DEPARTMENT OF LABOR AND ECONOMIC GROWTH

OFFICE OF FINANCIAL AND INSURANCE SERVICES

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

(By the authority conferred on the Office of Financial and Insurance Services by Section 547 of 1956 PA 215, MCL 500.547, by Section 210 of 1956 PA 218, MCL 500.210, and E.R.O. No. 2003-1, and pursuant to 15 U.S.C. 6801, 6805(a)(6), 6805(b), 6805(c))

R 500.551 Authority.

Rule 1. (a) These rules establish standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807, Chapter 5 of the Insurance Code, MCL 500.501 to 500.547, with penalties for violation specified in Chapter 20 of the Insurance Code, MCL 500.2001 to 500.2050.

(b) Section 501(a) of the Gramm-Leach-Bliley Act provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) of the Gramm-Leach-Bliley Act requires the state insurance regulatory authorities to establish appropriate standards relating to all of the following administrative, technical, and physical safeguards:

(i) To ensure the security and confidentiality of customer records and information.

(ii) To protect against any anticipated threats or hazards to the security or integrity of such records.

(iii) To protect against unauthorized access to or use of records or information that may result in substantial harm or inconvenience to a customer.

(c) Section 505(b)(2) calls on state insurance regulatory authorities to implement by rule the standards prescribed under Section 501(b) with respect to persons engaged in providing insurance; and the Governor signed 2001 PA 24 on June 18, 2001, creating Chapter 5 of the Insurance Code, titled "Privacy of Financial Information."

(d) Section 507 provides, among other things, that a state may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. MCL 500.501(3) provides that Chapter 5 of the Insurance Code - applicable to financial information - does not modify, limit, or supersede statute or rules governing the confidentiality or privacy of individually identifiable health or medical information under state law. To release such private or privileged health or medical information in Michigan generally requires the informed, written consent of the patient or his or her authorized representative. Nothing in these rules shall be construed to diminish state law, recent federal HIPAA standards (45 CFR Parts 160 and 164) that govern the privacy and security of protected health and medical information, or fair credit reporting act protections for medical information (15 U.S.C. 1681 et seq.). The safeguards established pursuant to these rules apply only to nonpublic personal financial information and do not diminish the duty of any licensee to comply with other more stringent state or federal laws affecting other types of customer information in the licensee's possession. For example, licensees are notified that MCL 750.410 (2) establishes criminal penalties for any person, firm, or corporation that buys, sells, furnishes, or receives "for any consideration" the identity of a patient or any information concerning treatment unless otherwise authorized by law, administrative rule, or valid legal process.

History: 2004 AACS.

R 500.552 Definitions.

Rule 2. As used in these rules:

(a) "Customer" means a customer of the licensee as the term customer is defined in MCL 500.503(h).

(b) "Customer information" means nonpublic personal financial information as defined in MCL 500.503(n) and (p) about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

(c) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

(d) "Licensee" means a licensee, as that term is defined in MCL 500.503(l), including third-party administrators under MCL 550.920.

(e) "Service provider" means a person that maintains, processes, or otherwise may access customer information through its provision of services directly to the licensee.

History: 2004 AACS.

R 500.553 Information security program.

Rule 3. Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

History: 2004 AACS.

R 500.554 Objectives of information security program.

Rule 4. A licensee's information security program shall be designed to do all of the following:

(a) Ensure the security and confidentiality of customer information.

(b) Protect against any anticipated threats or hazards to the security or integrity of the information.

(c) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

History: 2004 AACS.

R 500.555 Examples of methods of development and implementation.

Rule 5. (1) The actions and procedures described in R 500.556 to R 500.559 are examples of methods of implementation of the requirements of R 500.553 and R500.554. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement R 500.553 and R 500.554.

(2) A licensee who performs all actions and procedures of implementation specified in R 500.556 through R 500.559 shall be considered in compliance with R 500.553 and R 500.554.

History: 2004 AACS.

R 500.556 Assess risk; example.

Rule 6. To assess risk, a licensee may do all of the following:

(a) Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

(b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

(c) Assess the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

History: 2004 AACS.

R 500.557 Manage and control risk; example.

Rule 7. To manage and control risk, a licensee may do all of the following:

(a) Design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities.

(b) Train staff, as appropriate, to implement the licensee's information security program.

(c) Regularly test or otherwise regularly monitor the key controls, systems, and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

History: 2004 AACS.

R 500.558 Oversee service provider arrangements; example.

Rule 8. To oversee service provider arrangements, a licensee may do both of the following:

(a) Exercise appropriate due diligence in selecting its service providers.

(b) Require its service providers to implement appropriate measures designed to meet the objectives of these rules, and, where indicated by the licensee's risk assessment, take appropriate steps to confirm that its service providers have satisfied these obligations.

History: 2004 AACS.

R 500.559 Adjust program; example.

Rule 9. To adjust its program, a licensee monitors, evaluates, and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances, and joint ventures, outsourcing arrangements and changes to customer information systems.

History: 2004 AACS.

R 500.560 Violations.

Rule 10. (a) As provided in MCL 500.2013, a violation of any requirement of this regulation is an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this state.

(b) If a licensee complies with all requirements of the federal health insurance portability and accountability (HIPAA) privacy rule, including security standards and any more stringent laws, 45 CFR parts 160 and 164, for all customer information in the licensee's possession - financial, health, and medical - such compliance shall also constitute compliance with chapter 5 of the insurance code, MCL 500.501 to 500.547, and these safeguarding rules.

History: 2004 AACS.