

Safeguarding Social Security Numbers in Tennessee Government Records



Federal and state laws authorizing or requiring Social Security number (SSN) collection by public and private entities, the utility of using a SSN as a records management tool, and the lack of other unique personal identifiers have led to the adoption of the SSN as a primary personal identifier. Widespread collection and use of the SSN concerns both policy makers and consumer advocates because of its potential misuse by identity thieves. Tennessee state and local governments maintain a large number of SSNs in their records, but in most instances, access to SSNs is restricted by federal or state law.

Report Findings:

Tennessee law does not clearly direct local government record custodians on the treatment of SSNs in agency records. Public access to SSNs in state agency records is restricted by a single statute. However, access to SSNs in local government records is restricted by numerous statutes applying to specific records types. Local government records custodians seeking guidance on the legal status of SSNs may be confounded by the changing list of records-specific exceptions to the public records act appearing throughout *Tennessee Code Annotated*. Responses to the OREA survey of local government officials reflect variation in the treatment of records containing SSNs.

Some state and local government agencies lack written policies to protect SSNs in their records; the use of safeguards to protect SSNs in agency records varies. While most government agencies responding to the OREA survey take measures to protect SSNs, some lack agency level policies or procedures directing staff on appropriate and consistent safeguards for SSNs in their records. Recent state legislation requires state and local governments to develop procedures to safeguard confidential information contained on laptop computers and portable data storage devices.

Tennessee government agencies have reduced SSN use, but further reductions may be possible. Most government agencies in Tennessee responding to the OREA survey do not review SSN use to determine whether it is necessary for agency function. If SSNs are not unnecessarily included in records and reports, they cannot be stolen or inadvertently released.

Recommendations:

The General Assembly may wish to consider:

- appointing state and local government study committees to review government use and transmission of the SSN, the feasibility of further reductions of SSNs in government records, and confidential records statutes
- requiring local governments to develop specific, written policies on the protection of personal or confidential information in their paper and electronic records
- requiring additional records management assistance and training resources for local government officials
- requiring additional oversight to ensure that state and local agencies have developed and implemented information security policies and practices to protect confidential information, including SSNs maintained in their records

In addition, state and local government agencies should continue to implement policies and practices to restrict the storage of SSNs and other personal information on portable storage devices.

View the full report at <http://www.comptroller.state.tn.us/cpdivorea.htm>.

For more information, contact Patrick Hultman at (615)401-7881 or Patrick.Hultman@state.tn.us or Susan Mattson at (615)401-7884 or Susan.Mattson@state.tn.us.