304.3-766 Compliance requirements.

(1) A licensee shall be deemed in compliance with KRS 304.3-750 to 304.3-768 if the licensee:

(a) 1. Is subject to, governed by, and compliant with the privacy, security, and breach notifications rules issued by the United States Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, as amended, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, as amended;

2. Maintains nonpublic information in the same manner as protected health information; and

3. Submits to the commissioner:

a. An annual written statement certifying its compliance with the applicable provisions referenced under subparagraph 1. of this paragraph; and

b. A copy of any individual breach notification required under 45 C.F.R. sec. 164.404, as amended, at the same time as all affected individuals; or

(b) 1. Is a financial institution, as defined in KRS 304.9-135, that is subject to, governed by, and compliant with the privacy, security, and breach notification standards issued under Section 501 of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. sec. 6801, as amended; and

2. Submits to the commissioner:

a. An annual written statement certifying its compliance with the applicable provisions referenced under subparagraph 1. of this paragraph; and

b. A copy of any breach notification at the same time and in the same manner as notifications provided to the financial institution's federal regulatory authorities.

(2) Nothing in subsection (1)(a) of this section shall be construed to restrict the commissioner's authority to examine and investigate the affairs of any licensee under KRS 304.3-762 to verify the licensee's annual certification under this section.

Effective: January 1, 2023

History: Created 2022 Ky. Acts ch. 149, sec. 9, effective January 1, 2023.