

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2003

S

1

SENATE BILL 966

Short Title: Insurance Personal Info. Safeguards.

(Public)

Sponsors: Senators Dalton; and Dorsett.

Referred to: Commerce.

April 3, 2003

1 A BILL TO BE ENTITLED
2 AN ACT TO REQUIRE INSURERS TO IMPLEMENT SAFEGUARDS FOR THE
3 PROTECTION OF PERSONAL INFORMATION, PURSUANT TO THE
4 PROVISIONS OF THE GRAMM-LEACH-BLILEY ACT.

5 The General Assembly of North Carolina enacts:

6 **SECTION 1.** The heading for Article 39 of Chapter 58 of the General
7 Statutes reads as rewritten:

8 "Article 39.

9 ~~Insurance Information and Privacy Protection Act.~~

10 Consumer Information Privacy."

11 **SECTION 2.** Article 39 of Chapter 58 of the General Statutes is amended
12 by:

13 (1) Designating G.S. 58-39-1 through G.S. 58-39-76 as:

14 "Part 1. Insurance Information and Privacy Protection."

15 (2) Designating G.S. 58-39-80 through G.S. 58-39-125 as:

16 "Part 2. Enforcement, Sanctions, Remedies, and Rights." and

17 (3) Recodifying G.S. 58-39-70 as G.S. 58-39-125.

18 **SECTION 3.** G.S. 58-39-1 reads as rewritten:

19 "**§ 58-39-1. Short title.**titles.

20 This Article may be cited as the Consumer Information Privacy Act. Part 1 of this
21 Article may be cited as the Insurance Information and Privacy Protection Act. Part 3 of
22 this Article may be cited as the Personal Information Safeguards Act."

23 **SECTION 4.** G.S. 58-39-5 reads as rewritten:

24 "**§ 58-39-5. Purpose.**

25 The purpose of this Article is to establish standards for the collection, use, and
26 disclosure of information gathered in connection with insurance transactions by
27 insurance institutions, agents, or insurance-support organizations; to maintain a balance
28 between the need for information by those conducting the business of insurance and the
29 public's need for fairness in insurance information practices, including the need to

1 minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to
2 ascertain what information is being or has been collected about them in connection with
3 insurance transactions and to have access to such information for the purpose of
4 verifying or disputing its accuracy; to limit the disclosure of information collected in
5 connection with insurance transactions; and to enable insurance applicants and
6 policyholders to obtain the reasons for any adverse underwriting decision. The purpose
7 of this Article is also to establish standards for developing and implementing
8 administrative, technical, and physical safeguards to protect the security, confidentiality,
9 and integrity of an individual's personal information requiring protection under Parts 1
10 and 2 of this Article, as required by sections 501, 505, and 507 of the federal Gramm-
11 Leach-Bliley Act (Public Law 106-102), codified as 15 U.S.C. §§6801, 6805(b), and
12 6807. The purpose of this Article is also to provide privacy protection consistent with
13 federal regulations governing the privacy of medical records when this Article is
14 consistent with those federal regulations. In those instances in which this Article and the
15 federal privacy regulations are inconsistent and this Article provides privacy protection
16 beyond that offered by the federal regulations, the purpose of this Article is to provide
17 that additional privacy protection."

18 **SECTION 5.** Article 39 of Chapter 58 of the General Statutes is amended by
19 adding a new Part to read:

20 "Part 3. Personal Information Safeguards.

21 **"§ 58-39-130. Application.**

22 The safeguards established under this Part apply to all personal information of
23 individuals requiring protection under Parts 1 and 2 of this Article.

24 **"§ 58-39-135. Definitions.**

25 As used in this Part, in addition to the definitions in G.S. 58-39-15:

- 26 (1) 'Information systems' means the electronic or physical methods used to
27 access, collect, store, use, transmit, protect, or dispose of personal
28 information.
- 29 (2) 'Licensee' means any producer, as defined in G.S. 58-33-10(7), insurer,
30 MEWA, HMO, or service corporation governed by this Chapter.
31 'Licensee' does not mean:
- 32 a. An insurance-support organization.
- 33 b. A licensee who is a natural person operating within the scope of
34 the licensee's employment by or affiliation with an insurer or
35 producer.
- 36 c. A surplus lines insurer or licensee under Article 21 of this
37 Chapter.
- 38 (3) 'Service provider' means a person that maintains, processes, or
39 otherwise is permitted access to personal information through its
40 provision of services directly to the licensee and includes an insurance
41 support organization.

42 **"§ 58-39-140. Information security program.**

43 Each licensee shall implement a comprehensive written information security
44 program that includes administrative, technical, and physical safeguards for the

1 protection of personal information. The administrative, technical, and physical
2 safeguards included in the information security program shall be appropriate to the size
3 and complexity of the licensee and the nature and scope of its activities.

4 **"§ 58-39-145. Objectives of information security program.**

5 A licensee's information security program shall be designed to:

- 6 (1) Ensure the security and confidentiality of personal information;
- 7 (2) Protect against any anticipated threats or hazards to the security or
8 integrity of the information; and
- 9 (3) Protect against unauthorized access to or use of the information that
10 could result in substantial harm or inconvenience to any individual or
11 in a violation of Part 1 of this Article.

12 **"§ 58-39-150. Examples of development and implementation methods.**

13 The actions and procedures described in G.S. 58-39-155 through G.S. 58-39-170 are
14 examples of methods of implementation of the requirements of G.S. 58-39-140 and G.S.
15 58-39-145. These examples are non-exclusive illustrations of actions and procedures
16 that licensees may follow to implement G.S. 58-39-140 and G.S. 58-39-145.

17 **"§ 58-39-155. Risk assessment.**

18 The licensee identifies reasonably foreseeable internal or external threats that could
19 result in unauthorized disclosure, misuse, alteration, or destruction of personal
20 information or a licensee's information systems, and assesses the likelihood and
21 potential damage of these threats, taking into consideration the sensitivity of the
22 personal information involved. The licensee also assesses the sufficiency of policies,
23 procedures, information systems, and other safeguards in place to control risks.

24 **"§ 58-39-160. Risk management and control.**

25 The licensee:

- 26 (1) Designs its information security program to control the identified risks,
27 commensurate with the sensitivity of the information, as well as the
28 complexity and scope of the licensee's activities;
- 29 (2) Trains staff, as appropriate, to implement the licensee's information
30 security program; and
- 31 (3) Regularly tests or otherwise regularly monitors the key controls,
32 systems, and procedures of the information security program. The
33 frequency and nature of these tests or other monitoring practices are
34 determined by the licensee's risk assessment.

35 **"§ 58-39-165. Service provider arrangement oversight.**

36 The licensee:

- 37 (1) Exercises appropriate due diligence in selecting its service providers.
- 38 (2) Requires its service providers to implement appropriate measures
39 designed to meet the objectives of this Part and, where indicated by the
40 licensee's risk assessment, takes appropriate steps to confirm that its
41 service providers have satisfied these obligations.

42 **"§ 58-39-170. Program adjustment.**

43 The licensee monitors, evaluates, and adjusts, as appropriate, the information
44 security program in light of any relevant changes in technology, the sensitivity of an

1 individual's personal information, internal or external threats to information, and the
2 licensee's own changing business arrangements, such as mergers and acquisitions,
3 alliances and joint ventures, outsourcing arrangements, and changes to personal
4 information systems.

5 **"§ 58-39-175. Violation.**

6 A violation of G.S. 58-39-140 or G.S. 58-39-145 subjects the violator to Part 2 of
7 this Article.

8 **"§ 58-39-180. Effective date.**

9 Each licensee shall establish an information security program, including appropriate
10 policies and systems, under this Part by January 1, 2004."

11 **SECTION 6.** This act is effective when it becomes law.