WAC 284-04-625 Security breach notification requirements. (1) The commissioner defines failure to provide notice of security breaches in compliance with this section as an unfair practice for the following reasons:

(a) Many licensees fail or periodically fail to protect personal information and protected health information as defined in subsection (2)(a) and (b) of this section, resulting in security breaches affecting their customers or consumers.

(b) When a customer or consumer whose personal or protected health information has been breached seeks assistance from the commissioner, information about security breaches and what actions a licensee is taking to protect customers or consumers must be available to the commissioner.

(2) All licensees must notify the insurance commissioner about the number of customers or consumers potentially affected and what actions are being taken in writing within two business days after determining notification must be sent to consumers or customers in compliance with RCW 19.255.010 and 45 C.F.R. 164 pertaining to:

(a) A breach of personal information as defined in RCW 19.255.010 (4) and (5) that seems reasonably likely to subject customers to a risk of criminal activity; or

(b) A breach of unsecured protected health information as defined in 45 C.F.R. 164.402 which compromises the security or privacy of the protected information for licensees subject to 45 C.F.R. 164.

(3) For breaches of protected health information, licensees subject to 45 C.F.R. 164 must comply with the regulations (45 C.F.R. 164.400 through 164.410) adopted by the U.S. Department of Health and Human Services (HHS) governing these requirements including:

(a) Notification requirements for a security breach as defined by 45 C.F.R. 164.402, meaning an acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule which compromises the security or privacy of the protected health information.

(b) Notifying individuals, and other entities described in 45 C.F.R. 164.404 through 164.410.

(c) Notifying affected entities without unreasonable delay and in no case later than sixty calendar days following the discovery of the breach.

(d) Notifying documents that contain:

(i) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;

(ii) A description of the types of unsecured protected health information involved in the breach;

(iii) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(iv) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches; and

(v) Contact information for individuals to ask questions or learn additional information.

[Statutory Authority: RCW 48.02.060, 48.30.010, 48.43.505, Gramm-Leach Bliley Act, Pub. L. 102-106, Sec. 501(b), Sec. 505 (B)(2), and 45 C.F.R. Parts 160 and 164 (2013). WSR 13-11-004 (Matter No. R 2012-14), § 284-04-625, filed 5/1/13, effective 6/1/13.]