
SUBSTITUTE HOUSE BILL 1071

State of Washington

66th Legislature

2019 Regular Session

By House Innovation, Technology & Economic Development (originally sponsored by Representatives Kloba, Dolan, Tarleton, Slatter, Valdez, Ryu, Appleton, Smith, Stanford, and Frame; by request of Attorney General)

READ FIRST TIME 02/08/19.

1 AN ACT Relating to breach of security systems protecting personal
2 information; amending RCW 19.255.010 and 42.56.590; adding new
3 sections to chapter 19.255 RCW; adding new sections to chapter 42.56
4 RCW; and providing an effective date.

5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

6 NEW SECTION. **Sec. 1.** A new section is added to chapter 19.255
7 RCW to read as follows:

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

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

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

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

21 (A) Social security number;

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

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

8 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (a) Written notice;

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

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

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

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

30 (iii) Notification to major statewide media.

31 ~~((9)) (5) A person or business that maintains its own~~
32 ~~notification procedures as part of an information security policy for~~
33 ~~the treatment of personal information and is otherwise consistent~~
34 ~~with the timing requirements of this section is in compliance with~~
35 ~~the notification requirements of this section if the person or~~
36 ~~business notifies subject persons in accordance with its policies in~~
37 ~~the event of a breach of security of the system.~~

38 ~~((10) A covered entity under the federal health insurance~~
39 ~~portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et~~
40 ~~seq., is deemed to have complied with the requirements of this~~

1 ~~section with respect to protected health information if it has~~
2 ~~complied with section 13402 of the federal health information~~
3 ~~technology for economic and clinical health act, Public Law 111-5 as~~
4 ~~it existed on July 24, 2015. Covered entities shall notify the~~
5 ~~attorney general pursuant to subsection (15) of this section in~~
6 ~~compliance with the timeliness of notification requirements of~~
7 ~~section 13402 of the federal health information technology for~~
8 ~~economic and clinical health act, Public Law 111-5 as it existed on~~
9 ~~July 24, 2015, notwithstanding the notification requirement in~~
10 ~~subsection (16) of this section.~~

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

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

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

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

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

1 ~~(14))~~ (6) Any person or business that is required to issue
2 notification pursuant to this section shall meet all of the following
3 requirements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

38 ~~((16))~~ (8) Notification to affected consumers ~~((and to the~~
39 ~~attorney general))~~ under this section must be made in the most
40 expedient time possible ~~((and)),~~ without unreasonable delay, and no

1 more than (~~forty-five~~) thirty calendar days after the breach was
2 discovered, unless the delay is at the request of law enforcement as
3 provided in subsection (3) of this section, or the delay is due to
4 any measures necessary to determine the scope of the breach and
5 restore the reasonable integrity of the data system.

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

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

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

33 (2) A financial institution under the authority of the office of
34 the comptroller of the currency, the federal deposit insurance
35 corporation, the national credit union administration, or the federal
36 reserve system is deemed to have complied with the requirements of
37 this chapter with respect to "sensitive customer information" as
38 defined in the interagency guidelines establishing information
39 security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part

1 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part
2 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they
3 existed on July 24, 2015, if the financial institution provides
4 notice to affected consumers pursuant to the interagency guidelines
5 and the notice complies with the customer notice provisions of the
6 interagency guidelines establishing information security standards
7 and the interagency guidance on response programs for unauthorized
8 access to customer information and customer notice under 12 C.F.R.
9 Part 364 as it existed on July 24, 2015. The entity shall notify the
10 attorney general pursuant to RCW 19.255.010 in addition to providing
11 notice to its primary federal regulator.

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

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

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

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

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

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

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

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

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

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

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

29 ~~((For purposes of this section, "breach of the security of
30 the system" means unauthorized acquisition of data that compromises
31 the security, confidentiality, or integrity of personal information
32 maintained by the agency. Good faith acquisition of personal
33 information by an employee or agent of the agency for the purposes of
34 the agency is not a breach of the security of the system when the
35 personal information is not used or subject to further unauthorized
36 disclosure.~~

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

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

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

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

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

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

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

18 (a) Written notice;

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

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

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

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

31 (iii) Notification to major statewide media.

32 ~~((9))~~ (5) An agency that maintains its own notification
33 procedures as part of an information security policy for the
34 treatment of personal information and is otherwise consistent with
35 the timing requirements of this section is in compliance with the
36 notification requirements of this section if it notifies subject
37 persons in accordance with its policies in the event of a breach of
38 security of the system.

39 ~~((10) A covered entity under the federal health insurance~~
40 ~~portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et~~

1 ~~seq., is deemed to have complied with the requirements of this~~
2 ~~section with respect to protected health information if it has~~
3 ~~complied with section 13402 of the federal health information~~
4 ~~technology for economic and clinical health act, Public Law 111-5 as~~
5 ~~it existed on July 24, 2015. Covered entities shall notify the~~
6 ~~attorney general pursuant to subsection (14) of this section in~~
7 ~~compliance with the timeliness of notification requirements of~~
8 ~~section 13402 of the federal health information technology for~~
9 ~~economic and clinical health act, Public Law 111-5 as it existed on~~
10 ~~July 24, 2015, notwithstanding the notification requirement in~~
11 ~~subsection (15) of this section.~~

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

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

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

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

21 ~~(13)) (6) Any agency that is required to issue notification~~
22 ~~pursuant to this section shall meet all of the following~~
23 ~~requirements:~~

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

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

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

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

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

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

35 ~~((14)) (7) Any agency that is required to issue a notification~~
36 ~~pursuant to this section to more than five hundred Washington~~
37 ~~residents as a result of a single breach shall((, by the time notice~~
38 ~~is provided to affected individuals, electronically submit a single~~
39 ~~sample copy of that security breach notification, excluding any~~
40 ~~personally identifiable information, to)) notify the attorney general~~

1 of the breach no more than thirty days after the breach was
2 discovered.

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

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

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

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

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

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

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

17 ((15)) (8) Notification to affected individuals ((and to the
18 attorney general)) must be made in the most expedient time possible
19 ((and), without unreasonable delay, and no more than ((forty-five))
20 thirty calendar days after the breach was discovered, unless the
21 delay is at the request of law enforcement as provided in subsection
22 (3) of this section, or the delay is due to any measures necessary to
23 determine the scope of the breach and restore the reasonable
24 integrity of the data system.

25 (9) For purposes of this section, "breach of the security of the
26 system" means unauthorized acquisition of data that compromises the
27 security, confidentiality, or integrity of personal information
28 maintained by the agency. Good faith acquisition of personal
29 information by an employee or agent of the agency for the purposes of
30 the agency is not a breach of the security of the system when the
31 personal information is not used or subject to further unauthorized
32 disclosure.

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

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

37 (A) Social security number;

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

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

5 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

38 A covered entity under the federal health insurance portability
39 and accountability act of 1996, Title 42 U.S.C. Sec. 1320d et seq.,

1 is deemed to have complied with the requirements of this chapter with
2 respect to protected health information if it has complied with
3 section 13402 of the federal health information technology for
4 economic and clinical health act, P.L. 111-5 as it existed on July
5 24, 2015. Covered entities shall notify the attorney general pursuant
6 to RCW 42.56.590(7) in compliance with the timeliness of notification
7 requirements of section 13402 of the federal health information
8 technology for economic and clinical health act, P.L. 111-5 as it
9 existed on July 24, 2015, notwithstanding the timeline in RCW
10 42.56.590(7).

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

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

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

17 (b) Any agency that violates, proposes to violate, or has
18 violated this chapter may be enjoined.

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

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

--- END ---