

**The following is the Operations/Management section of Chapter 16 for the Advisory Organization Examination Protocol (C) Working Group to review**

**The current proposal is that all standards would apply to advisory organizations except standards 3 and 5. For Standard 8, substitute “line of business that are being written” with “regulated products and services that are being provided”**

## Chapter 16—General Examination Standards

The examination of the insurance operations of a regulated entity may involve reviewing one or more of the following business areas:

- A. Operations/Management
- B. Complaint Handling
- C. Marketing and Sales
- D. Producer Licensing
- E. Policyholder Service
- F. Underwriting and Rating
- G. Claims

When conducting an exam that reviews these areas, there are essential tests that should be completed. The tests are applied to determine if the regulated entity is meeting standards. Some standards may not be applicable to all jurisdictions. The standards may suggest other areas of review that may be appropriate on an individual state basis.

When an examination involves a depository institution or their affiliates, the bank may also be regulated by federal agencies, such as the Office of the Comptroller of the Currency, the Federal Reserve Board, the Office of Thrift Supervision or the Federal Deposit Insurance Corporation. In addition, banks may also be regulated at the state level. Many states have executed an agreement to share complaint information with one or more of these federal or state agencies. If the examination results find adverse trends or a pattern of activities that may be of concern to a federal or state agency and there is an agreement to share information, it may be appropriate to notify the agency of the examination findings.

This chapter contains examination standards that are relevant to nearly all types of examinations. Chapters 17 through 28 contain standards that are specific to various product lines and specialized entities.

### A. Operations/Management

#### 1. Purpose

The Operations/Management portion of the examination is designed to provide a view of what the regulated entity is and how it operates. It is not based on sampling techniques; it is more concerned with structure. This review is not intended to duplicate a financial examination review, but is important in providing the market conduct examiner with an understanding of the examinee. Many troubled companies have become so because management has not been structured to recognize and address the problems that can arise in the insurance industry. The areas to be considered in this kind of review include:

- a. History;
- b. Profile;
- c. Subcontractor oversight;
- d. Internal audits;
- e. Antifraud initiatives;
- f. Certificates of authority;

- g. Disaster recovery plan;
- h. Computer systems; and
- i. Privacy.

## 2. Techniques

Typically, the items to be reviewed here can be prepared by the regulated entity and provided at the pre-examination conference. Supplemental information, including history and profile may be available in the insurance department files. Other items suggest an active review of regulated entity files relating to managing general agent (MGA) or subcontractor oversight, internal audits, procedure manuals, record management, computer systems controls and antifraud plans. The latter category of items should have substantial supporting documentation.

The absence of subcontractor oversight, internal audit functions, written procedures or an antifraud plan should be specifically noted when preparing the examination report.

### a. History

The examiner should prepare for the examination report a very brief history of the regulated entity, including its formation; its type; its structure, including the parent corporation and other members of the group; and any major changes that are relevant to the current examination.

### b. Profile

The profile includes an overview of the regulated entity's operations, including management structure, type of carrier, states where the regulated entity is licensed and the entity's major line(s) of business. A total change in the management team may generate the need to review the regulated entity on an abbreviated time cycle.

The examiner should review Examination Tracking System (ETS) findings from prior examinations, Regulatory Information Retrieval System (RIRS) results, complaint index reports and reports from other NAIC applications and databases to determine if other regulators have expressed concerns that may require additional attention during the examination. RIRS and ETS information should not be included in the examination report.

The total written premiums for the major lines of business should be compared to the total writing in a given state to determine the market share. The loss, expense and combined ratios can be obtained from the expense exhibit attached to the annual statement or the NAIC Financial Analyst Workbench (FAW) system and may be calculated for the specific jurisdiction. Review IRIS ratios, which can be an indicator of market conduct problems. The surplus ratio should also be examined and noted for the period under review. Substantial shifts in the geographical area of operation and kinds of business written and volume should be noted, questioned and described.

### c. Subcontractor Oversight

The jurisdiction's statutes on MGAs and other subcontractors are sources of tests for this oversight. The aim is to ensure that a regulated entity using subcontractors engages in a

realistic level of oversight. Contracts should be reviewed to ensure compliance with the MGA statutes governing contract content and oversight features. The focus is on the oversight impacting records and actions considered in a market conduct examination such as, but not limited to, trade practices, claim practices, policy selection and issuance, rating, complaint handling, etc. Examiners should pay particular attention to a subcontractor's dealings with policyholders and claimants.

d. Internal Audits

A regulated entity that has no internal audit function lacks the ready means to detect structural problems until after problems have occurred. Any questionable findings about the internal audit function should be referred to the Examiner-in-Charge.

e. Antifraud Initiatives

The regulated entity should have antifraud initiatives reasonably calculated to detect, prosecute and prevent fraudulent insurance acts. Written procedural manuals or guides and antifraud plans should provide sufficient detail to enable employees to perform their functions in accordance with the goals and direction of management. In addition, insurers may be required by law to establish antifraud initiatives and examiners should be aware of any state-specific legal requirements pertaining to antifraud measures.

f. Certificates of Authority

The examiner should determine if the regulated entity's operations conform with the regulated entity's certificates of authority.

g. Disaster Recovery Plan

It is essential that the regulated entity has a formalized disaster recovery plan that will detail procedures for continuing operations in the event of any type of disaster. The examiners should determine if the regulated entity maintains separate backups of all records and facilities to continue operations.

h. Computer Systems

The examiners should determine the types of controls, safeguards and procedures for protecting the integrity of the computer information. The focus in this case is on those records subject to a market conduct examination that are maintained in electronic format, such as, but not limited to, underwriting files, claim files, rate and form filings, complaint files, statistical data used to support rates, etc.

The regulated entity should identify the location(s) of all Web sites maintained by or for and authorized by the regulated entity and all approved producer sites.

In addition, an Internet search using the regulated entity's name should be conducted using a search engine such as Yahoo, Google or WebCrawler. If any additional sites are located that the regulated entity did not identify, it should be specifically noted when preparing the examination report. The examiner should be mindful that some searches may produce a large

volume of “hits.” In such a situation, the examiner should employ sampling techniques to determine the regulated entity’s general practices on the Internet.

i. Minutes from All Meetings Attended by the Board of Directors

A review of the minutes of meetings with the board of directors should be conducted to ensure the board has proper oversight of the company’s operations and activities. Note to examiner: If you are examining a credit company, there may be statutes, rules, and regulations with specific requirements regarding the organization and structure of credit organizations.

j. Privacy

The NAIC has adopted several sets of privacy requirements and examiners will need to determine which requirement(s) the state imposes to conduct an examination. The first is the NAIC Insurance Information and Privacy Protection Model Act (hereinafter, the 1982 Model Act). The second NAIC approach was the Health Information Privacy Model Act, which had not been adopted by any state as of the end of 2000, although a few had related laws.

Next, the NAIC adopted the Privacy of Consumer Financial and Health Information Regulation (the 2000 Model Privacy Regulation) to assist states with promulgation of regulations to comply with certain requirements of Title V of the federal Gramm-Leach-Bliley Act (GLBA) (PL 102-106), enacted by Congress in 1999. And, in 2002, The Standards for Safeguarding Customer Information Model Regulation, (the 2002 Model Information Security Regulation) was adopted to assist states in establishing standards for development and implementation of safeguards by insurers to protect customer information, also required by Title V of GLBA.

In some cases, a state may have one or more of these measures, or a combination thereof, in force. NAIC records indicate that as of January 2005:

- 37 states plus the District of Columbia have enacted regulations/laws based on the 2000 Model Privacy Regulation
- Of those 38 jurisdictions:
  - 23 states include the financial and health provisions of the model (2 of those states have opt in instead of opt out requirements);
  - 14 states plus the District of Columbia have financial but not health provisions of the model; and,
  - 13 states have retained the 1982 Model Act on their books (note that several of these states have incorporated some GLB privacy protections into their current laws).

### **1982 Model Act**

The 1982 Model Act is focused primarily on the insurance application process, underwriting, policy issuance and related transactions. It requires various disclosures to applicants regarding the insurer's practices (e.g., that an investigative consumer report may be obtained and that information may be disclosed to insurance support organizations which, in turn, may retain and later re-disclose the information to others) and the applicant's rights (e.g., that the applicant has a right to obtain a copy of any investigative consumer report and that the applicant has the rights of access to and correction of information about him/her).

Notices providing these disclosures may be required at application and whenever there is a "change of status"—e.g., at renewal or reinstatement—if new or additional information is to be collected from a source other than the applicant. There is no requirement for annual notices. If an insurer intends to disclose information for the marketing of a product or service, the customer must be given an opportunity to opt out. Market Conduct Standards #10 and #11 are applicable only for those states that have enacted the 1982 Model Act or substantially similar privacy requirements.

### **2000 Model Privacy Regulation**

The 2000 Model Privacy Regulation was adopted to implement certain privacy provisions of the Gramm-Leach-Bliley Act. Title V of GLBA addressed the confidentiality of information about customers of "financial institutions," a term that includes insurance companies, banks and depository institutions, broker-dealers, investment companies, registered investment advisers and a variety of other kinds of businesses. Title V, as further implemented by the 2000 Model Privacy Regulation, requires that financial institutions establish and implement a privacy policy and provide notices to customers describing such policies and the customer's rights to opt out of disclosures other than those allowed by the exceptions in sections 14 through 16 (section 17B of the NAIC model regulation sets forth exceptions for the customer authorization requirement for certain health information disclosures). The adoption of regulations and guidelines was delegated to the functional regulators of the various financial institutions.

The federal functional regulators (including, among others, the Securities and Exchange Commission, the Office of the Comptroller of Currency and the Federal Trade Commission) and the NAIC have taken substantially similar positions in their regulations regarding the disclosure of customer personal information and notices. The federal regulations are nearly identical to each other, with very minor differences to reflect the different financial products and services involved and related business practices. The 2000 Model Privacy Regulation is very similar to the federal regulations with respect to the treatment of financial information, with appropriate changes for insurance products and services, as well as established business practices and relationships.

The notices required by the 2000 Model Privacy Regulation include initial, revised and annual privacy notices, which must reflect the privacy policy, including financial information disclosure practices, of the insurance regulated entity or other licensee. It should be noted that privacy policies differ from insurer to insurer, from insurer to other licensee, etc. There is no set format required for privacy notices, although they must be "clear and conspicuous" as that term is defined in the regulation. The regulation does, however, list the topics that the privacy notice must address. Since a privacy notice reflects a specific insurer's or other

licensee's own particular financial information privacy practices, notices will legitimately differ.

The 2000 Model Privacy Regulation differs from the federal agency regulations in that the model includes protections for certain health information. In general, a licensee must get an individual's approval (opt in) prior to disclosing nonpublic personal health information, unless the disclosure falls under an exception listed in subsection 17B or the licensee is in compliance with the health privacy regulation promulgated by the U.S. Department of Health and Human Services (HHS) pursuant to the federal Health Information Portability and Accountability Act (HIPAA). Even if the licensee is not subject to HIPAA, the 2000 Model Privacy Regulation allows the option of complying with the HHS standards as an alternative to the NAIC standards.

Market Conduct Standards #12, #13, #14, #15 and #16 are applicable for examination of compliance with the 2000 Model Privacy Regulation regarding the disclosure of customer information.

### **2002 Model Information Security Regulation**

The 2002 Model Information Security Regulation was adopted to establish standards regarding safeguarding of customer information, also required by Title V of GLBA. It should be noted that the 2002 Model Information Security Regulation requires that a licensee establish an information security program "appropriate to the size and complexity of the licensee," as well as appropriate to the "nature and scope of (the licensee's) activities." The regulation provides illustrative examples of various factors that a licensee may consider when developing its information security program.

Market Conduct Standard #17 is applicable for examination of compliance with the 2002 Model Information Security Regulation for security standards.

## **3. Tests and Standards**

The operations and management review includes, but is not limited to, the following standards addressing various aspects of a regulated entity's operations. The sequence of the standards listed here does not indicate priority of the standard.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 1**

**The regulated entity has an up-to-date, valid internal or external audit program.**

**Apply to:** All regulated entities

**Priority:** Recommended

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Audit plan and regulated entities' procedural manuals

\_\_\_\_\_ Audit reports and results

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Consumer Credit Insurance Model Regulation, Section 12  
Model Regulation to Require Reporting of Statistical Data by Property and Casualty Insurance  
Companies, Section 11

**Review Procedures and Criteria**

Review audit reports to determine if the function is providing meaningful information to management. If external, obtain an explanation.

Determine how management is using the reports.

Determine if the regulated entity responds to internal audit recommendations to correct, modify and implement procedures.

Determine if accuracy of internal statistical data and information systems is periodically tested by the regulated entity's audit program.

Determine if the regulated entity conducts periodic reviews of creditors with respect to their credit insurance business with such creditors.

Determine if the regulated entity has adopted edit and audit procedures to screen and check data submitted by the regulated entity's statistical agent.

Note: The examiner should be mindful of the proprietary nature of internal audit reports. Administrative action should not be recommended by the examiner based on results of internal audit findings for which the regulated entity has taken appropriate corrective action.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 2**

**The regulated entity has appropriate controls, safeguards and procedures for protecting the integrity of computer information.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Electronic records control, recovery/backup plan and regulated entities' procedural manuals; whether the records are electronic

\_\_\_\_\_ Negotiated contracts

Others Reviewed

\_\_\_\_\_  
\_\_\_\_\_

**NAIC Model References**

Privacy Protection Model Act

Health Information Privacy Model Act

**Review Procedures and Criteria**

Review regulated entity records, central recovery and backup procedures. The plan and procedures should be valid and up-to-date.

Review computer security procedures.

If the regulated entity permits changes to be made to policies either electronically or verbally, check what security procedures the regulated entity has established to permit these changes. These may include who has authority to make those changes, and what verification is done by the regulated entity with the insured after changes are made.

Ensure there is adequate security of applicant/insured data during the electronic transference of information. Identify any areas where the applicant's/insured's privacy is not properly protected.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 3**

**The regulated entity has antifraud initiatives in place that are reasonably calculated to detect, prosecute and prevent fraudulent insurance acts.**

**Apply to:** All regulated entities

**Priority:** Recommended

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity antifraud plan and procedural manuals

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Insurance Fraud Prevention Model Act

**Review Procedures and Criteria**

Review the regulated entity's antifraud initiatives in conjunction with applicable statutory requirements. Antifraud initiatives may include fraud investigators and an antifraud plan.

If the regulated entity has an antifraud plan, determine if the plan has been submitted to the insurance commissioner. Determine if the plan is adequate, up-to-date and in compliance with statutes, rules and regulations.

Review the regulated entity's implementation (staffing, support, etc.) of its plan and, if necessary, discuss with management.

Determine if the regulated entity has procedures in place to prevent persons convicted of a felony involving dishonesty or breach of trust from participating in the business of insurance.

Determine if the regulated entity has procedures in place to provide information regarding fraudulent insurance acts to the insurance commissioner and in a manner prescribed by the commissioner.

**STANDARDS  
OPERATIONS/MANAGEMENT**

<b>Standard 4</b> <b>The regulated entity has a valid disaster recovery plan.</b>
--

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Description of the regulated entity’s disaster recovery plan, procedural manuals and controls

\_\_\_\_\_ Description of protective devices for various hazards and procedures/controls for protection from those hazards

\_\_\_\_\_ Negotiated contracts

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

**Review Procedures and Criteria**

Determine that the regulated entity’s database(s) are protected from various hazards, including environmental hazards.

Review the regulated entity’s documents. Any additional areas or lack of information should be discussed with the regulated entity’s management. The disaster recovery plan should be valid, specific and operational, with procedures for implementation and should also be current. Failure of the regulated entity to adequately plan for the future means the standard was not met.

Failure of the regulated entity to adequately (on an ongoing basis) provide for off-site backup, failure of the regulated entity to provide adequate controls and, in the case of a catastrophe, failure to provide for recovery, means the standard was not met.

Standard #2 of this section also addresses disaster recovery issues.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 5**

**Contracts between the regulated entity and entities assuming a business function or acting on behalf of the regulated entity, such as, but not limited to, managing general agents (MGAs), general agents (GAs), third-party administrators (TPAs) and management agreements, must comply with applicable licensing requirements, statutes, rules and regulations.**

**Apply to** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Contracts

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Service Contracts Model Act  
Prepaid Legal Expense Model Act  
Managing General Agents Act

**Review Procedures and Criteria**

Review the contract to determine compliance with state statutes and rules.

The contract should specify the responsibilities of the subcontractor regarding recordkeeping and responsibilities of the regulated entity for conducting audits.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 6**

**The regulated entity is adequately monitoring the activities of any entity that contractually assumes a business function or is acting on behalf of the regulated entity.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Contracts

\_\_\_\_\_ Audit reports

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Managing General Agents Act, Section 5

Third Party Administrator Statute, Section 6

Consumer Credit Insurance Model Regulation, Section 12

Variable Life Insurance Model Regulation

**Review Procedures and Criteria**

Entities can include an MGA, GA or TPA. Suppliers of consulting, investment, administrative, sales, marketing, custodial or other services with respect to variable life insurance operations are also considered entities (Variable Life Insurance Model Regulation, Section 3E).

Review entity contracts to determine compliance with statutes, rules and regulations. The contract should specify the responsibilities of the MGA, GA and TPA concerning recordkeeping and responsibilities of the regulated entity for conducting audits.

Review audit reports to determine whether the regulated entity is adequately monitoring the activities of the contracted entity.

Review activities of entities to ensure compliance with applicable statutes and rules.

For credit insurance, each insurer is responsible for conducting a thorough periodic review of creditors with respect to their credit insurance business. The review should ensure compliance with statutes, rules and regulations. Written records of the reviews must be maintained by the insurer.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 7**

**Records are adequate, accessible, consistent and orderly and comply with state record retention requirements.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ All records, files and documents

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Complaints: Records to be Maintained

Market Conduct Record Retention Model Regulation

Unfair Claims Settlement Practices Act

Unfair Property and Casualty Claims Settlement Practices Model Regulation

Model Law on Examination, Section 4

Unfair Life, Accident and Health Claims Settlement Practices Model Regulation

**Review Procedures and Criteria**

Evaluate the orderly organization, legibility and structure of files.

Review state record retention requirements to determine regulated entity compliance.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 8**

**The regulated entity is licensed for the lines of business that are being written.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Certificate of authority or other similar documents

\_\_\_\_\_ Access NAIC financial system

\_\_\_\_\_ Regulated entity system

Others Reviewed

\_\_\_\_\_  
\_\_\_\_\_

**NAIC Model References**

Service Contracts Model Act  
Prepaid Legal Expense Model Act  
Nonadmitted Insurance Model Act

**Review Procedures and Criteria**

Review certificates of authority; compare writings with authorized lines.

Review financial annual statement submitted to the NAIC; compare writings with authorized states.

Obtain explanation of any discrepancies.

Access regulated entity system to verify that writings are in line with written premium reported in financial annual statement.

**Automation Tip:**

The Financial Applications section of NAIC's I-SITE contains the Annual Statement financial information for insurance companies that report to the NAIC. The most useful for market conduct examiners would be the Annual Statement Pick-a-Page. The State Page Exhibit displays the direct written premiums in any particular state for any particular year.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 9**

**The regulated entity cooperates on a timely basis with examiners performing the examinations.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations, especially insurance examination law

\_\_\_\_\_ All records, files and documents

Others Reviewed

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Model Law on Examinations

**Review Procedures and Criteria**

Monitor regulated entity's cooperation during the course of the exam; this may be noted in the examination report.

**Automation Tip:**

Requests for information or "crits" can be monitored using either a database or spreadsheet. The information that should be captured: area of review, type of request, contact person, date given, date due and date received. Databases and spreadsheets contain functions that will calculate the number of days between two dates. The information can be easily sorted and reviewed to see what is still outstanding and if the regulated entity is responding in a timely fashion.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 10**

**The regulated entity has procedures for the collection, use and disclosure of information gathered in connection with insurance transactions so as to minimize any improper intrusion into the privacy of applicants and policyholders.**

**Apply to:** All regulated entities

**Priority:** Recommended

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Written procedures of regulated entity for maintaining personal information and privileged information of applicants and policyholders

\_\_\_\_\_ The “Notice of Information Practices” required to be provided to applicants and policyholders

\_\_\_\_\_ Disclosure Authorization Forms

\_\_\_\_\_ Written procedures for the correction, amendment or deletion of recorded personal information

**Others Reviewed**

\_\_\_\_\_ \_\_\_\_\_  
\_\_\_\_\_ \_\_\_\_\_

**NAIC Model References**

Privacy Protection Model Act

Health Information Privacy Model Act

Unfair Discrimination Against Subjects of Abuse in Property and Casualty Insurance Model Act

Unfair Discrimination Against Subjects of Abuse in Life Insurance Model Act

Unfair Discrimination Against Subjects of Abuse in Health Benefit Plans Model Act

**Review Procedures and Criteria**

Determine if the regulated entity appropriately provides a “notice of information practices” which contains the required information.

Determine if the content of “disclosure authorization form” meets content standards.

Determine if the regulated entity properly handles the use of investigative consumer reports.

Determine if the regulated entity’s procedures appropriately limit access to personal information.

Determine if the regulated entity provides specific and accurate reasons for adverse underwriting decisions.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 11**

**The regulated entity has developed and implemented written policies, standards and procedures for the management of insurance information.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity procedure manual

\_\_\_\_\_ Regulated entity training manual

\_\_\_\_\_ Internal regulated entity claim audit procedures

\_\_\_\_\_ Regulated entity bulletins regarding insurance information

\_\_\_\_\_ Contractual arrangements between the carrier and a person other than the covered person

**Others Reviewed**

\_\_\_\_\_

\_\_\_\_\_

**NAIC Model References**

Health Information Privacy Model Act, Section 5

Insurance Information and Privacy Protection Model Act, Sections 4-9

**Review Procedures and Criteria**

Review regulated entity procedures, training manuals and claim bulletins to determine if regulated entity standards exist and whether standards comply with state law.

Review contractual arrangements between the regulated entity and other persons to determine if the contracts address privacy procedures and standards for the person with whom the regulated entity is contracting.

Review the regulated entity's methods for handling, disclosing, storing and disposing of insurance information. The examiners should determine whether there are procedures in place to ensure proper authorization is obtained prior to disclosure of insurance information.

Review the regulated entity's training manual to determine whether the regulated entity's employees are properly trained on the handling of insurance information.

Verify that the regulated entity provides a "Notice of Information Practices" to all applicants or policyholders or has procedures in place for the producer to deliver the notice. The examiner should determine whether the notice contains all provisions required by applicable state law.

Verify that the regulated entity specifies those questions designed to obtain information solely for marketing or research purposes.

Verify that the regulated entity has implemented reasonable procedures to address investigative consumer reports and personal interviews.

Verify that the regulated entity has established procedures to address access to, correction, amendment or deletion of recorded personal information.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 12**

**The regulated entity has policies and procedures to protect the privacy of nonpublic personal information relating to its customers, former customers and consumers that are not customers.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity privacy policies and procedures

\_\_\_\_\_ Other regulated entity manuals/instruction books

\_\_\_\_\_ Communication provided by the regulated entity to employees and producers subject to the regulated entity's privacy policies

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state's definition of "customer" and "consumer" to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state's privacy act/regulation.

**NAIC Model References**

Privacy of Consumer Financial and Health Information Model Regulation

**Review Procedures and Criteria**

Review the regulated entity's policies, practices and procedures regarding protection and disclosure of nonpublic personal information of customers, former customers and consumers who are not customers, to verify that they comply with applicable state laws regarding privacy.

Review employee procedures regarding the treatment of nonpublic personal information to verify that they comply with the regulated entity's privacy policies, practices and procedures and with applicable state laws regarding privacy.

As applicable, verify that the regulated entity/licensee has provided a copy of its privacy notice to its producers.

Determine that the regulated entity does not unfairly discriminate against customers and consumers who are not customers who (1) have opted out from the disclosure of nonpublic personal financial information to nonaffiliated third parties; and (2) have not authorized disclosure of nonpublic personal health information, if applicable.

Review all privacy-related consumer complaints and inquiries.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 13**

**The regulated entity provides privacy notices to its customers and, if applicable, to its consumers who are not customers regarding treatment of nonpublic personal financial information.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity privacy policies and procedures

\_\_\_\_\_ Sample notices to customers: initial, annual, revised and simplified, if applicable

\_\_\_\_\_ Sample notices to consumers that are not customers, if applicable: initial (standard and short form) notices and revised notice

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state’s definition of “customer” and “consumer” to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state’s privacy act/regulation.

**NAIC Model References**

Privacy of Consumer Financial and Health Information Model Regulation

**Review Procedures and Criteria**

Review the content of the regulated entity’s initial, annual and revised notices.

Verify that these notices are clear and conspicuous and accurately reflect privacy policies and practices.

Notices should include the following:

- Identification of the regulated entity, if applicable;
- The categories of nonpublic personal financial information that the regulated entity collects;
- The categories of nonpublic personal financial information that the regulated entity discloses, if applicable;
- The categories of affiliates and nonaffiliated third parties to whom the regulated entity discloses nonpublic personal financial information, other than disclosures permitted under sections 15 and 16 of the NAIC model regulation, if applicable;
- The categories of nonpublic personal financial information about the regulated entity’s former customers that the regulated entity discloses and the categories of affiliates and nonaffiliated

third parties to whom the regulated entity discloses nonpublic personal financial information about the regulated entity's former customers, other than disclosures permitted under sections 15 and 16 of the NAIC model regulation, if applicable;

- If a regulated entity discloses nonpublic personal financial information to a nonaffiliated third-party under Section 14 of the NAIC model regulation, a separate description of the categories of information the regulated entity discloses and the categories of third parties with whom the regulated entity has contracted;
- An explanation of the consumer's right to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right, if applicable;
- Any disclosures that the regulated entity may make under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. Section 1681a(d)(2)(A)(iii) (i.e., notices regarding the ability to opt out of disclosures of information among affiliates, other than transaction and experience information);
- The regulated entity's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- If a regulated entity only discloses nonpublic personal financial information as authorized under sections 15 and 16 of the NAIC model regulation, a statement that indicates the regulated entity makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

Review the content of the regulated entity's simplified notice, if applicable, which shall include:

- Identification of the regulated entity and affiliates or subsidiaries, if applicable;
- The categories of nonpublic personal financial information that the regulated entity collects;
- The regulated entity's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- That the regulated entity only discloses nonpublic personal financial information to affiliates and nonaffiliated third parties, as applicable, as authorized under sections 15 and 16 of the NAIC model regulation.

Review the content of the regulated entity's short-form notice for consumers who are not customers, if applicable, which shall state that the regulated entity's privacy notice is available upon request and provide a reasonable means by which the consumer may obtain a full notice.

Verify that the regulated entity's process for delivery of notices includes:

- Initial notice, if applicable, to consumers who are not customers;
- Initial notice to all customers, as required;
- Annual notice to all customers, as required;
- Revised notice to customers and consumers who are not customers entitled to notice, if applicable;
- Where applicable, simplified notices to customers, if the regulated entity only discloses nonpublic personal financial information about customers and former customers to affiliates and

nonaffiliated third parties as authorized under sections 15 and 16 of the NAIC model regulation (or the applicable sections under state law regarding privacy); and

- Short-form notices to consumers who are not customers, in lieu of initial notices, if applicable.

Verify that a notice is delivered to the regulated entity's customers at or prior to the time the regulated entity establishes a customer relationship (initial notice), and at least once in any period of twelve (12) consecutive months or once in each calendar year thereafter (annual notice) during the continuation of the customer relationship, if appropriate. If initial notice was provided to customers after the customer relationship was established, verify that the notice was delivered within a reasonable time after the customer relationship was established and (1) establishing the customer relationship was not at the customer's election; or (2) providing notice at or prior to the establishment of the relationship would have substantially delayed the customer's transaction and the customer agreed to receive the notice at a later time.

Verify that if the regulated entity discloses any consumer's nonpublic personal financial information to any nonaffiliated third-party, other than as authorized under section 15 or 16 of the NAIC model regulation (or the applicable sections under state laws regarding privacy), the regulated entity delivers a notice before disclosing the information.

Verify that individuals deemed consumers under applicable law are provided with an initial notice where applicable (such as where a licensee discloses a claimant's nonpublic personal financial information outside Sections 14 through 16 of the NAIC model regulation or its equivalent under state laws regarding privacy).

Verify that a notice was delivered to the regulated entity's customers and, if applicable, to consumers who are not customers in a manner that can reasonably be expected to provide actual notice. Verify that a notice was provided to the regulated entity's customers and, if applicable, to consumers who are not customers, in writing, or, if the licensee provides and if the consumer has agreed, electronically.

Verify that the regulated entity has provided customers with clear and conspicuous initial, annual and revised notices in a manner that allows the customer to retain the notices or obtain them later in writing or, if the customer has agreed, electronically.

If the regulated entity is an excess lines insurer and does not disclose nonpublic personal financial information to nonaffiliated third parties, except as authorized under sections 15 and 16 of the NAIC model regulation, verify that the notice set forth in section 4Q(3)(ii) of the NAIC model regulation has been delivered to all customers at the time the regulated entity established ongoing relationships with the customers. If the regulated entity makes disclosures other than as authorized under sections 15 and 16 of the NAIC model regulation, the regulated entity is required to comply with applicable initial, annual and revised notice requirements and the opt out requirements.

Review the regulated entity's notice content and notice delivery procedures to verify that the regulated entity complies with applicable statutes, rules and regulations regarding privacy.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 14**

**If the regulated entity discloses information subject to an opt out right, the regulated entity has policies and procedures in place so that nonpublic personal financial information will not be disclosed when a consumer who is not a customer has opted out, and the regulated entity provides opt out notices to its customers and other affected consumers.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity privacy policies and procedures

\_\_\_\_\_ Sample notices to customers: initial, annual and, if applicable, revised

\_\_\_\_\_ Sample notices to consumers who are not customers, if applicable

\_\_\_\_\_ Sample opt out notice, if applicable

\_\_\_\_\_ Regulated entity records of consumers and other customers who have opted out, if applicable

\_\_\_\_\_ Communication of customers' and consumers who are not customers' opt out elections to producers of record

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state's definition of "customer" and "consumer" to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state's privacy act/regulation.

**NAIC Model References**

Privacy of Consumer Financial and Health Information Model Regulation

**Review Procedures and Criteria**

Determine whether the regulated entity discloses nonpublic personal information relating to customers or consumers who are not customers beyond the scope permitted under sections 14, 15 and 16 of the NAIC model regulation.

- Verify that consumers who may be affected by such disclosures have been offered the opportunity to opt out before the disclosures are made. Continue with Steps 1 through 5 below.
- If not, verify that any communications the regulated entity makes regarding opt out rights are accurate and are in compliance with applicable law.

1. If applicable, verify that the regulated entity has policies and procedures in place so that customers and other affected consumers may opt out of the disclosure of their nonpublic personal financial information to nonaffiliated third parties, except to the extent such disclosure is permitted under sections 14, 15 and 16 of the NAIC model regulation.
2. If applicable, review the regulated entity's policies and procedures to verify that the regulated entity has the capability to keep nonpublic personal financial information from being unlawfully disclosed to nonaffiliated third parties when a consumer has opted out.
3. If applicable, verify that the regulated entity does not disclose, directly or through any affiliate, unless authorized or permitted by applicable federal and/or state law or regulations, nonpublic personal financial information about a consumer or to a nonaffiliated third-party except when:
  - The regulated entity has provided a notice to the consumer;
  - The regulated entity has provided an opt out notice to the consumer;
  - The regulated entity has given the consumer a reasonable opportunity to opt out of the disclosure before the regulated entity discloses the consumer's nonpublic personal financial information to a nonaffiliated third-party; and
  - The consumer does not opt out.
4. As applicable, determine that the regulated entity's initial, annual, revised and short-form notices accurately explain the consumer's right to opt out, including the methods by which the consumer may exercise that right at any time, in accordance with applicable law and the regulated entity's policies and procedures.
5. If applicable, review the content of the regulated entity's opt out notice to determine if it is clear and conspicuous and includes, either on the form or on the initial privacy notice:
  - A statement that the regulated entity discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third-party;
  - A statement that the consumer has the right to opt out of that disclosure; and
  - A reasonable means by which the consumer may exercise the opt out right.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 15**

**The regulated entity’s collection, use and disclosure of nonpublic personal financial information are in compliance with applicable statutes, rules and regulations.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity privacy policies and procedures

\_\_\_\_\_ Joint marketing agreements, if any

\_\_\_\_\_ Sample service agreements, if any, with nonaffiliated third parties involved in the regulated entity’s marketing activities

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state’s definition of “customer” and “consumer” to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state’s privacy act/regulation.

**NAIC Model References**

Privacy of Consumer Financial and Health Information Model Regulation

**Review Procedures and Criteria**

If the regulated entity discloses nonpublic personal financial information of its customers or consumers who are not customers to nonaffiliated third parties for joint marketing purposes, verify that all such disclosures are in compliance with the NAIC model regulation:

- Verify that the regulated entity has provided initial notices to its customers and other affected consumers that include the required information regarding the regulated entity’s joint marketing and servicing activities.
- Review joint marketing agreements, where applicable, to verify that they prohibit the nonaffiliated third-party from disclosing or using the nonpublic personal financial information received from the regulated entity other than to carry out the purposes for which the regulated entity disclosed the information, including use under an exception in sections 15 or 16 of the NAIC model regulation.

Verify that the regulated entity does not disclose nonpublic personal financial information that it receives from a nonaffiliated financial institution, except in compliance with the NAIC model regulation.

Review sample service agreements under which a third party markets a licensee's own products and services, if any, to verify inclusion of non-disclosure requirements.

Verify that the regulated entity prohibits disclosure of policy numbers or similar forms of access numbers or access codes for a consumer's policy or transaction account to any nonaffiliated third-party, except as permitted by applicable law or regulation regarding privacy.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 16**

**In states promulgating the health information provisions of the NAIC model regulation, or providing equivalent protection through other substantially similar laws under the jurisdiction of the insurance department, the regulated entity has policies and procedures in place so that nonpublic personal health information will not be disclosed, except as permitted by law, unless a customer or a consumer who is not a customer has authorized the disclosure.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity privacy policies and procedures

\_\_\_\_\_ Sample authorizations used by the regulated entity to permit disclosure of nonpublic personal health information, if applicable

\_\_\_\_\_ Regulated entity records of customer and other consumer authorizations

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state's definition of "customer" and "consumer" to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state's privacy act/regulation.

**NAIC Model References**

Privacy of Consumer Financial and Health Information Model Regulation

**Review Procedures and Criteria**

If applicable, verify that the regulated entity has policies and procedures in place to secure authorizations from its customers and consumers who are not customers before disclosing their nonpublic personal health information to nonaffiliated third parties, except to the extent such disclosure is permitted under subsection 17B of the NAIC model regulation.

If applicable, verify that the regulated entity has obtained valid authorizations from customers and consumers who are not customers before disclosing their nonpublic personal health information, except to the extent such disclosures are permitted under subsection 17B of the NAIC model regulation. A valid authorization shall include:

- The identity of the consumer who is the subject of the nonpublic personal health information;
- A general description of the types of nonpublic personal health information to be disclosed;
- A general description of the parties to whom the licensee discloses nonpublic personal health information;
- A general description of the purpose of the disclosure of the nonpublic personal health information;

- A general explanation of how the nonpublic personal health information will be used;
- The signature of the consumer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant disclosure authority and the date signed;
- A notice of the length of time for which the authorization is valid; and
- A notice that the consumer may revoke the authorization at any time, and an explanation of the procedure for making a revocation.

**STANDARDS  
OPERATIONS/MANAGEMENT**

**Standard 17**

**Each licensee shall implement a comprehensive written information security program for the protection of nonpublic customer information.**

**Apply to:** All regulated entities

**Priority:** Essential

**Documents to be Reviewed:**

\_\_\_\_\_ Applicable statutes, rules and regulations

\_\_\_\_\_ Regulated entity written materials describing its information security program

\_\_\_\_\_ Regulated entity policies, procedures and other materials it uses to implement its information security program

\_\_\_\_\_ Prior to conducting an examination, the examiner should review the state’s definition of “customer” and “consumer” to determine appropriate usage of the terms. The examiner should also review the various exceptions and exclusions contained in the state’s privacy act/regulation.

**NAIC Model References:**

Standards for Safeguarding Customer Information Model Regulation

**Review Procedures and Criteria:**

Review the regulated entity’s written information security program to determine whether the security program includes administrative, technical and physical safeguards.

Determine whether, when developing safeguards, the regulated entity took into consideration the:

- Size and complexity of the regulated entity; and
- Nature and scope of regulated entity’s activities.

In making the assessment above, consider factors such as: (1) the products and services offered by the regulated entity; (2) the methods of distribution for the products and services; (3) the types of information maintained by the regulated entity; (4) the size of the regulated entity (which may include the number of employees and the volume of business, etc.); (5) the marketing arrangements; and (6) the extent to which, or methods by which, the regulated entity communicates electronically with customers, producers and other third parties.

Evaluate whether the regulated entity’s information security program is designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of the information; and
- Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.