



STATE OF CONNECTICUT

INSURANCE DEPARTMENT

BULLETIN MC-23
June 13, 2017

TO: ALL HEALTH INSURERS, HEALTHCARE CENTERS, PHARMACY BENEFITS MANAGERS, THIRD PARTY ADMINISTRATORS, UTILIZATION REVIEW COMPANIES AND ANY OTHER ENTITY LICENSED TO DO A HEALTH INSURANCE BUSINESS IN CONNECTICUT

RE: CERTIFICATION AND NOTICE REQUIREMENTS CONCERNING SECURITY PROGRAM TO SAFEGUARD PERSONAL INFORMATION.

Connecticut General Statutes, Section 38a-999b, requires certain entities engaged in a health insurance business in Connecticut, to implement by October 1, 2017, and maintain a comprehensive information security program ("ISP") to safeguard the personal information it compiles or maintains on insureds and enrollees. C.G.S. Section 38a-999b(b) specifies program requirements and requires the program to be updated as necessary and practicable, but at least annually. Specifically, such requirements are applicable to (1) health insurer, HMO, and other entities licensed to write health insurance in Connecticut; (2) pharmacy benefits managers; (3) third-party administrators that administer health benefits; and (4) utilization review companies ("ISP Entities").

Beginning October 1, 2017, each ISP Entity must annually certify to the Insurance Commissioner, under penalty of perjury, that it maintains a program in compliance with C.G.S. Section 38a-999b. Pursuant to C.G.S. Section 38a-999b(d), the Insurance Commissioner or Attorney General may request a copy of such program to determine compliance. If either one determines the ISP is noncompliant, the ISP Entity must amend it to bring it into compliance to the Commissioner's or Attorney General's satisfaction.

C.G.S. Section 38a-999b(e) requires each ISP Entity that discovers an actual or suspected security breach to (1) notify each impacted state resident without unreasonable delay, but at least within 90 days of discovering the breach, unless federal law requires a shorter time; (2) offer impacted residents at least one year of free identity theft prevention and mitigation services; and (3) inform the residents how to (a) enroll in the services and (b) place a freeze on his or her credit file. Any ISP Entity that fails to comply with these requirements commits an unfair trade practice.

C.G.S. Section 38a-999b(f) requires the Insurance Commissioner to enforce the Act's provisions regarding an ISP Entity's comprehensive information security program.

Each ISP Entity is required to certify to the Insurance Commissioner, by October 1, 2017 and annually thereafter, that it maintains a comprehensive information security program that complies with the requirements of C.G.S. Section 38a-999b(b). Such certification shall be in the form as shown in the attachment to this bulletin signed by an officer of such entity and including all the information required under Section 38a-999b(b) of the Connecticut General Statutes. The certification will be considered incomplete if not executed by an authorized officer and must be submitted to the Insurance Department's Market Conduct Unit at cid.mc@ct.gov.

Katharine L. Wade
Insurance Commissioner



STATE OF CONNECTICUT

INSURANCE DEPARTMENT

ANNUAL CERTIFICATION INFORMATION SECURITY PROGRAM COMPLIANCE

Filed under C.G.S. Section 38a-999b(c)

The undersigned hereby certifies, on behalf of the Company named below, as follows:

1. The undersigned is the Chief Information Officer, Chief Compliance Officer or the Chief Privacy Officer (or holds an equivalent senior position, as indicated under his/her signature below) of the following company*:

Name: _____ (herein referred to as “the Company”)

Principal Office Address: _____

**Note: The certificate may name a group of affiliated companies, in which case the person signing will be deemed to be certifying as to the ISP of each affiliate within the named group.*

2. The Company currently maintains a comprehensive information security program (“ISP”) that complies with all requirements of subsection (b) of Section 38a-999b of the Connecticut General Statutes.
3. The name and contact information of the person designated by the Company to oversee the ISP and its maintenance under Section 38a-999(b)(2)(D) is as follows:

Designated ISP Employee Name: _____

Direct Phone: _____ Email: _____

IN WITNESS WHEREOF, and under penalty of perjury pursuant to C.G.S. Sec. 38a-999b(c), I have executed this Certificate on the date shown below.

Date: _____, 20__

Signed: _____

Printed Name: _____

Title: _____

Note: A facsimile of this Certificate must be filed annually by October 1st of each year by means of a .pdf file attached to an email sent to, cid.mc@ct.gov