

CERTIFICATION OF ENROLLMENT

SUBSTITUTE HOUSE BILL 1071

Chapter 241, Laws of 2019

66th Legislature
2019 Regular Session

NOTICE OF PERSONAL INFORMATION DATA BREACHES--VARIOUS PROVISIONS

EFFECTIVE DATE: March 1, 2020

Passed by the House April 22, 2019
Yeas 96 Nays 0

FRANK CHOPP

Speaker of the House of Representatives

Passed by the Senate April 15, 2019
Yeas 46 Nays 0

CYRUS HABIB

President of the Senate

Approved May 7, 2019 9:39 AM

JAY INSLEE

Governor of the State of Washington

CERTIFICATE

I, Bernard Dean, Chief Clerk of the House of Representatives of the State of Washington, do hereby certify that the attached is **SUBSTITUTE HOUSE BILL 1071** as passed by the House of Representatives and the Senate on the dates hereon set forth.

BERNARD DEAN

Chief Clerk

FILED

May 13, 2019

**Secretary of State
State of Washington**

SUBSTITUTE HOUSE BILL 1071

AS AMENDED BY THE SENATE

Passed Legislature - 2019 Regular Session

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 ~~((u)) notice((u)) 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; ~~((e))~~

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; or

31 (d)(i) If the breach of the security of the system involves
32 personal information including a user name or password, notice may be
33 provided electronically or by email. The notice must comply with
34 subsections (6), (7), and (8) of this section and must inform the
35 person whose personal information has been breached to promptly
36 change his or her password and security question or answer, as
37 applicable, or to take other appropriate steps to protect the online
38 account with the person or business and all other online accounts for
39 which the person whose personal information has been breached uses

1 the same user name or email address and password or security question
2 or answer;

3 (ii) However, when the breach of the security of the system
4 involves login credentials of an email account furnished by the
5 person or business, the person or business may not provide the
6 notification to that email address, but must provide notice using
7 another method described in this subsection (4). The notice must
8 comply with subsections (6), (7), and (8) of this section and must
9 inform the person whose personal information has been breached to
10 promptly change his or her password and security question or answer,
11 as applicable, or to take other appropriate steps to protect the
12 online account with the person or business and all other online
13 accounts for which the person whose personal information has been
14 breached uses the same user name or email address and password or
15 security question or answer.

16 ~~((9))~~ (5) A person or business that maintains its own
17 notification procedures as part of an information security policy for
18 the treatment of personal information and is otherwise consistent
19 with the timing requirements of this section is in compliance with
20 the notification requirements of this section if the person or
21 business notifies subject persons in accordance with its policies in
22 the event of a breach of security of the system.

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

36 ~~((11))~~ 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
40 this section with respect to "sensitive customer information" as

1 ~~defined in the interagency guidelines establishing information~~
2 ~~security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part~~
3 ~~208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part~~
4 ~~364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they~~
5 ~~existed on July 24, 2015, if the financial institution provides~~
6 ~~notice to affected consumers pursuant to the interagency guidelines~~
7 ~~and the notice complies with the customer notice provisions of the~~
8 ~~interagency guidelines establishing information security~~
9 ~~standards and the interagency guidance on response programs for~~
10 ~~unauthorized access to customer information and customer notice under~~
11 ~~12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall~~
12 ~~notify the attorney general pursuant to subsection (15) of this~~
13 ~~section in addition to providing notice to its primary federal~~
14 ~~regulator.~~

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

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

19 ~~(b) Any person or business that violates, proposes to violate, or~~
20 ~~has 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.~~

24 ~~(14)) (6) Any person or business that is required to issue~~
25 ~~notification pursuant to this section shall meet all of the following~~
26 ~~requirements:~~

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

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

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

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

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

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

38 ~~((15)) (7) Any person or business that is required to issue a~~
39 ~~notification pursuant to this section to more than five hundred~~
40 ~~Washington residents as a result of a single breach shall ~~((, by the~~~~

1 ~~time notice is provided to affected consumers, electronically submit~~
2 ~~a single sample copy of that security breach notification, excluding~~
3 ~~any personally identifiable information, to the attorney general))~~
4 notify the attorney general of the breach no more than thirty days
5 after the breach was discovered.

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

9 (i) The number of Washington consumers 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 time frame of exposure, if known, including the date of
14 the breach and the date of the discovery of the breach;

15 (iv) A summary of steps taken to contain the breach; 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 must be updated if any of
19 the information identified in (a) of this subsection is unknown at
20 the time notice is due.

21 ~~((16))~~ (8) Notification to affected consumers ((and to the
22 attorney general)) under this section must be made in the most
23 expedient time possible ((and)), without unreasonable delay, and no
24 more than ((forty-five)) thirty calendar days after the breach was
25 discovered, unless the delay is at the request of law enforcement as
26 provided in subsection (3) of this section, or the delay is due to
27 any measures necessary to determine the scope of the breach and
28 restore the reasonable integrity of the data system.

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

1 ~~protection act, chapter 19.86 RCW. An action to enforce this section~~
2 ~~may not be brought under RCW 19.86.090.)~~)

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

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

17 (2) A financial institution under the authority of the office of
18 the comptroller of the currency, the federal deposit insurance
19 corporation, the national credit union administration, or the federal
20 reserve system is deemed to have complied with the requirements of
21 this chapter with respect to "sensitive customer information" as
22 defined in the interagency guidelines establishing information
23 security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part
24 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part
25 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they
26 existed on July 24, 2015, if the financial institution provides
27 notice to affected consumers pursuant to the interagency guidelines
28 and the notice complies with the customer notice provisions of the
29 interagency guidelines establishing information security standards
30 and the interagency guidance on response programs for unauthorized
31 access to customer information and customer notice under 12 C.F.R.
32 Part 364 as it existed on July 24, 2015. The entity shall notify the
33 attorney general pursuant to RCW 19.255.010 in addition to providing
34 notice to its primary federal regulator.

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

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

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

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

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

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

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

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

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

38 (2) Any agency that maintains or possesses data that may
39 include ~~((s))~~ personal information that the agency does not own or

1 license shall notify the owner or licensee of the information of any
2 breach of the security of the data immediately following discovery,
3 if the personal information was, or is reasonably believed to have
4 been, acquired by an unauthorized person.

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

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

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

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

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

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

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

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

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

- 1 (a) Written notice;
- 2 (b) Electronic notice, if the notice provided is consistent with
3 the provisions regarding electronic records and signatures set forth
4 in 15 U.S.C. Sec. 7001; or
- 5 (c) Substitute notice, if the agency demonstrates that the cost
6 of providing notice would exceed two hundred fifty thousand dollars,
7 or that the affected class of subject persons to be notified exceeds
8 five hundred thousand, or the agency does not have sufficient contact
9 information. Substitute notice shall consist of all of the following:
- 10 (i) Email notice when the agency has an email address for the
11 subject persons;
- 12 (ii) Conspicuous posting of the notice on the agency's web site
13 page, if the agency maintains one; and
- 14 (iii) Notification to major statewide media.
- 15 ~~((9))~~ (5) An agency that maintains its own notification
16 procedures as part of an information security policy for the
17 treatment of personal information and is otherwise consistent with
18 the timing requirements of this section is in compliance with the
19 notification requirements of this section if it notifies subject
20 persons in accordance with its policies in the event of a breach of
21 security of the system.
- 22 ~~((10) A covered entity under the federal health insurance
23 portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et
24 seq., is deemed to have complied with the requirements of this
25 section with respect to protected health information if it has
26 complied with section 13402 of the federal health information
27 technology for economic and clinical health act, Public Law 111-5 as
28 it existed on July 24, 2015. Covered entities shall notify the
29 attorney general pursuant to subsection (14) of this section in
30 compliance with the timeliness of notification requirements of
31 section 13402 of the federal health information technology for
32 economic and clinical health act, Public Law 111-5 as it existed on
33 July 24, 2015, notwithstanding the notification requirement in
34 subsection (15) of this section.~~
- 35 ~~(11) Any waiver of the provisions of this section is contrary to
36 public policy, and is void and unenforceable.~~
- 37 ~~(12)(a) Any individual injured by a violation of this section may
38 institute a civil action to recover damages.~~
- 39 ~~(b) Any agency that violates, proposes to violate, or has
40 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 ~~(13))~~ (6) Any agency that is required to issue notification
5 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 agency
11 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;

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

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

18 ~~((14))~~ (7) Any agency that is required to issue a notification
19 pursuant to this section to more than five hundred Washington
20 residents as a result of a single breach shall ~~(, by the time notice~~
21 ~~is provided to affected individuals, electronically submit a single~~
22 ~~sample copy of that security breach notification, excluding any~~
23 ~~personally identifiable information, to)~~ notify the attorney general
24 of the breach no more than thirty days after the breach was
25 discovered.

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

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

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

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

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

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

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

1 ~~((15))~~ (8) Notification to affected individuals ~~((and to the~~
2 ~~attorney general))~~ must be made in the most expedient time possible
3 ~~((and)),~~ without unreasonable delay, and no more than ~~((forty-five))~~
4 thirty calendar days after the breach was discovered, unless the
5 delay is at the request of law enforcement as provided in subsection
6 (3) of this section, or the delay is due to any measures necessary to
7 determine the scope of the breach and restore the reasonable
8 integrity of the data system. An agency may delay notification to the
9 consumer for up to an additional fourteen days to allow for
10 notification to be translated into the primary language of the
11 affected consumers.

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

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

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

24 (A) Social security number;

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

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

31 (D) Full date of birth;

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

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

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

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

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

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

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

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

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

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

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

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

25 A covered entity under the federal health insurance portability
26 and accountability act of 1996, Title 42 U.S.C. Sec. 1320d et seq.,
27 is deemed to have complied with the requirements of this chapter with
28 respect to protected health information if it has complied with
29 section 13402 of the federal health information technology for
30 economic and clinical health act, P.L. 111-5 as it existed on July
31 24, 2015. Covered entities shall notify the attorney general pursuant
32 to RCW 42.56.590(7) in compliance with the timeliness of notification
33 requirements of section 13402 of the federal health information
34 technology for economic and clinical health act, P.L. 111-5 as it
35 existed on July 24, 2015, notwithstanding the timeline in RCW
36 42.56.590(7).

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

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

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

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

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

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

Passed by the House April 22, 2019.

Passed by the Senate April 15, 2019.

Approved by the Governor May 7, 2019.

Filed in Office of Secretary of State May 13, 2019.

--- END ---