__SHB 1071__ - S COMM AMD
By Committee on Environment, Energy & Technology

OUT OF ORDER 04/15/2019

Strike everything after the enacting clause and insert the following:

"__NEW SECTION.__ **Sec. 1.** A new section is added to chapter 19.255 RCW to read as follows:

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(2)(a) "Personal information" means:

(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) Social security number;

(B) Driver's license number or Washington identification card number;

(C) Account number or 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, or any other numbers or information that can be used to access a person's financial account;

(D) Full date of birth;

(E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

(F) Student, military, or passport identification number;

(G) Health insurance policy number or health insurance identification number;

(H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or

(I) Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

(ii) Username or email address in combination with a password or security questions and answers that would permit access to an online account; and

(iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:

(A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and

(B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(b) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(3) "Secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

Sec. 2. RCW 19.255.010 and 2015 c 64 s 2 are each amended to read as follows:

(1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system ((~~following discovery or notification of the breach in the security of the data~~)) to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains or possesses data that may include((~~s~~)) personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) ((~~For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.~~

~~(5) For purposes of this section, "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 elements:~~

~~(a) Social security number;~~

~~(b) Driver's license number or Washington identification card number; or~~

~~(c) Account number or 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.~~

~~(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

~~(7) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.~~

~~(8)~~)) For purposes of this section and except under subsection((~~s (9) and (10)~~)) (5) of this section and section 3 of this act, ((~~"~~))notice((~~"~~)) may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; ((~~or~~))

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the person or business has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media; or

(d)(i) Electronic or other form, if the breach of the security of the system involves personal information including a user name or password. The notice must direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer;

(ii) However, when the breach of the security of the system involves login credentials of an email account furnished by the person or business, the person or business may not comply with this section by providing the notification to that email address, but must comply with this section by providing notice using another method described in this section or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the person or business knows the resident customarily accesses the account.

((~~(9)~~)) (5) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

((~~(10) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection (15) of this section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection (16) of this section.~~

~~(11) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this section with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to subsection (15) of this section in addition to providing notice to its primary federal regulator.~~

~~(12) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.~~

~~(13)(a) Any consumer injured by a violation of this section may institute a civil action to recover damages.~~

~~(b) Any person or business that violates, proposes to violate, or has violated this section may be enjoined.~~

~~(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.~~

~~(14)~~)) (6) Any person or business that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting person or business subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; ((~~and~~))

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

((~~(15)~~)) (7) Any person or business that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall((~~, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general~~)) notify the attorney general of the breach no more than thirty days after the breach was discovered.

(a) The ((~~person or business~~)) notice to the attorney general shall ((~~also provide to the attorney general~~)) include the following information:

(i) The number of Washington consumers affected by the breach, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;

(iv) A summary of steps taken to contain the breach; and

(v) A single sample copy of the security breach notification, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

((~~(16)~~)) (8) Notification to affected consumers ((~~and to the attorney general~~)) under this section must be made in the most expedient time possible ((~~and~~)), without unreasonable delay, and no more than ((~~forty-five~~)) thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

((~~(17) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this section. For actions brought by the attorney general to enforce this section, the legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the attorney general to enforce this section, a violation of this section is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this section may not be brought under RCW 19.86.090.~~))

NEW SECTION. **Sec. 3.** A new section is added to chapter 19.255 RCW to read as follows:

(1) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this chapter with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to RCW 19.255.010(7) in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015, notwithstanding the timeline in RCW 19.255.010(7).

(2) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this chapter with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to RCW 19.255.010 in addition to providing notice to its primary federal regulator.

NEW SECTION. **Sec. 4.** A new section is added to chapter 19.255 RCW to read as follows:

(1) Any waiver of the provisions of this chapter is contrary to public policy, and is void and unenforceable.

(2) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter. For actions brought by the attorney general to enforce this chapter, the legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the attorney general to enforce this chapter, a violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this chapter may not be brought under RCW 19.86.090.

(3)(a) Any consumer injured by a violation of this chapter may institute a civil action to recover damages.

(b) Any person or business that violates, proposes to violate, or has violated this chapter may be enjoined.

(c) The rights and remedies available under this chapter are cumulative to each other and to any other rights and remedies available under law.

Sec. 5. RCW 42.56.590 and 2015 c 64 s 3 are each amended to read as follows:

(1)((~~(a)~~)) Any agency that owns or licenses data that includes personal information shall disclose any breach of the security of the system ((~~following discovery or notification of the breach in the security of the data~~)) to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

((~~(b) For purposes of this section, "agency" means the same as in RCW 42.56.010.~~))

(2) Any agency that maintains or possesses data that may include((~~s~~)) personal information that the agency does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) ((~~For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the~~

~~personal information is not used or subject to further unauthorized disclosure.~~

~~(5) For purposes of this section, "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 elements:~~

~~(a) Social security number;~~

~~(b) Driver's license number or Washington identification card number; or~~

~~(c) Full account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account.~~

~~(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.~~

~~(7) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.~~

~~(8)~~)) For purposes of this section and except under subsection((~~s (9) and (10)~~)) (5) of this section and section 6 of this act, notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the agency has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the agency's web site page, if the agency maintains one; and

(iii) Notification to major statewide media.

((~~(9)~~)) (5) An agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

((~~(10) A covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection (14) of this section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection (15) of this section.~~

~~(11) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.~~

~~(12)(a) Any individual injured by a violation of this section may institute a civil action to recover damages.~~

~~(b) Any agency that violates, proposes to violate, or has violated this section may be enjoined.~~

~~(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.~~

~~(13)~~)) (6) Any agency that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting agency subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

((~~(14)~~)) (7) Any agency that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall((~~, by the time notice is provided to affected individuals, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to~~)) notify the attorney general of the breach no more than thirty days after the breach was discovered.

(a) The ((~~agency shall also provide~~)) notice to the attorney general must include the following information:

(i) The number of Washington residents affected by the breach, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

(iii) A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach;

(iv) A summary of steps taken to contain the breach; and

(v) A single sample copy of the security breach notification, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

((~~(15)~~)) (8) Notification to affected individuals ((~~and to the attorney general~~)) must be made in the most expedient time possible ((~~and~~)), without unreasonable delay, and no more than ((~~forty-five~~)) thirty calendar days after the breach was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. An agency may delay notification to the consumer for up to an additional fourteen days to allow for notification to be translated into the primary language of the affected consumers.

(9) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the

personal information is not used or subject to further unauthorized disclosure.

(10)(a) For purposes of this section, "personal information" means:

(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements:

(A) Social security number;

(B) Driver's license number or Washington identification card number;

(C) Account number, credit or debit card number, or any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;

(D) Full date of birth;

(E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

(F) Student, military, or passport identification number;

(G) Health insurance policy number or health insurance identification number;

(H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or

(I) Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;

(ii) User name or email address in combination with a password or security questions and answers that would permit access to an online account; and

(iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if:

(A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and

(B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(b) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(11) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

NEW SECTION. **Sec. 6.** A new section is added to chapter 42.56 RCW to read as follows:

A covered entity under the federal health insurance portability and accountability act of 1996, Title 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this chapter with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to RCW 42.56.590(7) in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015, notwithstanding the timeline in RCW 42.56.590(7).

NEW SECTION. **Sec. 7.** A new section is added to chapter 42.56 RCW to read as follows:

(1) Any waiver of the provisions of RCW 42.56.590 or section 6 of this act is contrary to public policy, and is void and unenforceable.

(2)(a) Any consumer injured by a violation of RCW 42.56.590 may institute a civil action to recover damages.

(b) Any agency that violates, proposes to violate, or has violated RCW 42.56.590 may be enjoined.

(c) The rights and remedies available under RCW 42.56.590 are cumulative to each other and to any other rights and remedies available under law.

NEW SECTION. **Sec. 8.** This act takes effect March 1, 2020."

SHB 1071 - S COMM AMD
By Committee on Environment, Energy & Technology

OUT OF ORDER 04/15/2019

On page 1, line 2 of the title, after "information;" strike the remainder of the title and insert "amending RCW 19.255.010 and 42.56.590; adding new sections to chapter 19.255 RCW; adding new sections to chapter 42.56 RCW; and providing an effective date."

EFFECT: Authorizes alternative notification options if the breach of security involves personal information including username or password or login credentials of an email account. Authorizes an agency to delay notification to a consumer for up to an additional fourteen days in order for the notification to be translated into the consumer's primary language. Makes technical corrections.

--- END ---