CHAPTER 62a

STATE CONTRACTING: GENERAL PROVISIONS

Table of Contents



Sec. 4e-70. Requirements for state contractors who receive confidential information. Definitions. Minimum requirements. Prohibitions. Breach. Violation. Ban. Effect on other applicable laws. (a) As used in this section and section 4e-71:

(1) "Contractor" means an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to provide goods or services to the state.

(2) "State agency" means any agency with a department head, as defined in section 4-5.

(3) "State contracting agency" means any state agency disclosing confidential information to a contractor pursuant to a written agreement with such contractor for the provision of goods or services for the state.

(4) "Confidential information" means an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation,

personally identifiable information subject to 34 CFR 99, as amended from time to time and protected health information, as defined in 45 CFR 160.103, as amended from time to time. In addition, "confidential information" includes any information that a state contracting agency identifies as confidential to the contractor. "Confidential information" does not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records that are lawfully made available to the general public.

(5) "Confidential information breach" means an instance where an unauthorized person or entity accesses confidential information that is subject to or otherwise used in conjunction with any part of a written agreement with a state contracting agency in any manner, including, but not limited to, the following occurrences: (A) Any confidential information that is not encrypted or secured by any other method or technology that renders the personal information unreadable or unusable is misplaced, lost, stolen or subject to unauthorized access; (B) one or more third parties have accessed, or taken control or possession of, without prior written authorization from the state, (i) any confidential information that is not encrypted or protected, or (ii) any encrypted or protected confidential information together with the confidential process or key that is capable of compromising the integrity of the confidential information; or (C) there is a substantial risk of identity theft or fraud of the client of the state contracting agency, the contractor, the state contracting agency or the state.

(b) Except as provided in section 4e-71, every written agreement that authorizes a state contracting agency to share confidential information with a contractor shall require the contractor to, at a minimum, do the following:

(1) At its own expense, protect from a confidential information breach any and all confidential information that it comes to possess or control, wherever and however stored or maintained;

(2) Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law and written policies of the state contained in the agreement. Such data-security program shall include, but not be limited to, the following: (A) A security policy for contractor employees related to the storage, access and transportation of data containing confidential information; (B) reasonable restrictions on access to records containing confidential information, including the area where such records are kept and secure passwords for electronically stored records; (C) a process for reviewing policies and security measures at least annually; and (D) an active and ongoing employee security awareness program that is mandatory for all employees who may have access to confidential information provided by the state contracting agency that, at a minimum, advises such employees of the confidentiality of

the information, the safeguards required to protect the information and any applicable civil and criminal penalties for noncompliance pursuant to state and federal law;

(3) Limit access to confidential information to authorized contractor employees and authorized agents of the contractor, for authorized purposes as necessary for the completion of the contracted services or provision of the contracted goods;

(4) Maintain all electronic data constituting confidential information obtained from state contracting agencies: (A) In a secure server; (B) on secure drives; (C) behind firewall protections and monitored by intrusion detection software; (D) in a manner where access is restricted to authorized employees and their authorized agents; and (E) as otherwise required under state and federal law;

(5) Implement, maintain and update security and breach investigation procedures that are appropriate given the nature of the information disclosed and that are reasonably designed to protect the confidential information from unauthorized access, use, modification, disclosure, manipulation or destruction;

(6) Notify the state contracting agency and the Attorney General as soon as practical after the contractor becomes aware of or has reason to believe that any confidential information that the contractor possesses or controls has been subject to a confidential information breach;

(7) Immediately cease all use of the data provided by the state contracting agency or developed internally by the contractor pursuant to a written agreement with the state if so directed by the state contracting agency; and

(8) In accordance with the proposed timetable established pursuant to subdivision (1) of subsection (e) of this section, submit to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred. Any report submitted under this subdivision shall be considered information given in confidence and not required by statute, under subparagraph (B) of subdivision (5) of subsection (b) of section 1-210.

(c) A contractor shall not:

(1) Store data constituting confidential information on stand-alone computer or notebook hard disks or portable storage devices such as external or removable hard drives, flash cards, flash drives, compact disks or digital video disks, except as provided for in the agreement and including alternate measures of security assurance approved pursuant to section 4e-71; or

(2) Copy, reproduce or transmit data constituting confidential information, except as necessary for the completion of the contracted services or provision of the contracted goods.

(d) All copies of data constituting confidential information of any type, including, but not limited to, any modifications or additions to data that contain confidential information, are subject to the provisions of this section in the same manner as the original data.

(e) Except as provided in section 4e-71, every written agreement that authorizes a state contracting agency to share confidential information with a contractor shall:

(1) Include a proposed timetable for submittal to the office of the Attorney General and the state contracting agency either (A) a report detailing the breach or suspected breach, or (B) a report detailing why, upon further investigation, the contractor believes no breach has occurred; and

(2) Specify how the cost of any notification about, or investigation into, a confidential information breach is to be apportioned when the state contracting agency or contractor is the subject of such a breach.

(f) The notice required by subsection (b) of this section may be delayed (1) at the state contracting agency's sole discretion based on the report and, if applicable, the plan provided, or (2) if a law enforcement agency or intelligence agency notifies the contractor that such notification would impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subsection, notification shall be given as soon as reasonably feasible by the contractor to the applicable state contracting agency.

(g) The Attorney General may investigate any violation of this section. If the Attorney General finds that a contractor has violated or is violating any provision of this section, the Attorney General may bring a civil action in the superior court for the judicial district of Hartford under this section in the name of the state against such contractor. Nothing in this section shall be construed to create a private right of action.

(h) If the confidential information or personally identifiable information, as defined in 34 CFR 99.3, that has been subject to a confidential information breach consists of education records, the contractor may be subject to a five-year ban from receiving access to such information imposed by the State Department of Education.

(i) The requirements of this section shall be in addition to the requirements of section 36a-701b, and nothing in this section shall be construed to supersede a contractor's obligations pursuant to the Health Insurance Portability and Accountability Act of 1996 P.L. 104-191 (HIPAA), the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, (FERPA) or any other applicable federal or state law.

(P.A. 15-142, S. 1.)

History: P.A. 15-142 effective July 1, 2015.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 4e-71. Additional protections and alternate measures of security assurance for sharing of confidential information. The Secretary of the Office of Policy and Management, or the secretary's designee, may require additional protections or alternate measures of security assurance for any requirement of section 4e-70 where the facts and circumstances warrant such additional requirement or alternate measure after taking into consideration, among other factors, (1) the type of confidential information being shared, (2) the amount of confidential information being shared, (3) the purpose for which the information is being shared, and (4) the types of goods or services being contracted for.

(P.A. 15-142, S. 2.)

History: P.A. 15-142 effective July 1, 2015.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Secs. 4e-72 to 4e-75. Reserved for future use.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)

Sec. 4e-76. Modification of contracts. (a) The state may, in any public or special act, modify a contract to which it is a party (1) if any impairment to the contract is not substantial, or (2) (A) if any impairment to the contract is substantial, the public or special act serves a legitimate public purpose such as remedying a general social or economic problem, and (B) if such purpose is demonstrated, the means chosen to accomplish such purpose are reasonable and necessary.

(b) Any such impairment of a contract as described in subsection (a) of this section may be considered reasonable and necessary if (1) the state did not consider such impairment on par with other policy alternatives, (2) the state did not impose a drastic impairment when an evident and more moderate course of action would serve its purpose equally well, and (3) the state did not act unreasonably in light of the surrounding circumstances.

(c) Subsections (a) and (b) of this section shall not be construed to apply to (1) investments by the State Treasurer or administered by the State Treasurer or any contracts related thereto, or (2) bonds, notes, evidences of indebtedness or other direct or contingent obligations of the state for borrowed money or any contracts related thereto.

(June Sp. Sess. P.A. 17-2, S. 221; June Sp. Sess. P.A. 17-4, S. 22.)

History: June Sp. Sess. P.A. 17-2 effective October 31, 2017; June Sp. Sess. P.A. 17-4 added Subsec. (c) re construction of Subsecs. (a) and (b), effective November 21, 2017.

(Return to Chapter Table of Contents) (Return to List of Chapters) (Return to List of Titles)