and to inhibit fire migration. Shelves should be deep enough so that there is no overhang of boxes. Oversize materials (such as engineering drawings) should be in oversize shelving or metal cabinets.

Foldering and boxing of records

To the extent possible, records should be kept in acid-neutral paperboard boxes and folders (available from archival suppliers). This often requires removing records from original folders and boxes to new ones and labeling the new containers.

Disaster plan

A well-devised disaster plan for actions to take in case of fire, flood, water leakage, earthquake, theft, bomb-threats, or other dangers to archives should be written. There are good models of disaster plans already in existence. Local archives can acquire one of these and adapt it to local conditions.²³⁴ [For more discussion on disaster contingency planning and vital records preservation plans, see the next chapter.] Archives staff should be trained in its provisions and should know what to do in any emergency.

Technical Assistance

The Tennessee State Library and Archives is making an active effort to encourage the development of local and regional archives across the state. It is an excellent source of technical assistance and advice in developing an archives. The Tennessee State Library and Archives has produced a series of Tennessee Archives Management Advisories that provide a wealth of information on a number of topics. Much of the material in this chapter has been adapted from those publications but it only scratches the surface of the information available from the Tennessee State Library and Archives on archives and preservation of records. A listing of the archives management advisories can be found in the appendix to this manual under Sources of Additional Information.

For further information, please contact Dr. Wayne Moore, assistant state archivist, Tennessee State Library and Archives, (615) 253-3458, e-mail: wayne.moore@state.tn.us.

D

isaster Preparedness

Disasters. By their very nature, they are unexpected events. Severe weather, earthquakes, floods, or fire can strike anywhere at anytime with little or no warning. Disasters can irreparably change individual lives, halt the normal commerce of business and industry, and, as the tornado in Montgomery County in 1999 violently demonstrated, disasters can even disrupt the operation of government.

With all the ancient and venerable courthouses still standing in our state, you might consider it a rare occurrence for county government offices to be seriously damaged. But consider this telling statistic: Tennessee's neighbor to the South, Georgia, has had more than 100 courthouse fires in the course of the history of that state.²³⁵

The occurrence of disasters cannot be eliminated, but they can be prepared for and their impact can be lessened. Tragedies such as the devastation to downtown Clarksville by the tornado that struck there only highlight the importance of having a good disaster recovery plan in place. Even though a number of county offices were damaged or destroyed by the storm, they were able to recover, relocate, and return to providing services to the residents of Montgomery County in a remarkably short time. Their ability to do so was at least as attributable to planning, preparation, and procedures in place before the storm as it was by emergency responses after the fact.

In order to lessen the impact of a disaster, there are two things every county should do.

- ▶ 1. The county should develop a disaster contingency plan.
- ▶ 2. The county should institute a vital records protection program.

Contingency Plans

Contingency plans should be detailed and instructive and address the specific needs of every office of county government. They should anticipate the various types of disasters your county might face. Response to a flood will be different from response to a fire or earthquake or tornado. In addition to furnishing officials and staff members with copies of the plan, duplicates of the plan should also be stored off-site in case of disasters of truly catastrophic proportions. The best recovery plan will do no good if the only copy is locked inside a file cabinet in an office that is burning down.

A good disaster contingency plan will

- Designate who is in charge of recovery operations and who will be working on recovery teams. It should include all necessary information for contacting these people at any hour of the day or night;
- Anticipate the types of disaster the county may face and provide basic instructions for the first responders to an emergency to ensure that everything possible is done to minimize damage and preserve the safety of individuals responding to the disaster (e.g. evacuation plans, directions for shutting off electrical current in case of a flood, locations of shut-off valves in case of a broken water line);
- Include an inventory of supplies and equipment that are available for use in salvage efforts. The inventory should identify locations of important supplies and equipment—everything from heavy machinery to fire extinguishers to mops and buckets;

- Identify alternative office space and other facilities which might be used if the county needs temporary space for relocation or salvage operations;
- Include current contact information for experts in emergency management like TEMA, FEMA, and other governmental entities, plus commercial entities that can provide expertise in recovery and salvage if the disaster is too large for the county to handle by itself;
- Have a plan for acquiring replacement office equipment and supplies quickly and efficiently. This will be especially essential if computer equipment was damaged in the disaster.

Vital Records Protection

A companion to the disaster contingency plan is the vital records protection program. People can be evacuated; office space and supplies can be replaced. But the records of a local government are one of its most vital and vulnerable resources. If steps have not been taken to protect important records prior to a disaster, the resumption of regular operations after a disaster will be far more difficult and costly.

Whereas a contingency plan will provide instructions on how to respond immediately after a disaster, a vital records protection plan will inform government offices on the ongoing steps that should be regularly practiced in order to preserve the important information of the office. Records protection plans will vary depending on the volume and format of the records to be protected, the resources available to the county, and the technology present in offices. Any plan should, at a minimum, provide procedures for identifying, duplicating, and safeguarding vital records.

No office can afford to expend the amount of resources it would take to ensure the protection of every record in the office. For that reason, it is important to determine which records are truly vital and which are not.

Records management experts have divided records into four classes

- (1) Nonessential records—those that if lost would not really be missed. Most convenience files, internal memos, and many routine papers of completed transactions fall into this category.
- (2) Useful records—records containing information which if lost would cause some difficulty but which could be easily replaced.
- (3) Important records— those records that cannot be dispensed with and that can be replaced only through the expenditure of substantial time, money, or manpower.
- (4) Vital records—those records which are essential and cannot be replaced. Vital records contain information essential to the continuity of operations or to the protection of the rights of the government or of individual citizens.²³⁶

Begin by protecting those records that are indispensable. Since you cannot anticipate and prevent every possible disaster, the best course of action is to make sure there are off-site archival quality²³⁷ copies of the county's most important records.

Remember: Disasters do not have to be big to be devastating. Little emergencies like a leaky roof or a burst water pipe can do tremendous damage to records.

If some records are stored in electronic format, state laws require that certain back-up procedures are followed to prevent loss of data.²³⁸ For obvious reasons tape or disk backups of electronic data should not be stored in the same location as the computer system itself. While less fragile than electronic records, paper records and microfilm also must be properly stored and cared for in order to prevent destruction of the records in the event of a disaster or from the ravages of time. Wherever possible, a county should archive its permanent records in a location or facility that is designed for records preservation. (See the discussion in a previous chapter in this manual on archives.)

If you need assistance in developing these plans for your county, both CTAS and the Tennessee State Library and Archives can help. Copies of disaster contingency plans and other publications on records protection are available upon request from Carol Roberts, Tennessee State Library and Archives, by phone at (615) 253-6446 or via e-mail at carol.roberts@state.tn.us.

Recovery of Stolen or Misappropriated Records

While it usually does not reach disastrous proportions, there are also certain human behaviors that you need to be prepared to respond to. If records are inappropriately removed from the office where they belong, the official who has custody of the records is not without remedy. Of course, criminal theft charges can be brought against someone who steals county documents. But what may prove to be a more practical remedy is to pursue an action to recover personal property.²³⁹ This action, also known as replevin, is a judicial proceeding whereby property that is in the wrong hands can be returned to the rightful owner or custodian. It is initiated by filing a complaint in the circuit or chancery court or by causing a warrant to issue in the general sessions court.²⁴⁰ Ultimately, the proceeding may result in the issuance of a writ of possession that directs the proper officer to take the property from the defendant and return it to the plaintiff.²⁴¹ If you need to pursue such an action to recover misappropriated county records, contact the county attorney.

C onclusion

The preceding materials will hopefully provide county officials and county public records commissions with enough ammunition to begin the battle of records management. It is our hope that, regardless of the level of records management currently present in your county, you found something of use in these chapters. The rest of this manual is comprised of the retention schedules for county offices and appendices of statutes, guidelines, forms, sample resolutions, and a list of sources of additional information, as well as the references and endnotes for the preceding text.

ENDNOTES

1. T.C.A. § 10-7-404.
2. *Bayless v. Knox County*, 286 S.W.2d 597 (Tenn. 1955).
3. T.C.A. § 8-19-111(b)
4. T.C.A. § 10-7-102.
5. T.C.A. § 10-7-104.
6. T.C.A. § 10-7-105.
7. T.C.A. § 10-7-201, *et seq.*
8. T.C.A. § 10-7-120.
9. T.C.A. § 10-7-121.
10. T.C.A. § 10-7-123.
11. T.C.A. § 10-7-202.
12. T.C.A. § 10-7-301, *et seq.*
13. 1959 Public Chapter 253.
14. T.C.A. § 10-7-401.
15. 1994 Public Chapter 884.
16. T.C.A. § 10-7-401.
17. Op. Tenn. Att’y Gen. No. 98-114 (June 23, 1998).
18. T.C.A. § 10-7-402.
19. T.C.A. § 10-7-402.
20. T.C.A. § 10-7-402.
21. T.C.A. § 10-7-403.
22. 1999 Public Chapter 167.
23. T.C.A. § 10-7-401, *et seq.*
24. T.C.A. § 10-7-406.

25. T.C.A. § 10-7-404.
26. T.C.A. § 10-7-414.
27. T.C.A. § 10-7-414.
28. T.C.A. § 10-7-411.
29. T.C.A. § 10-7-411(c).
30. T.C.A. § 10-7-413(b).
31. See Tennessee Archives Management Advisory 99-009.
32. T.C.A. § 10-7-409.
33. T.C.A. § 10-7-408.
34. T.C.A. § 10-7-404(b).
35. *Using the Freedom of Information Act, a Step-by-Step Guide*, an American Civil Liberties Union Publication available on the Internet at <http://www.aclu.org/library/foia/html#introduction>.
36. T.C.A. § 10-7-503, which makes most state and local government records in Tennessee public, passed in 1957.
37. 5 U.S.C.A. § 552(a).
38. See Note 33, above.
39. 5. U.S.C.A. § 552(f)
40. T.C.A. § 10-7-503.
41. See generally, *Memphis Publishing Co. v. Holt*, 710 S.W.2d 513 (Tenn. 1986).
42. T.C.A. § 10-7-505(d).
43. *Griffin v. City of Knoxville*, 821 S.W.2d 921, 924 (Tenn. 1991).
44. *Robin M. Cole v. Donal Campbell*, 968 S.W.2d 274 (Tenn. 1998).
45. Op. Tenn. Att’y Gen. No. 99-067 (March 18, 1999) re-affirmed by Op. Tenn. Att’y Gen. No. 01-132 (August 22, 2001).
46. Op. Tenn. Att’y Gen. No. 99-067 (March 18, 1999).
47. T.C.A. § 10-7-506(a).

48. See Op. Tenn. Att’y Gen. No. 01-021 (February 8, 2001).
49. T.C.A. § 10-7-506(a).
50. Op. Tenn. Att’y Gen. No. 99-067 (March 18, 1999).
51. *Waller v. Bryan*, 16 S.W.3d 770, (Tenn. App. 1999).
52. *Waller*, at 773.
53. *Tennessean v. Electric Power Board of Nashville*, 979 S.W.2d 297, at 305 (Tenn. 1998) and Op. Tenn. Att’y Gen. Nos. 01-021 (February 8, 2001) and 80-455 (September 19, 1980).
54. Op. Tenn. Att’y Gen. No. 80-455 (September 19, 1980).
55. Op. Tenn. Att’y Gen. No. 01-021 (February 8, 2001).
56. Op. Tenn. Att’y Gen. No. 01-021, at page 4.
57. Op. Tenn. Att’y Gen. No. 00-101 (May 24, 2000).
58. T.C.A. § 8-21-408.
59. *Nixon v. Warner Communications*, 435 U.S. 589, 98 S.Ct. 1306 (1978).
60. *Ray v. State*, 984 S.W.2d 236, 238 (Tenn. Crim. App. 1997).
61. *Smith v. Securities and Exchange Commission*, 129 F.3d 356, 359 (6th Cir. 1997). See also Op. Tenn. Att’y Gen. No. 02-075 (June 12, 2002).
62. *Ballard v. Herzke*, 924 S.W.2d 652, 661-662 (Tenn. 1996).
63. *Ray v. State*, at 238.
64. *Knoxville News-Sentinel v. Huskey*, 982 S.W.2d 359, 362 (Tenn. Crim. App. 1998)
65. *In re Knoxville News-Sentinel*, 723 F.2d 470, at 474 (6th Cir. 1983).
66. Op. Tenn. Att’y Gen. No. 02-075 (June 12, 2002).
67. T.C.A. § 40-32-101(b).
68. *State v. Powell*, 1999 WL 512072 (Tenn. Ct. App. July 21, 1999, permission to appeal denied January 24, 2000).
69. T.C.A. § 40-35-313.
70. T.C.A. § 40-35-313(b).
71. T.C.A. §§ 40-15-105.

72. T.C.A. § 40-27-109.
73. T.C.A. § 38-6-118.
74. T.C.A. § 40-32-101(a)(4).
75. T.C.A. § 40-32-101(a)(6).
76. T.C.A. § 55-10-711.
77. T.C.A. §§ 57-3-412 and 57-5-301.
78. T.C.A. § 36-4-127.
79. T.C.A. § 30-2-712.
80. T.C.A. § 34-1-124.
81. T.C.A. § 10-7-513.
82. Op. Tenn. Att’y Gen. No. 01-021 (February 8, 2001).
83. T.C.A. §§ 10-7-121 and 10-7-406.
84. *Tennessean v. Electric Power Board of Nashville*, 979 S.W.2d 297 (Tenn. 1998).
85. *Tennessean v. Electric Power Board of Nashville*, 979 S.W.2d 297, at 300.
86. *George v. Record Custodian*, 485 N.W.2d 460 (Wis.App.1992).
87. *Tennessean v. Electric Power Board of Nashville*, 1997 WL 83403 (Tenn.Ct.App. 1997).
88. *Tennessean v. Electric Power Board of Nashville*, 979 S.W.2d 297, at 304.
89. *Tennessean v. Electric Power Board of Nashville*, 979 S.W.2d 297, at 305.
90. T.C.A. § 10-7-123.
91. T.C.A. § 10-7-123.
92. T.C.A. § 10-7-123(a)(1).
93. T.C.A. § 10-7-123(a)(4).
94. T.C.A. § 2-2-138.
95. Op. Tenn. Att’y Gen. No. 04-114 (July 19, 2004).
96. Op. Tenn. Att’y Gen. No. 04-114.
97. Op. Tenn. Att’y Gen. No. 00-058 (March 31, 2000).

98. Op. Tenn. Att’y Gen. No. 00-014 (January 26, 2000).
99. T.C.A. § 10-7-505(a).
100. T.C.A. § 10-7-505(b).
101. T.C.A. § 10-7-505(c).
102. T.C.A. § 10-7-505(e).
103. T.C.A. § 10-7-505(f).
104. T.C.A. § 10-7-505(g).
105. *Griffin v. City of Knoxville*, 821 S.W.2d 921, 924 (Tenn. 1991) as quoted in Op. Tenn. Att’y Gen. No. 99-011 (January 25, 1999).
106. T.C.A. § 10-7-504.
107. Op. Tenn. Att’y Gen. No. 04-084 (May 4, 2004).
108. T.C.A. § 10-7-504.
109. Op. Tenn. Att’y Gen. No. 99-022 (February 9, 1999).
110. See Op. Tenn. Att’y Gen. No. 01-165 (September 15, 2001) for a discussion of the confidentiality of phone numbers and other identifying numbers used in the enforcement of the business tax.
111. See *Appman v. Worthington*, 746 S.W.2d 165, 166 (Tenn. 1987) and *Ballard v. Herzke*, 924 S.W.2d 652, 662 (Tenn. 1996).
112. T.C.A. § 10-7-504(b). See also Op. Tenn. Att’y Gen. 01-040 (March 19, 2001).
113. T.C.A. § 10-7-504(c).
114. T.C.A. § 10-7-506(c).
115. Op. Tenn. Att’y Gen. No. 02-016 (February 6, 2002).
116. 5 U.S.C. § 552a and Op. Tenn. Att’y Gen. No. 02-016 (February 6, 2002).
117. 5 U.S.C. § 552a.
118. 42 U.S.C. 666(a)(13). Note that the attorney general has opined that this law does not prohibit the disclosure of marriage licenses or marriage license applications containing social security numbers. Op. Tenn. Att’y Gen. No. 98-065 (March 17, 1998).
119. 26 U.S.C. §§ 6103 and 7213 and 42 U.S.C. §§ 654a and 666.

120. 26 U.S.C. §§ 7213 and 7431.
121. T.C.A. § 4-4-125.
122. 2003 Public Chapters 124 and 35.
123. 18 U.S.C. § 2721 through § 2725.
124. T.C.A. §§ 55-25-101, *et seq.*
125. T.C.A. §§ 55-25-104 through 55-25-107 and 18 U.S.C.A. § 2721.
126. T.C.A. § 55-25-103(6).
127. 18 U.S.C. § 2721(b)(1) and T.C.A. § 55-25-107.
128. 18 U.S.C. § 2721 and T.C.A. § 55-25-105 through 107.
129. T.C.A. § 68-3-205.
130. T.C.A. § 68-3-205(d).
131. T.C.A. § 10-7-503(c).
132. T.C.A. § 10-7-504(g).
133. T.C.A. § 68-11-302.
134. T.C.A. § 68-11-304.
135. T.C.A. § 68-11-305.
136. T.C.A. § 68-11-307.
137. T.C.A. § 68-10-113.
138. See T.C.A. §§ 68-140-501, *et seq.*, especially § 68-140-519 and the official Rules of the Tennessee Department of Health, Bureau of Manpower and Facilities, Emergency Medical Services Division, Rules 1200-12-1-.05, 1200-12-1-.09 and 1200-12-1-.15.
139. T.C.A. § 68-140-519.
140. Rules of the Emergency Medical Services Division, Rules 1200-12-1-.15.
141. Department of Health and Human Services, Office for Civil Rights HIPAA Privacy Rule Summary available on the Internet at <http://www.os.dhhs.gov/ocr/privacysummary.pdf>.
142. 45 C.F.R. § 164.501.
143. 45 C.F.R. § 160.102.

144. 45 C.F.R. §§ 160.102 and 160.103.
145. 45 C.F.R. § 160.102.
146. 45 C.F.R. Part 162.
147. 45 C.F.R. § 164.504.
148. 45 C.F.R. § 164.530.
149. Op. Tenn. Att’y Gen. 04-153 (October 7, 2004).
150. Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952 with related regulations found in 16 CFR Part 682.
151. T.C.A. § 10-7-504.
152. 20 U.S.C.A. § 1232g with related regulations found in 34 C.F.R. Part 99.
153. 2002 Public Chapter 621 codified as T.C.A. §§ 49-50-1501 *et seq.*
154. T.C.A. § 49-50-1503.
155. T.C.A. § 49-50-1504.
156. T.C.A. § 49-50-1505.
157. T.C.A. § 49-50-1506.
158. T.C.A. § 49-50-1507.
159. T.C.A. § 49-50-1507.
160. T.C.A. § 49-50-1508.
161. T.C.A. § 49-50-1509.
162. T.C.A. § 49-50-1508.
163. T.C.A. § 49-6-902.
164. T.C.A. § 49-6-902(b).
165. T.C.A. § 49-2-301(b)(1)(C) and (D).
166. T.C.A. § 49-2-301(b)(2).
167. T.C.A. § 49-2-301(b)(1)(Y).

168. *Managing Records on Limited Resources*, p. 3.
169. *The Daily Management of Records and Information—A Guide for Local Governments*, issued by the National Association of Government Archives and Records Administrators, p. 1.
170. *The Daily Management of Records and Information*, p. 2.
171. “Studies show that between 1 and 3 percent of an organization’s records are not available to the users due to one of these causes.” *The Daily Management of Records and Information* p. 3.
172. *The Daily Management of Records and Information*, pp. 2 and 3.
173. *The Daily Management of Records and Information*, p. 8.
174. *Managing Records on Limited Resources—A Guide for Local Governments*, Stephen E. Haller, CRM, issued by the National Association of Government Archives and Records Administrators, November 11, 1991, p. 2.
175. T.C.A. § 10-7-301.
176. T.C.A. §§ 10-7-406(b) and 10-7-413.
177. T.C.A. § 10-7-301.
178. T.C.A. §§ 10-7-406(b) and 10-7-413.
179. T.C.A. § 10-7-406.
180. T.C.A. § 10-7-404(a).
181. T.C.A. § 10-7-413.
182. T.C.A. § 10-7-404(d)(2).
183. T.C.A. § 10-7-404(d)(1).
184. See Op. Tenn. Att’y Gen. No. 01-040 (March 19, 2001).
185. T.C.A. § 10-7-404(a).
186. T.C.A. § 10-7-404(a).
187. T.C.A. § 18-1-202.
188. T.C.A. § 18-1-202(b).
189. T.C.A. § 18-1-202.
190. T.C.A. § 10-7-404(c).

191. T.C.A. § 10-7-412.
192. T.C.A. § 10-7-404.
193. T.C.A. § 10-7-404(a).
194. T.C.A. § 10-7-413.
195. 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.
196. In this manual, the term microfilm or microfilming will be used generally to discuss the various micro-photographic processes available.
197. *Using Microfilm*, Julian L. Mims, CRM, issued by the National Association of Government Archives and Records Administrators (February, 1992), p. 1.
198. *Using Microfilm*, p.1.
199. *Using Microfilm*, p.1.
200. T.C.A. § 10-7-404(a).
201. T.C.A. § 10-7-406.
202. T.C.A. § 10-7-406.
203. T.C.A. § 2-2-137.
204. Title 10, Chapter 7, Part 5.
205. Tennessee Archives Management Advisory 99-005, Microfilming Permanent Records, January 11, 1999.
206. T.C.A. § 10-7-501.
207. T.C.A. § 10-7-121.
208. T.C.A. § 10-7-121.
209. T.C.A. § 10-7-404(d)(1).
210. See Tennessee Archives Management Advisory 99-006.
211. T.C.A. § 10-7-404(d)(1).
212. T.C.A. § 10-7-301.
213. See T.C.A. § 10-7-403.

214. *Times Publishing Company v. City of Clearwater*, 830 So.2d 844 (District Court of Appeal of Florida, Second District, 2002).
215. *Times Publishing Company*, at 847.
216. 15 U.S.C. §§ 7001, *et seq.*
217. 2001 Public Chapter 72, codified primarily in T.C.A. §§ 47-10-101, *et seq.*
218. 15 U.S.C. § 7001(a)(1) and (2).
219. 15 U.S.C.A. § 7003(a).
220. 15 U.S.C.A. § 7003(b).
221. *A Guide for the Selection and Development of Local Government Records Storage Facilities*, compiled by A.K. Johnson, Jr., CRM, issued by the National Association of Government Archives and Records Administrators (2nd printing, 1991), p. 9.
222. *A Guide for the Selection and Development of Local Government Records Storage Facilities*, p. 2.
223. *A Guide for the Selection and Development of Local Government Records Storage Facilities*, p. 2.
224. *A Guide for the Selection and Development of Local Government Records Storage Facilities*, p. 4.
225. *A Guide for the Selection and Development of Local Government Records Storage Facilities*, p. 11.
226. *Managing Records on Limited Resources—A Guide for Local Governments*, Stephen E. Haller, CRM, issued by the National Association of Government Archives and Records Administrators, November 11, 1991, p. 10.
227. These recommendations are from the Tennessee Archives Management Advisory (TAMA) 99-004 Basic Archives Management Guidelines, p. 5.
228. More detailed standards are available from the Tennessee State Library and Archives.
229. In the past, some people have regarded archives as “dead” storage and put valuable records into rooms with old furniture, cleaning equipment, fuel stores, or into fire-trap attics and basements with dirt, vermin and the like. That kind of negligence endangers the very evidence that public interest needs to save and protect.
230. There are stricter archival standards, with narrower ranges of tolerance for ideal conditions. Some materials may also require slightly optimum temperature and humidity. However, these present standards are tolerable for local archives that do not have the resources for highly-sophisticated environmental control systems.

231. Incandescent lights do not produce strong ultra-violet rays, but fluorescent lamps do and they must be shielded with ultra-violet ray filters if they are used.
232. Much damage has been done to records when local fire-fighters treat archives as they would any other storehouse of replaceable goods.
233. Wood is flammable and it often gives off gasses and oils that may damage archives.
234. The University Library of Tennessee Technological University in Cookeville has a well-developed disaster plan that may be used as a model. Other models are available from TSLA and CTAS.
235. This chilling fact is pointed out in a publication entitled *Protecting Records—A Guide for Local Governments*, by Harmon Smith, issued by the National Association of Government Archives and Records Administrators (published March 1992), p. 6.
236. *Protecting Records*, p. 3.
237. According to the Tennessee State Library and Archives, the only media that will assure long-term survival of vital records are carbon-based ink on acid neutral paper and archival quality silver gelatin microfilm created and kept under conditions that meet archival standards. See Tennessee Archives Management Advisory 99-07.
238. For information regarding these procedures, see the chapter in this part regarding alternative storage media.
239. See T.C.A. §§ 29-30-101, *et seq.*
240. T.C.A. § 29-30-103.
241. T.C.A. § 29-30-107.