
SENATE BILL 5064

State of Washington

66th Legislature

2019 Regular Session

By Senators Nguyen, Darneille, Hasegawa, Wellman, Keiser, Zeiger, Kuderer, and Saldaña; by request of Attorney General

Prefiled 12/31/18. Read first time 01/14/19. Referred to Committee on Environment, Energy & Technology.

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; and adding new sections to chapter
4 42.56 RCW.

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 resources;
- 8 (D) Full date of birth;
- 9 (E) Digital signature;
- 10 (F) Student, military, or passport identification number;
- 11 (G) Health insurance policy number or health insurance
12 identification number;
- 13 (H) Any information about a consumer's medical history or mental
14 or physical condition or about a health care professional's medical
15 diagnosis or treatment of the consumer; or
- 16 (I) Biometric data generated by automatic measurements of an
17 individual's biological characteristics, such as a fingerprint,
18 voiceprint, eye retinas, irises, or other unique biological patterns
19 or characteristics that is used to identify a specific individual;
- 20 (ii) Username or email address, in combination with a password or
21 security questions and answers, that would permit access to an online
22 account; and
- 23 (iii) Any of the data elements or any combination of the data
24 elements described in (a)(i) of this subsection without the
25 consumer's first name or first initial and last name if:
- 26 (A) Encryption, redaction, or other methods have not rendered the
27 data element or combination of data elements unusable; and
- 28 (B) The data element or combination of data elements would enable
29 a person to commit identity theft against a consumer.
- 30 (b) Personal information does not include publicly available
31 information that is lawfully made available to the general public
32 from federal, state, or local government records.
- 33 (3) "Secured" means encrypted in a manner that meets or exceeds
34 the national institute of standards and technology standard or is
35 otherwise modified so that the personal information is rendered
36 unreadable, unusable, or undecipherable by an unauthorized person.

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

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

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

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

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

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

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

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

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.~~

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 subsections (9)~~
16 ~~and (10) of this section,)) "Notice" may be provided by one of the~~
17 ~~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 person or business demonstrates
23 that the cost of providing notice would exceed two hundred fifty
24 thousand dollars, or that the affected class of subject persons to be
25 notified exceeds five hundred thousand, or the person or business
26 does not have sufficient contact information. Substitute notice shall
27 consist of all of the following:

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

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

32 (iii) Notification to major statewide media.

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

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

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

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

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

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

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

4 ~~(14))~~ (6) Any person or business that is required to issue
5 notification pursuant to this section shall meet all of the following
6 requirements:

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

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

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

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

14 (iii) A timeline of when the breach began, when it was
15 discovered, the containment date, and all windows of intrusion; and

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

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

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

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

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

33 (iii) A timeline of when the breach began, when it was
34 discovered, the containment date, and all windows of intrusion;

35 (iv) A summary of containment efforts; and

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

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

1 ~~((16))~~ (8) Notification to affected consumers ~~((and to the~~
2 ~~attorney general))~~ under this section must be made in the most
3 expedient time possible and without unreasonable delay, no more than
4 ~~((forty-five))~~ thirty calendar days after the breach was discovered,
5 unless at the request of law enforcement as provided in subsection
6 (3) of this section, or due to any measures necessary to determine
7 the scope of the breach and restore the reasonable integrity of the
8 data system.

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

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

24 (1) A covered entity under the federal health insurance
25 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
26 seq., is deemed to have complied with the requirements of this
27 section with respect to protected health information if it has
28 complied with section 13402 of the federal health information
29 technology for economic and clinical health act, P.L. 111-5 as it
30 existed on July 24, 2015. Covered entities shall notify the attorney
31 general pursuant to RCW 19.255.010 in compliance with the timeliness
32 of notification requirements of section 13402 of the federal health
33 information technology for economic and clinical health act, P.L.
34 111-5 as it existed on July 24, 2015, notwithstanding the
35 notification requirement in RCW 19.255.010(8).

36 (2) A financial institution under the authority of the office of
37 the comptroller of the currency, the federal deposit insurance
38 corporation, the national credit union administration, or the federal
39 reserve system is deemed to have complied with the requirements of

1 this section with respect to "sensitive customer information" as
2 defined in the interagency guidelines establishing information
3 security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part
4 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part
5 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they
6 existed on July 24, 2015, if the financial institution provides
7 notice to affected consumers pursuant to the interagency guidelines
8 and the notice complies with the customer notice provisions of the
9 interagency guidelines establishing information security standards
10 and the interagency guidance on response programs for unauthorized
11 access to customer information and customer notice under 12 C.F.R.
12 Part 364 as it existed on July 24, 2015. The entity shall notify the
13 attorney general pursuant to RCW 19.255.010 in addition to providing
14 notice to its primary federal regulator.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 ~~(8) For purposes of this section and except under subsections (9)~~
20 ~~and (10) of this section,)~~ Notice may be provided by one of the
21 following methods:

22 (a) Written notice;

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

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

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

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

35 (iii) Notification to major statewide media.

36 ~~((9))~~ (5) An agency that maintains its own notification
37 procedures as part of an information security policy for the
38 treatment of personal information and is otherwise consistent with
39 the timing requirements of this section is in compliance with the
40 notification requirements of this section if it notifies subject

1 persons in accordance with its policies in the event of a breach of
2 security of the system.

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

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

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

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

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

25 ~~(13))~~ (6) Any agency that is required to issue notification
26 pursuant to this section shall meet all of the following
27 requirements:

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

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

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

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 timeline of when the breach began, when it was
36 discovered, the containment date, and all windows of intrusion; and

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

39 ~~((14))~~ (7) Any agency that is required to issue a notification
40 pursuant to this section ~~((to more than five hundred Washington~~

1 residents as a result of a single breach shall, by the time notice is
2 provided to affected individuals, electronically submit a single
3 sample copy of that security breach notification, excluding any
4 personally identifiable information, to)) shall notify the attorney
5 general of the breach no more than fourteen days after the breach was
6 discovered.

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

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

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

13 (iii) A timeline of when the breach began, when it was
14 discovered, the containment date, and all windows of intrusion;

15 (iv) A summary of containment efforts; and

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

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

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

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

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

38 (i) An individual's first name or first initial and last name in
39 combination 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;

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

8 (D) Full date of birth;

9 (E) Digital signature;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 (2)(a) Any consumer injured by a violation of this section may
18 institute a civil action to recover damages.

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

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

--- END ---