County Technical Assistance Service

Published on *e-Li* (http://ctas-eli.ctas.tennessee.edu) September 17, 2019

Special Considerations and Specific Types of Confidential Records

Dear Reader:

The following document was created from the CTAS electronic library known as e-Li. This online library is maintained daily by CTAS staff and seeks to represent the most current information regarding issues relative to Tennessee county government.

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

Please feel free to contact us if you have questions or comments regarding this information or any other e-Li material.

Sincerely,

The University of Tennessee
County Technical Assistance Service
226 Capitol Blvd. Suite 400
Nashville, TN. 37219
615-532-3555 phone
615-532-3699 fax
ctas@tennessee.edu
www.ctas.tennessee.edu

Table of Contents

Special Considerations and Specific Types of Confidential Records

Reference Number: CTAS-1169

Personally Identifying Information

Reference Number: CTAS-1170

In 2016 the General Assembly amended T.C.A. § 10-7-504 to provide that no governmental entity shall publicly disclose *personally identifying information* of any citizen of the state unless: (i) Permission is given by the citizen; (ii) Distribution is authorized under state or federal law; or (iii) Distribution is made: (*a*) To a consumer reporting agency as defined by the federal Fair Credit Reporting Act (15 U.S.C. §§ 1681 et seq.); (*b*) To a financial institution subject to the privacy provisions of the federal Gramm Leach Bliley Act (15 U.S.C. § 6802); or (*c*) To a financial institution subject to the International Money Laundering Abatement and Financial Anti–Terrorism Act of 2001 (31 U.S.C. §§ 5311 et seq.).

The law defines “personally identifying information” to include: (i) Social security numbers; (ii) Official state or government issued driver licenses or identification numbers; (iii) Alien registration numbers or passport numbers; (iv) Employer or taxpayer identification numbers; (v) Unique biometric data, such as fingerprints, voice prints, retina or iris images, or other unique physical representations; or (vi) Unique electronic identification numbers, routing codes or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data.

The law provides that it does not prohibit the use of personally identifying information by a governmental entity in the performance of its functions or the disclosure of personally identifying information to another governmental entity, or an agency of the federal government, or a private person or entity that has been authorized to perform certain duties as a contractor of the governmental entity.

Motor Vehicle Registration Records

Reference Number: CTAS-1171

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.[1] In addition, in 1996, our state legislature adopted the Uniform Motor Vehicle Records Disclosure Act that closely parallels the language of the federal act.[2] 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.[3] 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.[4] Use of the information is generally allowed for governmental agencies in carrying out their functions.[5] Additionally, the statutes include about a dozen other authorized uses whereby certain private parties have rights to access the records for those specified purposes.[6] 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.

---

[1] 18 U.S.C. § 2721 through § 2725.

[2] T.C.A. §§ 55-25-101, *et seq.*

[3] T.C.A. §§ 55-25-104 through 55-25-107 and 18 U.S.C.A. § 2721.
[4] T.C.A. § 55-25-103(6).
[5] 18 U.S.C. § 2721(b)(1) and T.C.A. § 55-25-107.
[6] 18 U.S.C. § 2721 and T.C.A. § 55-25-105 through 107.

Vital Records

Reference Number: CTAS-1172

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.[1] 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.[2]

---

[1] T.C.A. § 68-3-205.
[2] T.C.A. § 68-3-205(d).

Law Enforcement Personnel Records

Reference Number: CTAS-1173

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.[1]

In addition, T.C.A. § 10-7-504(g) provides that the personnel information of law enforcement personnel shall be redacted where there is a reason not to disclose the information as determined by the sheriff or the sheriff's designee. When a request to inspect includes personal information and the request is for a professional, business, or official purpose, the sheriff or custodian shall consider the specific circumstances to determine whether there is a reason not to disclose and shall release all information, except information made confidential in T.C.A. § 10-7-504(f), if there is not such a reason. In all other circumstances, the officer shall be notified prior to disclosure of the personal information and shall be given a reasonable opportunity to be heard and oppose the release of the information. In addition to the requirements of T.C.A. § 10-7-503(c), the request for a professional, business, or official purpose shall include the person's business address, business telephone number and email address. The request may be made on official or business letterhead and the person making the request shall provide the name and contact number or email address for a supervisor for verification purposes. If the sheriff, the sheriff's designee, or the custodian of the information decides to withhold personal information, a specific reason shall be given to the requestor in writing within two (2) business days, and the file shall be released with the personal information redacted. For purposes of T.C.A. § 10-7-504(g), personal information shall include the officer's residential address, home and personal cellular telephone number; place of employment; name, work address and telephone numbers of the officer's immediate family; name, location, and

telephone number of any educational institution or daycare provider where the officer's spouse or child is enrolled.

In addition to the provisions relative to the office's residential address in T.C.A. § 10-7-504(g), subsection (f) of the same statute provides that the residential address of a law enforcement officer held by the county in its capacity as an employer shall be confidential and any person who releases the information commits a Class B misdemeanor if the person acts with criminal negligence, or a Class A misdemeanor if the person knows the information is to be treated as confidential and intentionally releases the information to the public.

Finally, T.C.A. § 10-7-504(g) also provides that the sheriff may segregate information that could be used to identify or to locate an officer designated as working undercover.[2]

---

[1] T.C.A. § 10-7-503(c).

[2] T.C.A. § 10-7-504(g).

Computerized Data Breaches

Reference Number: CTAS-2204

Under T.C.A. § 47-18-2901 counties must create safeguards to ensure the security of personal information on laptop computers and other removable storage devices. Failure to comply with this requirement creates a cause of action against the county if identity theft results. Also, T.C.A. § 47-18-2107 requires any holder of computerized personal information that is confidential to disclose any breach of the security of the system to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Domestic Violence Prevention and Protection Documents

Reference Number: CTAS-1174

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 you 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

Reference Number: CTAS-1175

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.[1] Certain hospital records are not public records.[2] 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.[3] 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.[4] Records held by a local health department related to sexually transmitted diseases are strictly confidential.[5]

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.[6] The information in run records that relates to the medical condition and treatment of the patient is specifically declared confidential.[7] 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.[8]

---

[1] T.C.A. § 68-11-302.

[2] T.C.A. § 68-11-304.

[3] T.C.A. § 68-11-305.

[4] T.C.A. § 68-11-307.

[5] T.C.A. § 68-10-113.

[6] See T.C.A. §§ 68-140-301, *et seq.*, especially § 68-140-319 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.

[7] T.C.A. § 68-140-319.

[8] Rules of the Emergency Medical Services Division, Rules 1200-12-1-.15.

HIPAA

Reference Number: CTAS-1176

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.[1] Protected health information includes all individually identifiable health information held by a covered entity or its business associate in any form or media.[2] 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.[3] 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.[4] 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.[5] These include claims, benefit eligibility inquiries, referral authorization requests, or certain other transactions listed under the HIPAA Transactions Rule.[6] 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.[7] 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.[8]

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. 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, Health Information Privacy. 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.[9]

---

[1] Department of Health and Human Services, Office for Civil Rights HIPAA Privacy Rule Summary

[2] 45 C.F.R. § 164.501.

[3] 45 C.F.R. § 160.102.

[4] 45 C.F.R. §§ 160.102 and 160.103.

[5] 45 C.F.R. § 160.102.

[6] 45 C.F.R. Part 162.

[7] 45 C.F.R. § 164.504.

[8] 45 C.F.R. § 164.530.

[9] Op. Tenn. Att'y Gen. 04-153 (October 7, 2004).

Credit Card Numbers and Credit Reports

Reference Number: CTAS-1177

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. 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 are notification requirements that apply when a breach of security has allowed improper access to electronic 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 Commission[1]. 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.

---

[1] 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.

Source URL: http://ctas-eli.ctas.tennessee.edu/reference/special-considerations-and-specific-types-confidential-records