Draft: 5/24/18

Market Conduct Examination Standards (D) Working Group
Conference Call
May 10, 2018

The Market Conduct Examination Standards (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met via conference call May 10, 2018. The following Working Group members participated: Bruce R. Ramge, Chair, and Cindy Williamson (NE); Jim Mealer, Vice Chair (MO); Jimmy Harris and Mel Heaps (AR); Bruce Glaser and Damion Hughes (CO); Kurt Swan (CT); Sharon Shipp (DC); Debra Peirce (GA); Lori Cunningham (KY); Richard Bradley and Mary Lou Moran (MA); Denise Lamy (NH); Peggy Willard-Ross (NV); Sylvia Lawson and Mark McLeod (NY); Angela Dingus and Don Layson (OH); Joel Sander (OK); Constance Arnold (PA); Julie Fairbanks and Yolanda Tennyson (VA); Chris Rouleau (VT); Jeanette Plitt (WA); and Barbara Belling, Diane Dambach, Darcy Paskey and Rebecca Rebholz (WI); and Mark Hooker (WV).

1. Adopted its April 5 Minutes

The Working Group met April 5 and reviewed and adopted six draft annuity standardized data requests—addressing in force contracts, replaced contracts, new business declinations, plan codes, payment/withdrawal/surrender and claims—for inclusion in the reference documents of the *Market Regulation Handbook* (Handbook). The Working Group also discussed a draft document outlining the procedures for updating the Handbook.

Mr. Mealer made a motion, seconded by Ms. Plitt, to adopt the Working Group's April 5 minutes (Attachment XXXXX). The motion passed unanimously.

2. Discussed a Draft Procedures Document Updating the Handbook, April 9 Draft

Director Ramge said a new draft document outlining the procedures for updating the Handbook was developed for the purpose of documenting how changes are made to the Handbook. Director Ramge said that the document was revised per Lisa Tate's (ACLI—American Council of Life Insurers) suggestion in the April 5 Working Group conference call—moving the last sentence in Item 5 to the beginning of Item 5, and the draft was distributed on April 9. Ms. Tate provided additional comments dated April 27, which suggested that Item 5 in the April 9 draft document be replaced by the following suggested language: "Revised or new content adopted by the Working Group and the Market Regulation and Consumer Affairs (D) Committee is considered by the NAIC Executive (EX) Committee and Plenary. Changes approved by the Executive Committee and Plenary by the end of a given calendar year will be included in the subsequent year's Handbook. The changes will be posted on the Market Regulation Handbook Updates web page on StateNet for regulators and on the Market Regulation Handbook Updates web page for purchasers of the current edition of the Handbook."

Ms. Plitt and Mr. Mealer asked that an updated version of the draft procedures document be distributed to illustrate the changes proposed by the ACLI, so that the changes may be seen in context. Director Ramge said that an updated version of the draft would be distributed, and he asked that any additional comments be forwarded to NAIC staff by May 24.

3. Discussed Other Matters

Director Ramge said NAIC staff will provide advance email notice of the next Working Group conference call.

Having no further business, the Market Conduct Examination Standards (D) Working Group adjourned.

W:\National Meetings\2018\Summer\Cmte\D\MCES\5-10.docx

PROCEDURES FOR AMENDING THE *MARKET REGULATION HANDBOOK*

The procedures that the Market Conduct Examination Standards (D) Working Group (Working Group) follows for changes, amendments and/or modifications to the *Market Regulation Handbook* (Handbook) follow.

1. When Working Group members or NAIC support staff identify an issue that could lead to relevant changes to the Handbook, an initial draft is prepared by NAIC staff, with input from the chair of the Working Group and regulator subject matter experts, as needed.

2. Exposure drafts are exposed for comment prior to open Working Group meetings, then reviewed and discussed during open Working Group meetings. Comments and suggested revisions received from regulators and interested parties may be incorporated into reviewed exposure drafts. The Working Group adopts amendments to the Handbook by a majority vote at open meetings.

3. Initial comment periods on Working Group exposure drafts are 30 days in length. The Working Group may consider an additional exposure period of less than 30 days, for subsequent revisions to the same draft.

4. Working Group members, interested regulators and interested parties are notified of the Working Group's consideration of new or revised content for the Handbook in advance of the meeting via email and on the NAIC website.

5. ~~Changes adopted by the NAIC Executive (EX) Committee and Plenary by the end of a given calendar year are included in the subsequent year's Handbook. After the adoption of Handbook changes by the Market Regulation and Consumer Affairs (D) Committee, the changes are posted on the Market Regulation Handbook Updates web page on StateNet for regulators and on the Market Regulation Handbook Updates web page, for purchasers of the current edition of the Handbook.~~
   Revised or new content adopted by the Working Group and the Market Regulation and Consumer Affairs (D) Committee is considered by the NAIC Executive (EX) Committee and Plenary. Changes approved by the Executive Committee and Plenary by the end of a given calendar year will be included in the subsequent year's Handbook. The changes will be posted on the Market Regulation Handbook Updates web page on StateNet for regulators and on the Market Regulation Handbook Updates web page for purchasers of the current edition of the Handbook.
   The above revision to Item 5 incorporates the revised language proposed by the ACLI in their comments dated 4/27/18, to replace the language in Item 5 of the 4/9/18 draft procedures document).
6. Every volume of the Handbook specifies that the Handbook contains all NAIC guidance adopted in the previous calendar year.

G:\MKTREG\DATA\D Working Groups\D WG 2018 MCES (PCW)\Docs_WG Calls 2018\MCES WG Procedures\Current Drafts\Proc_Mkt_Reg_Hdbk_5-10_18.docx

_____ (*Chapter/Section/Title TBD*)—Conducting the Mental Health Parity and Addiction Equity Act (MHPAEA) Related Examination

Introduction

The intent of _____ (*Chapter/Section/Title TBD*)—Conducting the Mental Health Parity and Addiction Equity Act (MHPAEA) Related Examination in the *Market Regulation Handbook* is primarily to provide guidance when reviewing insurers whose business includes major medical policies offering mental health and/or substance use disorder coverage.

The examination standards in *Market Regulation Handbook* Chapter 20—Conducting the Health Examination provide guidance specific to all health carriers, but large group coverage may or may not include offering mental health and/or substance use disorder coverage. _____ (*Chapter/Section/Title TBD*) strictly applies to examinations to determine compliance with the Mental Health Parity and Addiction Equity Act (MHPAEA) of 2008 found at 42 U.S.C. 300gg-26 and its implementing regulations found at 45 CFR 146.136 and 45 CFR 147.160, and is to be used for plans that offer mental health and/or substance use disorder benefits.

MHPAEA examinations focus on barriers to covered benefits ("treatment limitations"), including financial barriers such as copayments, and medical management barriers such as preauthorization requirements. An insurer violates MHPAEA if it imposes higher treatment limitations on mental health or substance use disorder benefits, compared to the treatment limitations for medical and surgical benefits. MHPAEA applies to group health plans, and by incorporation of mental health and substance use disorder treatment as an essential health benefit under the Affordable Care Act, MHPAEA applies to qualified health plans in the individual and small group market. Some states may have mental health parity requirements that are stricter than federal requirements.

Federal law relies on state insurance regulators as the first-line enforcers of health reform provisions in the individual, small group and large group insurance markets.

Examination Standards

Each examination standard includes a citation to MHPAEA and its implementing regulations, but additional standards can be found in federal guidance documents and state law or state interpretation of federal law. Please note that the federal government periodically updates its guidance documents related to MHPAEA. Examiners should refer to the U.S. Departments of Labor, Health and Human Services, and Treasury for any updates or new MHPAEA guidance. Examiners should also contact their state's legal division for assistance and interpretation of such guidance, as well as any additional state requirements.

Collaboration Methodology

The development of state market conduct compliance tools for MHPAEA will result in enhanced state collaboration, to provide more consistent interpretation and review of parity standards.

LIST OF QUESTIONS

Question 1.
Is this insurance coverage exempt from MHPAEA? If so, please indicate the reason (e.g., retiree-only plan, excepted benefits, small employer exception, increased cost exception).

Question 2.
If not exempt, does the insurance coverage provide MH/SUD benefits in addition to providing M/S benefits?

Unless the insurance coverage is exempt or does not provide MH/SUD benefits (note that MH/SUD is one of the EHB for QHPs), continue to the following sections to examine compliance with requirements under MHPAEA.

Question 3.
Does the insurance coverage provide MH/SUD benefits in every classification in which M/S benefits are provided?

Because parity analysis for this standard is at the classification level, data must be collected for each classification. An example data collection tool is provided, which collects information needed to answer this question.

Question 4.
If the plan includes multiple tiers in its prescription drug formulary, are the tier classifications based on reasonable factors (such as cost, efficacy, generic versus brand name, and mail order versus pharmacy pick-up) determined in accordance with the rules for NQTLs, and without regard to whether the drug is generally prescribed for MH/SUD or M/S benefits?

See 45 CFR 146.136(c)(3)(iii)(A).

Question 5.
If the plan includes multiple network tiers of in-network providers, is the tiering based on reasonable factors (such as quality, performance, and market standards) determined in accordance with the rules for NQTLs and without regard to whether a provider provides services with respect to MH/SUD benefits or M/S benefits?

See 45 CFR 146.136(c)(3)(iii)(B).

Question 6.
Does the plan comply with the prohibition on lifetime dollar limits or annual dollar limits for MH/SUD benefits that are lower than the lifetime or annual dollar limits imposed on M/S benefits?

See 45 CFR 146.136(b). This prohibition applies only to dollar limits on what the plan would pay, and not to dollar limits on what an individual may be charged. If a plan or issuer does not include an aggregate lifetime or annual dollar limit on any M/S benefits, or it includes one that applies to less than one-third of all M/S benefits, it may not impose an aggregate lifetime or annual dollar limit on MH/SUD benefits. 45 CFR 146.136(b)(2). Also note that for QHPs, lifetime limits and annual dollar limits are prohibited for EHBs, including MH/SUD services.

Question 7.
Does the plan impose financial requirements (deductibles, copayments, coinsurance, and out-of-pocket maximums) or quantitative treatment limitations (annual, episode, and lifetime day and visit limits) on MH/SUD benefits in any classification that are more restrictive than the predominant financial requirement or quantitative treatment limitation of that type that applies to substantially all M/S benefits in the same classification?

See 45 CFR 146.136(c)(2). Because parity analysis is at the classification level and analysis is based on the dollar amount for expected benefits paid, data must be collected per classification. An example data collection tool is provided, which collects information needed to answer this question.

Financial Requirements (FRs) include deductibles, copayments, coinsurance, and out-of-pocket maximums. 45 CFR 146.136(c)(1)(ii). Quantitative Treatment Limitations (QTLs) include annual, episode, and lifetime day and visit limits, for example number of treatments, visits, or days of coverage. 45 CFR 146.136(c)(1)(ii).

Classification is important because it prevents insurers from selecting a more favorable comparison point on the M/S side in order to justify imposing a higher treatment limitation on the MH/SUD side. For example, if a higher copayment applies for physical therapy, but a lower copayment applies for the rest of outpatient in-network M/S treatment, the insurer cannot use only the physical therapy benefits to justify imposing that higher copayment for all MH/SUD outpatient in-network treatment.

If a FR (copayment or coinsurance) or QTL (session or day limit) for MH/SUD benefits raises concern for the examiner, the first step is to identify the comparison point by looking at M/S benefits for that classification. Determine whether the FR or QTL applies to two-thirds of the M/S benefits for that classification. "Applies" means that a copayment, coinsurance, session or day limit applies to the benefits, regardless of the dollar amount, coinsurance percentage, or number of sessions or days. Benefits are judged based on the expected payments in a year. If less than two-thirds of the M/S benefits in a classification have the same FR or QTL, then the FR or QTL cannot be imposed on those MH/SUD benefits in the same classification. If two-thirds of the payments in a year are for M/S benefits in a classification are limited by a FR or QTL, the examiner will go on to the next step to look at the specific copayment dollar amount, coinsurance percentage, or limitation on number of sessions or days.

If the FR or QTL is imposed on two-thirds of the M/S benefits in a classification, then the "level" (copayment dollar amount, coinsurance percentage, or limitation on number of days or sessions) is analyzed for parity in a second step. In this second step, the examiner will look at the M/S benefits to which the FR or QTL applies and find the "predominant" limitation—this means the specific limitation dollar amount, coinsurance percentage, or limitation on number of sessions or days that applies to more than 50% of the benefits in that classification. If less than 50% of the M/S benefits in a classification are subject to the "level" of FR or QTL, then that FR or QTL at that "level" cannot be imposed on MH/SUD benefits in the same classification.

Question 8.
Does the plan apply any cumulative financial requirement or cumulative QTL for MH/SUD benefits in a classification that accumulates separately from any cumulative financial requirement or QTL established for M/S benefits in the same classification?

See 45 CFR 146.136(c)(3)(v). For example, a plan may not impose an annual $250 deductible on M/S benefits in a classification and a separate $250 deductible on MH/SUD benefits in the same classification. Cumulative financial requirements are financial requirements that determine whether or to what extent benefits are provided based on accumulated amounts and include deductibles and out-of-pocket maximums (but do not include aggregate lifetime or annual dollar limits because those two terms are excluded from the meaning of financial requirements). 45 CFR 146.136(a).

Question 9.
Does the plan impose Non-Quantitative Treatment Limitations (NQTLs) on MH/SUD benefits in any classification that are comparable to, and applied no more stringently than, those used in applying the limitation to M/S benefits within the same classification?

Please provide or make available copies of the following procedures. For any procedure that does not apply to all plan benefits, provide a cover sheet that describes the benefits to which the procedure applies, separated into MH/SUD and M/S benefits. If parity questions arise, you may be asked to provide the expected plan payments attributable to benefits for a particular NQTL.

a) Medical management standards limiting or excluding benefits based on medical necessity or medical appropriateness, or based on whether the treatment is experimental or investigative;

b) Prior authorization and ongoing authorization requirements;

c) Concurrent review standards;

d) Formulary design for prescription drugs;

e) For plans with multiple network tiers (such as preferred providers and participating providers), network tier design;

f) Standards for provider admission to participate in a network, including reimbursement rates;

g) Plan or issuer methods for determining usual, customary and reasonable charges;

h) Refusal to pay for higher-cost therapies until it can be shown that a lower-cost therapy is not effective (also known as "fail-first" policies or "step therapy" protocols);

i) Exclusions of specific treatments for certain conditions;

j) Restrictions on applicable provider billing codes;

k) Standards for providing access to out-of-network providers;

l) Exclusions based on failure to complete a course of treatment; and

m) Restrictions based on geographic location, facility type, provider specialty, and other criteria that limit the scope or duration of benefits for services provided under the plan or coverage.

See 45 CFR 146.136(c)(4)(i) and pages 14-20 of the Self-Compliance Tool for the Mental Health Parity and Addiction Equity Act (MHPAEA) for analysis advice.

Question 10.
Does the insurer comply with MHPAEA disclosure requirements including criteria for medical necessity determinations for MH/SUD benefits, reasonable access to and copies (free of charge) of all documents, records, and other information relevant to the claim for benefits, including documents with information about the processes, strategies, evidentiary standards, and other factors used to apply an NQTL with respect to M/S benefits and MH/SUD benefits under the plan?

See 45 CFR 146.136(d)(3).

G:\MKTREG\DATA\D Working Groups\D WG 2018 MCES (PCW)\Docs_WG Calls 2018\Mental Health Parity\Current Draft\Mental Health Parity 7-09-18.docx

DATA COLLECTION TOOL FOR MENTAL HEALTH PARITY ANALYSIS

Most parity analysis examines benefits by comparing MH/SUD to M/S within a classification. 45 CFR 146.136(c)(2)(i). The exception is aggregate lifetime or annual dollar limits, which are examined for the plan as a whole. 45 CFR 146.136(b). The following is intended to simplify data collection for parity analysis at the classification level.

GUIDANCE FOR PLACING BENEFITS INTO CLASSIFICATIONS

CLASSIFICATION OF BENEFITS:

MH/SUD and M/S benefits must be mapped to one of six classifications of benefits: (1) inpatient in-network, (2) inpatient out-of-network, (3) outpatient in-network, (4) outpatient out-of-network, (5) prescription drugs, and (6) emergency care. 45 CFR 146.136(c)(2)(ii).

- The "inpatient" classification refers to services or items provided to a beneficiary when a physician has written an order for admission to a facility, while the "outpatient" classification refers to services or items provided in a setting that does not require a physician's order for admission and does not meet the definition of emergency care.

- "Office visits" are a permissible sub-classification separate from other outpatient services, as well as for plans that use multiple tiers of in-network providers.

- The term "emergency care" refers to services or items delivered in an emergency department setting or to stabilize an emergency or crisis, other than in an inpatient setting.

- Some benefits, for example lab and radiology, may fit into multiple classifications depending on whether they are provided during an inpatient stay, on an outpatient basis, or in the emergency department. For benefits that fit into multiple classifications, the insurer should divide them into classifications, including the dollars that will be paid for those services as divided.

- Insurers should use the same decision-making standards to classify all benefits, so that the same standard applies to M/S and MH/SUD classifications. For example, if a plan classifies care in skilled nursing facilities and rehabilitation hospitals for M/S benefits as inpatient benefits, it must classify covered care in residential treatment facilities for MH/SUD benefits as inpatient benefits.

FINANCIAL REQUIREMENTS AND QUANTITATIVE TREATMENT LIMITATIONS:

Financial Requirements (FRs) include deductibles, copayments, coinsurance, and out-of-pocket maximums. 45 CFR 146.136(c)(1)(ii). Quantitative Treatment Limitations (QTLs) include annual, episode, and lifetime day and visit limits, for example number of treatments, visits, or days of coverage. 45 CFR 146.136(c)(1)(ii). A two-part cost analysis test applies to financial requirements (FRs) and quantitative treatment limitations (QTLs). The general parity rule is that no FR or QTL may apply to MH/SUD benefits in a classification if the FR or QTL is more restrictive than the predominant financial requirement or treatment limitation of that type that applies to substantially all M/S benefits in the same classification.

NON-QUANTITATIVE TREATMENT LIMITATIONS:

Non-Quantitative Treatment Limitations include but are not limited to medical management, step therapy, and pre-authorization. Coverage cannot impose a NQTL with respect to MH/SUD benefits in any classification unless, under the terms of the plan as written and in operation, any processes, strategies, evidentiary standards, or other

factors included in applying the NQTL to MH/SUD benefits in the classification are comparable to, and are applied no more stringently than, the processes, strategies, evidentiary standards, or other factors used in applying the limitation with respect to M/S benefits in the classification.
All plan standards that limit the scope or duration of benefits for services are subject to the NQTL parity requirements. This includes restrictions such as geographic limits, facility-type limits, and network adequacy.

Because medical management standards do not fit into a chart the way copays or deductibles would, NQTLs are not included for initial data collection in the chart below. Instead, the insurer is asked to provide a copy of the procedures for listed types of NQTLs, with a description of the benefits to which the procedure applies, with the benefits separated into MH/SUD and M/S. If a parity concern arises from the insurer's description of benefits to which a particular NQTL procedure applies, dollar amounts for benefits in each classification can be requested using blanks in the chart below.

	Inpatient In-Network	Inpatient Out-of-Network	Outpatient In-Network Office Visit (if network tiers, acceptable to separate into tiers)	Outpatient In-Network, All Benefits Other than Office Visit	Outpatient Out-of-Network Office Visit	Outpatient Out-of-Network, All Benefits Other than Office Visit	Emergency Care	Prescription Drugs
Does the plan provide MH/SUD benefits?								
Does the plan provide M/S benefits?								
Total dollar amount of all plan payments for MH/SUD benefits expected to be paid for the relevant plan year								
Total dollar amount of all plan payments for M/S benefits expected to be paid for the relevant plan year								
List each financial requirement that applies to the classification for MH/SUD benefits, and attribute expected plan payments to each applicable financial requirement								
List each financial requirement that applies to the classification for M/S benefits, and attribute expected plan payments to each applicable financial requirement								
Does the plan impose a separate cumulative financial requirement or QTL for MH/SUD benefits that accumulates separately from any cumulative financial requirement or QTL for M/S benefits?								

	Inpatient In-Network	Inpatient Out-of-Network	Outpatient In-Network Office Visit (if network tiers, acceptable to separate into tiers)	Outpatient In-Network, All Benefits Other than Office Visit	Outpatient Out-of-Network Office Visit	Outpatient Out-of-Network, All Benefits Other than Office Visit	Emergency Care	Prescription Drugs
List each QTL that applies to the classification for MH/SUD benefits, and attribute expected plan payments to each applicable QTL								
List each QTL that applies to the classification for M/S benefits, and attribute expected plan payments to each applicable QTL								
[Add specific NQTL if a concern arises]								

MARKET REGULATION HANDBOOK
INSURANCE DATA SECURITY PRE-BREACH AND POST-BREACH CHECKLISTS

Company Name	
Period of Examination	
Examination Field Date	
Prepared By	
Date	

GUIDANCE

NAIC Insurance Data Security Model Law (#668)

OVERVIEW

The purpose and intent of the Insurance Data Security Model Law is to establish standards for data security and standards for the investigation of and notification to the Commissioner or Director of Insurance of a Cybersecurity Event affecting Licensees.

REVIEW GUIDELINES AND INSTRUCTIONS

When reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668) for the prevention of a Cybersecurity Event as defined in the model law, please refer to the examination checklist attached as Exhibit A hereto.

When reviewing a Licensee's Information Security Program and response to a Cybersecurity Event for compliance with the Insurance Data Security Model Law subsequent to a suspected and/or known Cybersecurity Event as defined in the model law, please refer to both examination checklists attached as Exhibits A and Exhibit B hereto.

When considering whether to underake such a review, refer to Section 9 of NAIC Model #668, which provides certain exceptions to compliance for Licensees with fewer than ten employees; Licensees subject to the Health Insurance Portability and Accountability Act (Pub.L, 104-191, 110 Stat. 1936, enacted August 21, 1996); and certain employees, agents, representatives, or designees of Licensees who are in themselves Licensees.

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

INFORMATION SECURITY PROGRAM (Sections 4A and 4B)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
1. Does the Licensee have a written Information Security Program (ISP)?	
2. Does the ISP clearly state the person(s) at the Licensee responsible for the program?	
3. Has the ISP been reviewed and approved by the Licensee's executive management?	
4. Has the ISP been reviewed and approved by the Licensee's Board of Directors? (Section 4E)	
5. Has the ISP been reviewed and approved by the Licensee's IT steering committee?	
6. How often is the ISP reviewed and updated? (Section 4G)	
7. Are any functions of the ISP outsourced to third parties? (*If YES, identify any such providers, review their roles and responsibilities, and the Licensee's oversight of the third parties*.)	
8. Does the ISP contain appropriate administrative, technical and physical safeguards for the protection of Nonpublic Information and the Licensee's Information Systems?	
9. Does the Licensee stay informed regarding emerging threats and vulnerabilities? (Section 4D(4))	
10. Does the Licensee regularly communicate with its employees regarding security issues?	
11. Does the Licensee ensure that employees' hardware is updated on a timely basis to ensure necessary security software updates and patches have been downloaded and installed?	
12. Does the Licensee provide cybersecurity awareness training to its personnel? (Section 4D(5))	
13. How soon after onboarding a new employee does the Licensee provide cybersecurity awareness training? At what intervals is the training renewed?	
14. Does the Licensee utilize reasonable security measures when sharing information? (Section 4D(4))	

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

RISK ASSESSMENT (Section 4C)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
15. Has the Licensee conducted a Risk Assessment to identify foreseeable internal and external threats to its information security?	
16. When was the last Risk Assessment conducted or updated?	
17. Has the Licensee designed its ISP to address issues identified in its Risk Assessment?	
18. Are Cybersecurity Risks included in the Licensee's Enterprise Risk Management process? (Section 4D(3))	

COMPONENTS OF INFORMATION SECURITY PROGRAM (Section 4D)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
19. Has the Licensee determined that the following security measures are appropriate, and has the Licensee implemented them as part of its ISP? *(If NO for any item, interview the appropriate responsible personnel to discuss the reason(s) such measures were not implemented.)*	
19a. Access controls to limit access to Information Systems to Authorized Individuals?	
19b. Physical controls on access to Nonpublic Information to limit access to Authorized Individuals?	
19c. Protection of Nonpublic Information by encryption or other appropriate means while being transmitted externally or stored on portable computing devices or media?	
19d. Secure development practices for in-house applications and procedures for testing the security of externally developed applications?	
19e. Controls for individuals accessing Nonpublic Information such as Multi-Factor Authentication?	
19f. Regular testing and monitoring of systems to detect actual and attempted attacks or intrusions into Information Systems?	
19g. Audit trails in the ISP to detect and respond to Cybersecurity Events and permit reconstruction of material financial transactions?	
19h. Measures to prevent Nonpublic Information from physical damage, loss or destruction?	
19i. Secure disposal procedures for Nonpublic Information?	

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

THIRD-PARTY SERVICE PROVIDERS (Section 4F)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
20. Does the Licensee have Third-Party Service Providers with which it shares Nonpublic Information?	
21. Does the Licensee include information security standards as part of its contracts with such providers?	
22. Does the Licensee conduct inspections or reviews of its providers' information security practices?	

INCIDENT RESPONSE PLAN (Section 4H)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
23. Does the ISP contain a written incident response plan and/or detailed process for responding to a Cybersecurity Event?	
24. Does the incident response plan provide clear guidance on when to initiate a Cybersecurity Event investigation?	
25. Does the incident response plan contain a list of clear and well-defined objectives?	
26. Does the incident response plan provide clear roles, responsibilities and levels of decision-making authority?	
27. Does the incident response plan require written assessment of the nature and scope of a Cybersecurity Event?	
28. Does the incident response plan require determination of whether any Nonpublic Information was exposed during a Cybersecurity Event and to what extent?	
29. Does the incident response plan provide clear steps to be taken to restore the security of any information systems compromised in a Cybersecurity Event?	
30. Does the incident response plan sufficiently address steps to take when a Cybersecurity Event occurs at a Third-Party Service Provider where data provided by the Licensee is potentially at risk?	
31. Does the incident response plan provide detailed instructions for external and internal communications, as well as information sharing with regulatory authorities?	
32. Does the incident response plan define various levels of remediation based on the severity of identified weaknesses?	

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

DOCUMENTATION AND REPORTING

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
33. Does the ISP describe documentation and reporting procedures for Cybersecurity Events and related incident response activities? (Section 4H)	
34. Does the ISP require a post-event evaluation following a Cybersecurity Event? (Section 4H)	
35. Does the ISP require retention of all records related to Cybersecurity Events for a minimum of five years? (Section 5D)	
36. Has the Licensee prepared and submitted annual certifications to its domiciliary state Commissioner/Director of Insurance? (Section 4I)	

PRIOR EXAMINATION FINDINGS

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
37. Has the Licensee addressed and implemented corrective actions to any material findings from any prior examinations?	

Exhibit B: Supplemental Incident Response Plan Investigation (Post-Breach) and Notification Cybersecurity Event Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 5 and 6

POST-EVENT INVESTIGATION BY LICENSEE (Section 5)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
1. Did the Licensee conduct a prompt investigation of the Cybersecurity Event? (Section 5A)	
2. Did the Licensee appropriately determine the nature and scope of the Cybersecurity Event? (Section 5B)	

NOTICE TO COMMISSIONER/DIRECTOR OF INSURANCE (Section 6)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
3. Did the Licensee provide timely notice (no later than 72 hours) to the Commissioner or Director of Insurance following the Cybersecurity Event? (Section 6A)	
4. Did the Notification to the Commissioner or Director of Insurance include the following information, to the extent reasonably available? (Section 6B)	
4a. The date of the Cybersecurity Event, or the date upon which it was discovered?	
4b. A description of how the Nonpublic Information was exposed, lost, stolen or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any?	
4c. How the Cybersecurity Event was discovered?	
4d. Whether any lost, stolen or breached Nonpublic Information has been recovered, and if so, how this was done?	
4e. The identity of the source of the Cybersecurity Event?	
4f. Whether the Licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies? *(If YES, did the Licensee provide the date(s) of such notification(s)?)*	
4g. A description of the specific types of Nonpublic Information acquired without authorization?	
4h. The period during which the Information System was compromised by the Cybersecurity Event?	
4i. A best estimate of the number of total Consumers in this state and globally affected by the Cybersecurity Event?	
4j. The results of any internal review of automated controls and internal procedures and whether or not such controls and procedures were followed?	
4k. A description of efforts being undertaken to remediate the circumstances which permitted the Cybersecurity Event to occur?	
4l. A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate the Cybersecurity Event and to notify affected Consumers?	
4m. The name of a contact person familiar with the Cybersecurity Event and authorized to act for the Licensee?	
5. Did the Licensee provide timely updates to the initial notification and Questions 4a-4m above? (Section 6B)	

OTHER NOTIFICATIONS (Section 6)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
6. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to Consumers? (*If YES, did the Licensee provide a copy of the notification to the Commissioner(s)/Directors of all affected states?)* (Section 6C)	
7. Did the reinsurer Licensee provide timely and sufficient notice of the Cybersecurity Event to ceding insurers? (Section 6E)	
8. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to independent insurance producers and/or producers of record of affected Consumers? (Section 6F)	

THIRD PARTY SERVICE PROVIDERS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
9. Did the Cybersecurity Event occur at a Third-Party Service Provider? *(If YES, did the Licensee fulfill its obligations to ensure compliance with this law, either directly or by the Third-Party Service Provider?)* (Sections 5C and 6D)	

POST-EVENT ANALYSIS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
10. What changes if any are being considered to the Licensee's ISP as a result of the Cybersecurity Event and the Licensee's response?	

