144.2131 SECURITY OF VITAL RECORDS SYSTEM.

The state registrar shall:

(1) authenticate all users of the system of vital records and document that all users require access based on their official duties;

(2) authorize authenticated users of the system of vital records to access specific components of the vital records systems necessary for their official roles and duties;

(3) establish separation of duties between staff roles that may be susceptible to fraud or misuse and routinely perform audits of staff work for the purposes of identifying fraud or misuse within the vital records system;

(4) require that authenticated and authorized users of the system of vital records maintain a specified level of training related to security and provide written acknowledgment of security procedures and penalties;

(5) validate data submitted for registration through site visits or with independent sources outside the registration system at a frequency specified by the state registrar to maximize the integrity of the data collected;

(6) protect personally identifiable information and maintain systems pursuant to applicable state and federal laws;

(7) accept a report of death if the decedent was born in Minnesota or if the decedent was a resident of Minnesota from the United States Department of Defense or the United States Department of State when the death of a United States citizen occurs outside the United States;

(8) match death records registered in Minnesota and death records provided from other jurisdictions to live birth records in Minnesota;

(9) match death records received from the United States Department of Defense or the United States Department of State for deaths of United States citizens occurring outside the United States to live birth records in Minnesota;

(10) work with law enforcement to initiate and provide evidence for active fraud investigations;

(11) provide secure workplace, storage, and technology environments that have limited role-based access;

(12) maintain overt, covert, and forensic security measures for certifications, verifications, and automated systems that are part of the vital records system; and

(13) comply with applicable state and federal laws and rules associated with information technology systems and related information security requirements.

History: *2013 c 108 art 12 s 18; 2015 c 21 art 1 s 109*