

SHB 1071 - S COMM AMD
By Committee on Ways & Means

ADOPTED 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 ~~((~~))notice(~~((~~))) 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; ~~((~~)

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) If the breach of the security of the system involves
20 personal information including a user name or password, notice may be
21 provided electronically or by email. The notice must comply with
22 subsections (6), (7), and (8) of this section and must inform the
23 person whose personal information has been breached to promptly
24 change his or her password and security question or answer, as
25 applicable, or to take other appropriate steps to protect the online
26 account with the person or business and all other online accounts for
27 which the person whose personal information has been breached uses
28 the same user name or email address and password or security question
29 or answer;

30 (ii) However, when the breach of the security of the system
31 involves login credentials of an email account furnished by the
32 person or business, the person or business may not provide the
33 notification to that email address, but must provide notice using
34 another method described in this subsection (4). The notice must
35 comply with subsections (6), (7), and (8) of this section and must
36 inform the person whose personal information has been breached to
37 promptly change his or her password and security question or answer,
38 as applicable, or to take other appropriate steps to protect the
39 online account with the person or business and all other online
40 accounts for which the person whose personal information has been

1 breached uses the same user name or email address and password or
2 security question or answer.

3 ((+9)) (5) A person or business that maintains its own
4 notification procedures as part of an information security policy for
5 the treatment of personal information and is otherwise consistent
6 with the timing requirements of this section is in compliance with
7 the notification requirements of this section if the person or
8 business notifies subject persons in accordance with its policies in
9 the event of a breach of security of the system.

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

23 ~~(11) A financial institution under the authority of the office of~~
24 ~~the comptroller of the currency, the federal deposit insurance~~
25 ~~corporation, the national credit union administration, or the federal~~
26 ~~reserve system is deemed to have complied with the requirements of~~
27 ~~this section with respect to "sensitive customer information" as~~
28 ~~defined in the interagency guidelines establishing information~~
29 ~~security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part~~
30 ~~208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part~~
31 ~~364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they~~
32 ~~existed on July 24, 2015, if the financial institution provides~~
33 ~~notice to affected consumers pursuant to the interagency guidelines~~
34 ~~and the notice complies with the customer notice provisions of the~~
35 ~~interagency guidelines establishing information security~~
36 ~~standards and the interagency guidance on response programs for~~
37 ~~unauthorized access to customer information and customer notice under~~
38 ~~12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall~~
39 ~~notify the attorney general pursuant to subsection (15) of this~~

1 ~~section in addition to providing notice to its primary federal~~
2 ~~regulator.~~

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

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

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

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

12 ~~(14))~~ (6) Any person or business that is required to issue
13 notification pursuant to this section shall meet all of the following
14 requirements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 timeliness of notification requirements of section 13402 of the
2 federal health information technology for economic and clinical
3 health act, P.L. 111-5 as it existed on July 24, 2015,
4 notwithstanding the timeline in RCW 19.255.010(7).

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

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

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

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

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

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

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

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

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

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

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

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

38 (4) ~~((For purposes of this section, "breach of the security of
39 the system" means unauthorized acquisition of data that compromises~~

1 ~~the security, confidentiality, or integrity of personal information~~
2 ~~maintained by the agency. Good faith acquisition of personal~~
3 ~~information by an employee or agent of the agency for the purposes of~~
4 ~~the agency is not a breach of the security of the system when the~~
5 ~~personal information is not used or subject to further unauthorized~~
6 ~~disclosure.~~

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

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

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

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

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

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

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

28 ~~(a) Written notice;~~

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

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

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

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

1 (iii) Notification to major statewide media.

2 ~~((9))~~ (5) An agency that maintains its own notification
3 procedures as part of an information security policy for the
4 treatment of personal information and is otherwise consistent with
5 the timing requirements of this section is in compliance with the
6 notification requirements of this section if it notifies subject
7 persons in accordance with its policies in the event of a breach of
8 security of the system.

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

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

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

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

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

31 ~~(13))~~ (6) Any agency that is required to issue notification
32 pursuant to this section shall meet all of the following
33 requirements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

38 (9) For purposes of this section, "breach of the security of the
39 system" means unauthorized acquisition of data that compromises the
40 security, confidentiality, or integrity of personal information

1 maintained by the agency. Good faith acquisition of personal
2 information by an employee or agent of the agency for the purposes of
3 the agency is not a breach of the security of the system when the
4 personal information is not used or subject to further unauthorized
5 disclosure.

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

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

10 (A) Social security number;

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

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

17 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

11 A covered entity under the federal health insurance portability
12 and accountability act of 1996, Title 42 U.S.C. Sec. 1320d et seq.,
13 is deemed to have complied with the requirements of this chapter with
14 respect to protected health information if it has complied with
15 section 13402 of the federal health information technology for
16 economic and clinical health act, P.L. 111-5 as it existed on July
17 24, 2015. Covered entities shall notify the attorney general pursuant
18 to RCW 42.56.590(7) in compliance with the timeliness of notification
19 requirements of section 13402 of the federal health information
20 technology for economic and clinical health act, P.L. 111-5 as it
21 existed on July 24, 2015, notwithstanding the timeline in RCW
22 42.56.590(7).

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

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

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

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

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

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

ADOPTED 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. Clarifies notification compliance requirements if the breach involves personal information including a user name or password or involves login credentials of an email account furnished by the person or business.

--- END ---