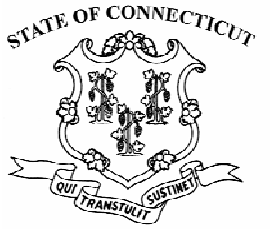

Substitute Senate Bill No. 949

Public Act No. 15-142

AN ACT IMPROVING DATA SECURITY AND AGENCY EFFECTIVENESS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective July 1, 2015*) (a) As used in this section and section 2 of this act:

(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 of the general statutes.

(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 2 of this act, 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 of the general statutes.

(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 2 of this act; 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 2 of this act, 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 of the general statutes, as amended by this act, 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.

Sec. 2. (NEW) (*Effective July 1, 2015*) 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 1 of this act 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.

Sec. 3. Section 4-66 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective from passage*):

The Secretary of the Office of Policy and Management shall have the following functions and powers:

(1) To keep on file information concerning the state's general accounts;

(2) **[**to**]** To furnish all accounting statements relating to the financial condition of the state as a whole, to the condition and operation of state funds, to appropriations, to reserves and to costs of operations;

(3) **[**to**]** To furnish such statements as and when they are required for administrative purposes and, at the end of each fiscal period, to prepare and publish such financial statements and data as will convey to the General Assembly the essential facts as to the financial condition, the revenues and expenditures and the costs of operations of the state government;

(4) **[**to**]** To furnish to the State Comptroller on or before the twentieth day of each month cumulative monthly statements of revenues and expenditures to the end of the last-completed month together with **[**(1)**]** (A) a statement of estimated revenue by source to the end of the fiscal year, at least in the same detail as appears in the budget act, and **[**(2)**]** (B) a statement of appropriation requirements of the state's General Fund to the end of the fiscal year itemized as far as practicable for each budgeted agency, including estimates of lapsing appropriations, unallocated lapsing balances and unallocated appropriation requirements;

(5) **[**to**]** To transmit to the Office of Fiscal Analysis a copy of monthly

position data and monthly bond project run;

(6) **[**to**]** To inquire into the operation of, and make or recommend improvement in, the methods employed in the preparation of the budget and the procedure followed in determining whether the funds expended by the departments, boards, commissions and institutions supported in whole or in part by the state are wisely, judiciously and economically expended and to submit such findings and recommendations to the General Assembly at each regular session, together with drafts of proposed legislation, if any;

(7) **[**to**]** To examine each department, state college, state hospital, state-aided hospital, reformatory and prison and each other institution or other agency supported in whole or in part by the state, except public schools, for the purpose of determining the effectiveness of its policies, management, internal organization and operating procedures and the character, amount, quality and cost of the service rendered by each such department, institution or agency;

(8) **[**to**]** To recommend, and to assist any such department, institution or agency to effect, improvements in organization, management methods and procedures and to report its findings and recommendations and submit drafts of proposed legislation, if any, to the General Assembly at each regular session;

(9) **[**to**]** To consider and devise ways and means whereby comprehensive plans and designs to meet the needs of the several departments and institutions with respect to physical plant and equipment and whereby financial plans and programs for the capital expenditures involved may be made in advance and to make or assist in making such plans;

(10) **[**to**]** To devise and prescribe the form of operating reports that shall be periodically required from the several departments, boards,

commissions, institutions and agencies supported in whole or in part by the state;

(11) **[**to**]** To require the several departments, boards, commissions, institutions and agencies to make such reports for such periods as said secretary may determine; and

(12) **[**to**]** To verify the correctness of, and to analyze, all such reports and to take such action as may be deemed necessary to remedy unsatisfactory conditions disclosed by such reports.

Sec. 4. (NEW) (*Effective July 1, 2015*) (a) For purposes of this section:

(1) "Data" means statistical or factual information that: (A) is reflected in a list, table, graph, chart, or other nonnarrative form that can be digitally transmitted or processed; (B) is regularly created and maintained by or on behalf of an executive agency; and (C) records a measurement, transaction or determination related to the mission of the executive agency or is provided to such agency by any third party as required by any provision of law. "Data" does not include return and return information, as defined in section 12-15 of the general statutes;

(2) "Executive agency" means any agency with a department head, as defined in section 4-5 of the general statutes, a constituent unit of higher education, as defined in section 10a-1 of the general statutes, or the Office of Higher Education, established by section 10a-1d of the general statutes; and

(3) "State agency" means any office, department, board, council, commission, institution, constituent unit of the state system of higher education, technical high school or other agency in the executive, legislative or judicial branch of state government.

(b) The Secretary of the Office of Policy and Management shall

develop a program to access, link, analyze and share data maintained by executive agencies and to respond to queries from any state agency, and from any private entity or person that would otherwise require access to data maintained by two or more executive agencies. The secretary shall give priority to queries that seek to measure outcomes for state-funded programs or that may facilitate the development of policies to promote the effective, efficient and best use of state resources.

(c) The secretary shall establish policies and procedures to:

(1) Review and respond to queries to ensure (A) a response is permitted under state and federal law; (B) the privacy and confidentiality of protected data can be assured; and (C) the query is based on sound research design principles; and

(2) Protect and ensure the security, privacy, confidentiality and administrative value of data collected and maintained by executive agencies.

(d) The secretary shall, in consultation with the Chief Information Officer, develop and implement a secure information technology solution to link data across executive agencies and to develop and implement a detailed data security and safeguarding plan for the data accessed or shared through such solution.

(e) The secretary shall request from, and execute a memorandum of agreement with, each executive agency detailing data-sharing between the agency and the Office of Policy and Management. Each such agreement shall authorize the Office of Policy and Management to act on behalf of the executive agency that is a party to such agreement for purposes of data access, matching and sharing and shall include provisions to ensure the proper use, security and confidentiality of the data shared. Any executive agency that is requested by the secretary to

execute such an agreement shall comply with such request.

(f) The secretary shall notify the applicable executive agency when data within such agency's custody has been requested under subsection (b) of this section.

(g) The Secretary of the Office of Policy and Management shall be an authorized representative of the Labor Commissioner or administrator of unemployment compensation under chapter 567 of the general statutes and shall receive upon request by the secretary any information in the Labor Commissioner's possession relating to employment records that may include, but need not be limited to: Employee name, Social Security number, current residential address, name and address of the employer, employer North American Industry Classification System code and wages. In addition, the Labor Department, upon the request of the Secretary of the Office of Policy and Management, shall furnish unemployment compensation wage records contained in the quarterly returns required and maintained by the Labor Commissioner pursuant to section 31-254 of the general statutes, for purposes of this section.

(h) For the purposes of the Freedom of Information Act, as defined in section 1-200 of the general statutes, the Office of Policy and Management shall not be considered the agency with custody or control of any public records or files that are made accessible to said office pursuant to this section, but shall be considered the agency with custody and control of any public records or files created by the Office of Policy and Management, including, but not limited to, all reports generated by said office in response to queries posed under subsection (b) of this section.

Sec. 5. (NEW) (*Effective October 1, 2015*) (a) As used in this section:

(1) "Breach of security" has the same meaning as provided in section

36a-701b of the general statutes, as amended by this act;

(2) "Company" means a health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager, as defined in section 38a-479aaa of the general statutes, third-party administrator, as defined in section 38a-720 of the general statutes, that administers health benefits, and utilization review company, as defined in section 38a-591a of the general statutes;

(3) "Encryption" means the rendering of electronic data into a form that is unreadable or unusable without the use of a confidential process or key; and

(4) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data: (A) A Social Security number; (B) a driver's license number or a state identification number; (C) protected health information as defined in 45 CFR 160.103, as amended from time to time; (D) a taxpayer identification number; (E) an alien registration number; (F) a government passport number; (G) a demand deposit account number; (H) a savings account number; (I) a credit card number; (J) a debit card number; or (K) unique biometric data such as a fingerprint, a voice print, a retina or an iris image, or other unique physical representations. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

(b) (1) Not later than October 1, 2017, each company shall implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company. Such security program shall be in writing and contain administrative, technical and physical safeguards that are appropriate to (A) the size,

scope and type of business of such company, (B) the amount of resources available to such company, (C) the amount of data compiled or maintained by such company, and (D) the need for security and confidentiality of such data.

(2) Each company shall update such security program as often as necessary and practicable but at least annually and shall include in such security program:

(A) Secure computer and Internet user authentication protocols that include, but are not limited to, (i) control of user identifications and other identifiers, (ii) multifactor authentication that includes a reasonably secure method of assigning and selecting a password or the use of unique identifier technologies such as biometrics or security tokens, (iii) control of security passwords to ensure that such passwords are maintained in a location and format that do not compromise the security of personal information, (iv) restriction of access to only active users and active user accounts, and (v) the blocking of access after multiple unsuccessful attempts to gain access to data compiled or maintained by a company;

(B) Secure access control measures that include, but are not limited to, (i) restriction of access to personal information to only those individuals who require such data to perform their job duties, (ii) assignment, to each individual with computer and Internet access to data compiled or maintained by such company, of passwords that are not vendor-assigned default passwords and that require resetting not less than every six months and of unique user identifications, that are designed to maintain the integrity of the security of the access controls, (iii) encryption of all personal information while being transmitted on a public Internet network or wirelessly, (iv) encryption of all personal information stored on a laptop computer or other portable device, (v) monitoring of such company's security systems for breaches of security, (vi) for personal information that is stored or accessible on a

system that is connected to the Internet, reasonably up-to-date software security protection that can support updates and patches, including, but not limited to, firewall protection, operating system security patches and malicious software protection, and (vii) employee education and training on the proper use of the company's security systems and the importance of the security of personal information;

(C) Designation of one or more employees to oversee such security program and the maintenance of such security program;

(D) (i) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality or integrity of any electronic, paper or other records that contain personal information, (ii) evaluation and improvement where necessary of the effectiveness of the current safeguards for limiting such risks, including, but not limited to, (I) ongoing employee training, (II) employee compliance with security policies and procedures, and (III) means for detecting and preventing security system failures, and (iii) the upgrade of safeguards as necessary to limit risks;

(E) Development of employee security policies and procedures for the storage of, access to, transport of and transmittal of personal information off-premises;

(F) Imposition of disciplinary measures on employees for violating security policies or procedures or other provisions of the comprehensive information security program;

(G) Prevention of terminated, inactive or retired employees from accessing personal information;

(H) Oversight of third parties with which such company enters into contracts or agreements that have or will have access to personal information compiled or maintained by the company, by (i) selecting third parties that are capable of maintaining appropriate safeguards

consistent with this subsection to protect such personal information, and (ii) requiring such third parties by contract or agreement to implement and maintain such safeguards;

(I) Reasonable restrictions on physical access to personal information in paper format and storage of such data in locked facilities, storage areas or containers;

(J) Review of the scope of the secure access control measures at least annually or whenever there is a material change in the company's business practices that may affect the security, confidentiality or integrity of personal information;

(K) Mandatory post-incident review by the company following any actual or suspected breach of security, and documentation of actions the company takes in response to such breach, including any changes the company makes to its business practices relating to the safeguarding of personal information; and

(L) Any other safeguards the company believes will enhance its comprehensive information security program.

(c) On or after October 1, 2017, each company shall certify annually to the Insurance Department, under penalty of perjury, that it maintains a comprehensive information security program that complies with the requirements of subsection (b) of this section.

(d) Upon request by the Insurance Commissioner or by the Attorney General, each company shall provide to the commissioner or the Attorney General a copy of its comprehensive information security program. If the commissioner or the Attorney General determines that such security program does not conform to the requirements set forth in subsection (b) of this section, the commissioner or the Attorney General shall notify the company of such determination and such company shall make changes as necessary to bring such security

program into conformance to the commissioner's or the Attorney General's satisfaction.

(e) Each company that discovers an actual or suspected breach of security shall (1) comply with the notice requirements set forth in section 36a-701b of the general statutes, as amended by this act, (2) be subject to the penalty set forth in subsection (g) of section 36a-701b of the general statutes, as amended by this act, for failure to comply, and (3) offer appropriate identity theft prevention services and, if applicable, identity theft mitigation services, as set forth in subparagraph (B) of subdivision (2) of subsection (b) of section 36a-701b of the general statutes, as amended by this act.

(f) The Insurance Commissioner shall enforce the provisions of subsections (b) to (d), inclusive, of this section.

Sec. 6. Section 36a-701b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2015*):

(a) For purposes of this section, (1) "breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; and (2) "personal information" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: **[**(1)**]** (A) Social Security number; **[**(2)**]** (B) driver's license number or state identification card number; or **[**(3)**]** (C) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely

distributed media.

(b) (1) Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was **[**,**]** breached or is reasonably believed to have been **[**, accessed by an unauthorized person through such breach of security**]** breached. Such notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

(2) If notice of a breach of security is required by subdivision (1) of this subsection: **[**, the**]**

(A) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General; and

(B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to

each resident whose personal information under subparagraph (A) of subdivision (4) of subsection (a) of section 5 of this act or subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twelve months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

(c) Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was **[**,**]** breached or is reasonably believed to have been **[**accessed by an unauthorized person**]** breached.

(d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

(e) Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this

subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information. Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.

(f) Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

(g) Failure to comply with the requirements of this section shall

constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

Sec. 7. (NEW) (*Effective July 1, 2016*) (a) As used in this section, "smartphone" means a hand-held cellular mobile telephone or other mobile voice communications handset device that includes all of the following features: (1) A mobile operating system, (2) the capability to utilize mobile software applications, access and browse the Internet, utilize text messaging, utilize digital voice service and send and receive electronic mail, (3) wireless network connectivity, and (4) the capability of operating on a long-term evolution network or on any successor wireless data network communication standard. A smartphone does not include a telephone commonly referred to as a "feature" or "messaging" telephone, a laptop computer, a tablet device or a device that has only electronic reading capability.

(b) From the effective date of this section until July 1, 2017, no person shall offer a new model of a smartphone for retail sale in this state, unless such smartphone includes software or hardware, or a combination of both, or software that is downloadable upon initial activation upon purchase, that once initiated and successfully communicated by an authorized user, render inoperable the essential features of the smartphone to an unauthorized user.

Approved June 30, 2015