

**SHB 1071** - S COMM AMD

By Committee on Environment, Energy & Technology

**OUT OF ORDER 04/15/2019**

1 Strike everything after the enacting clause and insert the  
2 following:

3 "NEW SECTION. **Sec. 1.** A new section is added to chapter 19.255  
4 RCW to read as follows:

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

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

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

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

18 (A) Social security number;

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

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

26 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 (5) ~~For purposes of this section, "personal information" means an~~  
23 ~~individual's first name or first initial and last name in combination~~  
24 ~~with any one or more of the following data elements:~~

25 (a) ~~Social security number;~~

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

28 (c) ~~Account number or credit or debit card number, in combination~~  
29 ~~with any required security code, access code, or password that would~~  
30 ~~permit access to an individual's financial account.~~

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

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

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

4       (a) Written notice;

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

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

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

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

18       (iii) Notification to major statewide media; or

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

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

38       (~~(9))~~) (5) A person or business that maintains its own  
39 notification procedures as part of an information security policy for  
40 the treatment of personal information and is otherwise consistent

1 with the timing requirements of this section is in compliance with  
2 the notification requirements of this section if the person or  
3 business notifies subject persons in accordance with its policies in  
4 the event of a breach of security of the system.

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

18 ~~(11) A financial institution under the authority of the office of~~  
19 ~~the comptroller of the currency, the federal deposit insurance~~  
20 ~~corporation, the national credit union administration, or the federal~~  
21 ~~reserve system is deemed to have complied with the requirements of~~  
22 ~~this section with respect to "sensitive customer information" as~~  
23 ~~defined in the interagency guidelines establishing information~~  
24 ~~security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part~~  
25 ~~208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part~~  
26 ~~364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they~~  
27 ~~existed on July 24, 2015, if the financial institution provides~~  
28 ~~notice to affected consumers pursuant to the interagency guidelines~~  
29 ~~and the notice complies with the customer notice provisions of the~~  
30 ~~interagency guidelines establishing information security~~  
31 ~~standards and the interagency guidance on response programs for~~  
32 ~~unauthorized access to customer information and customer notice under~~  
33 ~~12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall~~  
34 ~~notify the attorney general pursuant to subsection (15) of this~~  
35 ~~section in addition to providing notice to its primary federal~~  
36 ~~regulator.~~

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

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

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

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

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

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

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

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

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

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

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

20 ~~((15))~~ (7) Any person or business that is required to issue a  
21 notification pursuant to this section to more than five hundred  
22 Washington residents as a result of a single breach shall ~~((, by the~~  
23 ~~time notice is provided to affected consumers, electronically submit~~  
24 ~~a single sample copy of that security breach notification, excluding~~  
25 ~~any personally identifiable information, to the attorney general))~~  
26 notify the attorney general of the breach no more than thirty days  
27 after the breach was discovered.

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

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

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

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

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

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

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

4 ~~((16))~~ (8) Notification to affected consumers ~~((and to the~~  
5 ~~attorney general))~~ under this section must be made in the most  
6 expedient time possible ~~((and)),~~ without unreasonable delay, and no  
7 more than ~~((forty-five))~~ thirty calendar days after the breach was  
8 discovered, unless the delay is at the request of law enforcement as  
9 provided in subsection (3) of this section, or the delay is due to  
10 any measures necessary to determine the scope of the breach and  
11 restore the reasonable integrity of the data system.

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

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

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

1 (2) A financial institution under the authority of the office of  
2 the comptroller of the currency, the federal deposit insurance  
3 corporation, the national credit union administration, or the federal  
4 reserve system is deemed to have complied with the requirements of  
5 this chapter with respect to "sensitive customer information" as  
6 defined in the interagency guidelines establishing information  
7 security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part  
8 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part  
9 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they  
10 existed on July 24, 2015, if the financial institution provides  
11 notice to affected consumers pursuant to the interagency guidelines  
12 and the notice complies with the customer notice provisions of the  
13 interagency guidelines establishing information security standards  
14 and the interagency guidance on response programs for unauthorized  
15 access to customer information and customer notice under 12 C.F.R.  
16 Part 364 as it existed on July 24, 2015. The entity shall notify the  
17 attorney general pursuant to RCW 19.255.010 in addition to providing  
18 notice to its primary federal regulator.

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

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

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

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

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



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

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

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

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

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

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

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

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

3 ~~(5) For purposes of this section, "personal information" means an~~  
4 ~~individual's first name or first initial and last name in combination~~  
5 ~~with any one or more of the following data elements:~~

6 ~~(a) Social security number;~~

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

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

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

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

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

24 ~~(a) Written notice;~~

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

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

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

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

37 ~~(iii) Notification to major statewide media.~~

38 ~~((9)) (5) An agency that maintains its own notification~~  
39 ~~procedures as part of an information security policy for the~~  
40 ~~treatment of personal information and is otherwise consistent with~~

1 the timing requirements of this section is in compliance with the  
2 notification requirements of this section if it notifies subject  
3 persons in accordance with its policies in the event of a breach of  
4 security of the system.

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

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

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

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

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

27 ~~(13))~~ (6) Any agency that is required to issue notification  
28 pursuant to this section shall meet all of the following  
29 requirements:

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

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

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

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

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

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

1       ~~((14))~~ (7) Any agency that is required to issue a notification  
2 pursuant to this section to more than five hundred Washington  
3 residents as a result of a single breach shall ~~((, by the time notice~~  
4 ~~is provided to affected individuals, electronically submit a single~~  
5 ~~sample copy of that security breach notification, excluding any~~  
6 ~~personally identifiable information, to)) notify the attorney general  
7 of the breach no more than thirty days after the breach was  
8 discovered.~~

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

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

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

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

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

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

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

23       ~~((15))~~ (8) Notification to affected individuals ~~((and to the~~  
24 ~~attorney general))~~ must be made in the most expedient time possible  
25 ~~((and)),~~ without unreasonable delay, and no more than ~~((forty-five))~~  
26 thirty calendar days after the breach was discovered, unless the  
27 delay is at the request of law enforcement as provided in subsection  
28 (3) of this section, or the delay is due to any measures necessary to  
29 determine the scope of the breach and restore the reasonable  
30 integrity of the data system. An agency may delay notification to the  
31 consumer for up to an additional fourteen days to allow for  
32 notification to be translated into the primary language of the  
33 affected consumers.

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

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

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

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

7 (A) Social security number;

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

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

14 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

8       A covered entity under the federal health insurance portability  
9 and accountability act of 1996, Title 42 U.S.C. Sec. 1320d et seq.,  
10 is deemed to have complied with the requirements of this chapter with  
11 respect to protected health information if it has complied with  
12 section 13402 of the federal health information technology for  
13 economic and clinical health act, P.L. 111-5 as it existed on July  
14 24, 2015. Covered entities shall notify the attorney general pursuant  
15 to RCW 42.56.590(7) in compliance with the timeliness of notification  
16 requirements of section 13402 of the federal health information  
17 technology for economic and clinical health act, P.L. 111-5 as it  
18 existed on July 24, 2015, notwithstanding the timeline in RCW  
19 42.56.590(7).

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

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

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

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

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

31       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**

1        On page 1, line 2 of the title, after "information;" strike the  
2 remainder of the title and insert "amending RCW 19.255.010 and  
3 42.56.590; adding new sections to chapter 19.255 RCW; adding new  
4 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 ---