TECHNICAL UPDATE

CTSI Serving Colorado's Counties

Volume 25 Number 31 August 3, 2021

Security Breaches and Personal Information

During the 2018 legislative session, the state of Colorado amended Colo. Rev. Stat. Ann § 6-1-716 (2006), to include governmental entities. The statute concerns how a person's information (e.g., social security number, passport ID, medical information, password, username, email address, etc.) is stored, disposed of, and in the case of a data breach, how they are notified about the breach. The law went into effect on September 1, 2018.

The amended statute defines a governmental entity as: *any state agency or institution, including the judicial department, county, city and county, incorporated city or town, school district, special improvement district, authority, and every other kind of district, instrumentality, or political subdivision of the state organized pursuant to law. Article 73, Section 24-73-101-(4)(a)"..*

WRITTEN POLICY REQUIRED

The amended statute requires that a governmental entity that keeps paper or electronic documents containing personal identifying information develop a written policy for the destruction or proper disposal of those documents after the information is no longer needed. Furthermore, counties must take "reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." Colo. Rev. Stat. § 6-1-713.5(1).

EXPANDED BREACH NOTIFICATION

When a county becomes aware that a breach of unencrypted computerized data has occurred, it must inform the affected parties within 30 days. Counties may delay the notification if law enforcement investigating the breach deems a delay necessary for their investigation; however, counties must inform affected parties in the most expedient time possible without unreasonable delay once cleared to do so by law enforcement. Third-party service providers used by the county must be informed that their cooperation with the county and law enforcement is required in the case of a data breach.

ATTORNEY GENERAL & CONSUMER REPORTING NOTIFICATION

For data breaches that compromise the personal data of more than 500 Colorado citizens, the Colorado Attorney General's Office must be notified no later than 30 days after the date the breach was discovered. For data breaches affecting more than 1000 Colorado residents, the governmental entity must also notify all nationwide consumer reporting agencies. Furthermore, any waivers of notification rights or responsibilities that residents may have signed before the amended legislation are void as they are now against public policy.

WHAT THIS MEANS FOR COUNTIES

Counties should ensure that they have a written policy detailing the safe disposal of electronic and paper records containing personal identifying information and ensure that they are taking reasonable security precautions to protect that information and comply with the notification requirement. For more information or for a sample policy, please contact CTSI at 303 861 0507.