_____ (*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. Treatment limitations are classified into three general groups: financial requirements (for example, copayments), quantitative treatment limitations (for example, limits on number of treatments), and non-quantitative treatment limitations (for example, 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 ACA-compliant 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? [Explain or complete the attached Data Collection Tool.]

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? Explain.

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? Explain.

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? Explain.

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? [Explain or complete the attached Data Collection Tool.]

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? [Explain or complete the attached Data Collection Tool.]

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 cover sheet template is provided as part of the Data Collection Tool.]

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? Please provide or make available copies of documents that contain the required disclosures, with the disclosures flagged in those documents.

See 45 CFR 146.136(d)(3).

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.~~A template cover sheet for NQTLs is provided below.

FINANCIAL REQUIREMENT AND QUANTITATIVE TREATMENT LIMITATION DATA								
	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]*~~								

NON-QUANTITATIVE TREATMENT LIMITATION COVER SHEET								
Describe the NQTL to which this cover sheet applies:								
	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
Describe MH/SUD benefits to which this NQTL applies for each category.								
Describe M/S benefits to which this NQTL applies for each category.								

ABHW
Advancing Health Care Policy
for Mental Health and Addiction

August 8, 2018

Via Electronic Mail (Petra Wallace - pwallace@naic.org)
Director Bruce R. Ramge
Nebraska Department of Insurance
941 O Street, Suite 400
Lincoln, NE 68508

Re: Mental Health Parity Guidance

Dear Director Ramge,

I am writing to you today in your capacity as Chair of the Market Conduct Exam Standards (D) Working Group of the National Association of Insurance Commissioners (NAIC) to comment on the July 9th, 2018 draft Mental Health Parity Guidance on behalf of the Association for Behavioral Health and Wellness (ABHW).

ABHW is the leading association working to advance federal policy on mental health and addiction services. Founded in 1994, ABHW is dedicated to shifting the paradigm in treatment and policies for mental health and addiction to ensure access to quality care, improve overall health outcomes, and advance solutions for public health challenges. Our members include top national and regional health plans that care for more than 175 million people in both the public and private sectors.

For the last two decades, ABHW has supported mental health and addiction parity. We were an original member of the Coalition for Fairness in Mental Illness Coverage (Fairness Coalition), a coalition developed to win equitable coverage of mental health treatment. ABHW

Association for Behavioral Health and Wellness
1325 G Street NW · Suite 500 · Washington DC, 20005 · 202.449.7660 · ABHW.ORG

served as the Chair of the Fairness Coalition in the four years prior to passage of the Mental Health Parity and Addiction Equity Act (MHPAEA). We were closely involved in the writing of the Senate legislation and actively participated in the negotiations of the final bill that became law.

We appreciate the Working Group's efforts to drive consistent interpretation and enforcement of MHPAEA across states. Currently, our members encounter little uniformity in this area and this is extremely problematic for health plans that operate in multiple states.

Before delving into our comments we want to point out an inaccuracy on page one of attachment three of the NAIC draft parity document, it states "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." While this may be true in most situations, it is not necessarily true 100 percent of the time and such a statement can mislead a state's interpretation of the law. According to FAQs issued by the Departments of Labor (DOL), Health and Human Services (HHS), and Treasury (collectively, the Departments), "the general rule is that a plan may not impose a financial requirement or quantitative treatment limitation applicable to mental health or substance use disorder benefits in any classification that is more restrictive than the predominant financial requirement or quantitative limitation of that type applied to substantially all medical/surgical benefits in the same classification." This is an important point as there could be times where treatment limitations vary between a medical service and a behavioral health service and the plan would not be in violation of parity. We request that you clarify the statement "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" to reflect the predominant and substantially all test required by MHPAEA.

Our specific comments are focused on questions nine and ten in your draft guidance and are detailed below. In addition to considering our remarks, we encourage you to wait to finalize your approach in these two

areas until the guidance issued by the Departments on April 23rd, 2018, is finalized in order to help ensure consistency in the interpretation and expectations for compliance.

Question Nine:

The draft NAIC guidance directs reviewers to pages 14-20 of the DOL Self-Compliance Tool for MHPAEA (Compliance Tool). The nonquantitative treatment limit (NQTL) analysis provided in the revised Compliance Tool changes the analysis as described in federal MHPAEA regulation by introducing a new requirement not referenced in the law, regulatory text, or previous parity guidance. We propose NAIC include in their guidance that an NQTL analysis needs to be consistent with the final rule, which does not require that a specific process, strategy, and/or evidentiary standard be used in applying an NQTL.

Background

The Compliance Tool's four-step analysis is to:

1. Identify the NQTL.
2. Identify the factors the plan or issuer considered in the design of the NQTL.
3. Identify the sources (including any processes, strategies, and evidentiary standards) used to define the factors identified in Step 2 to design the NQTL, including any threshold at which each factor will implicate the NQTL.
4. Evaluate whether the processes, strategies, and evidentiary standards used in applying the NQTL are comparable and no more stringently applied to mental health/substance use disorder (MH/SUD) than to medical/surgical benefits.

In Steps 2 and 3, the Departments erroneously separate out "processes, strategies and evidentiary standards" from their equivalent "factors" used in applying the NQTL. In addition, in Step 3, the Departments go on to introduce the term "source" and categorize the processes, strategies and evidentiary standards as sources, rather than factors, as they are

identified in the regulatory text.

Instead of bringing clarity to the NQTL analysis as required by the 21st Century Cures Act, the Departments have added further complexity to the process in their articulation of Step 2 and Step 3 of the analysis defined in the Compliance Tool. Plans and issuers have no context and no resources to reference in clarifying how to interpret the meaning of "source" because it has not previously been used or defined in the parity regulation or associated guidance. It is also not clear how a "source" in Step 3 differs from a "factor" in Step 2 or whether the Departments are making an intentional distinction between these terms by included them in two separate steps.

The tool appears to suggest that there needs to be a process, strategy, and/or evidentiary standard for each factor. In contrast, the final rule requires that compliance be weighed against the processes, strategies, evidentiary standards or other factors actually used in applying an NQTL. It does not necessarily require an evidentiary standard to be used for each factor or that any specific factor be considered when applying an NQTL.

Question Ten:

The draft NAIC guidance expands the disclosure requirements beyond those in MHPAEA; therefore, we recommend that the NAIC language be amended to clearly articulate the disclosure requirements derived from MHPAEA and to the extent that the requirement to disclose additional documents is noted, we suggest that the notation make clear the source for that requirement.

Background

MHPAEA requires disclosure of: 1) "the criteria for medical necessity determinations made under the group health plan with respect to MH/SUD benefits;" and 2) "the reason for any denial under the group health plan (or health insurance coverage offered in connection with such plan) of reimbursement or payment for services with respect to MH/SUD benefits.". The draft guidance seems to combine what the law requires to

be disclosed under MHPAEA and the relevant documents individuals may request in the context of an appeal.

A general information request is not only broader than the MHPAEA required disclosures, it is also more expansive than disclosure rules under the Employee Retirement Income Security Act (ERISA). The creation of a new disclosure obligation for release of general information exceeds disclosure requirements in current law, subverting congressional intent as to the scope of mandated disclosure in this area.

Thank you for the opportunity to comment on the Workgroup's draft guidance. If you would like to discuss our letter I can be reached at greeenberg@abhw.org or (202) 449-7660.

Sincerely,

Pamela Greenberg, MPP
President and CEO

Association for Behavioral Health and Wellness
1325 G Street NW · Suite 500 · Washington DC, 20005 · 202.449.7660 · ABHW.ORG

FROM THE NAIC CONSUMER REPRESENTATIVES

To: Market Conduct Examination Standards (D) Working Group
Chair Ramge
Vice Chair Mealer
Petra Wallace

Date: August 8, 2018

Re: Market Regulation Handbook Standards: Mental Health Parity

The undersigned NAIC consumer representatives write to comment on the proposed Market Conduct Examinations Standards related to the enforcement of mental health parity protections under the Mental Health Parity and Addiction Equity Act (MHPAEA). MHPAEA was designed to end insurance discrimination against people with mental health and substance use conditions. Although MHPAEA was enacted in 2008—10 years ago—some insurers have continued to engage in discriminatory practices, and states and the federal government have struggled with enforcement efforts. These services are needed now more than ever, particularly in the face of a national opioid crisis and a rise in suicide rates.

Given these challenges, we applaud your efforts and leadership to promote compliance with MHPAEA standards during market conduct exams. Including a part of the Market Regulation Handbook on mental health and substance use parity will help ensure that all companies comply with MHPAEA's standards under 42 U.S.C. 300gg-26 and implementing regulations at 45 CFR 146.136 and 45 CFR 147.160.

MHPAEA prevents insurers from imposing less favorable limitations on mental health or substance use disorder benefits compared to what is considered medical or surgical benefits. To meet this standard, insurers must demonstrate compliance in terms of defining mental health or substance use disorder benefits, classifying benefits, financial requirements, quantitative treatment limitations (QTLs), and nonquantitative treatment limitations (NQTLs). Active monitoring and enforcement of these protections remains critical to ensuring that enrollees receive the benefits of MHPAEA.

Our primary recommendation is that the standards be more formalized and better aligned with other existing standards in the Market Regulation Handbook. Instead of a list of questions as was proposed, we urge the Working Group to develop specific MHPAEA standards, identify documents to be reviewed, more clearly state the application of MHPAEA, and develop specific review procedures and criteria.

Other chapters of the Market Regulation Handbook—such as those related to preexisting condition exclusions, guaranteed issue, and Section 1557—each reflect more standardized and structured information that examiners should review, collect, and analyze. Many of these chapters also refer examiners to additional resources, which could be particularly helpful for MHPAEA enforcement. Although the current questions that have been identified are helpful, we urge the development of specific MHPAEA market conduct examination standards that lay out these standards more clearly.

To that end, we encourage you to review the seven MHPAEA standards recommended by our colleagues at the National Alliance on Mental Illness (NAMI).[1] NAMI has decades of experience in advocating for

[1] National Alliance on Mental Illness, *NAMI Draft Mental Health Parity Exam Standards*, July 19, 2018, available at: https://www.naic.org/documents/cmte_d_market_conduct_exam_standards_exposure_nami_draft_mhp_exam_standards.pdf.

mental health parity and serving those affected by mental illness. The standards that NAMI submitted are aligned with those currently under development by the Clear Health Quality Institute (CHQI). The draft CHQI standards—which are now open for public comment—are intended to be an accreditation program for insurers and health benefits administrators to better assess and understand their MHPAEA compliance processes. NAMI's proposed standards also reflect recent federal guidance on NQTLs that were published by the U.S. Departments of Health and Human Services, Labor, and the Treasury as required under the 21st Century Cures Act.

Thank you in advance for your consideration, and we look forward to continuing to work closely with the Working Group on these new standards. If you have any questions, please contact Katie Keith (katie@out2enroll.org) or Brendan Riley (brendan@ncjustice.org).

Sincerely,

Ashley Blackburn	Anna Howard	Brendan Riley
Dave Chandrasekaran	Debra Judy	Jim Roberts
Laura Colbert	Katie Keith	Carl Schmid
Eric Ellsworth	Claire McAndrew	Andrew Sperling
Marguerite Herman	Lincoln Nehring	Lorri Unumb

From: Mitchell, Martin [mailto:mmitchell@ahip.org]
Sent: Wednesday, August 08, 2018 3:47 PM
To: Wallace, Petra
Subject: NAIC Requested Comments on Mental Health Parity-Related Examination Standards Revisions to the Market Regulation Handbook

Director Ramge, Chair
Market Conduct Examination Standards (D) Working Group
c/o Petra Wallace
NAIC Market Regulation Specialist

August 8, 2018

Director Ramge:

I would ask that you accept this informal communication as initial comments in response to your request for them in the matter of Mental Health Parity Examination Standards. I wish to set forth some of our members concerns that certain aspects of the proposed examination standards appear to be based in part on existing federal sub-regulatory guidance that may need to be reconciled with the more recently adopted mental health parity final rule. With this in mind we would ask that the Working Group further review the guidance. To that end, while it may be premature to submit specific comments at this time, we would submit the following two specific comments that may highlight in part the nature of our concerns.

QUESTION 9: The guidelines direct reviewers to pages 14-20 of the Self-Compliance Tool. There are some concerns about the approach taken under the tool in terms of steps 2 and 3 where the tool appears to suggest that there needs to be a process, strategy, and/or evidentiary standard for each factor. In contrast, the final rule requires that compliance be weighed against the processes, strategies, evidentiary standards or other factors actually used in applying an NQTL. It does not necessarily require an evidentiary standard to be used for each factor or that any specific factor be considered when applying an NQTL. While we have no concerns with referencing the guide itself, it might be helpful to include a note that an analysis need only be consistent with the final rule, which does not require that a specific process, strategy, and/or evidentiary standard be used in applying an NQTL.

QUESTION 10: It appears that question 10 confuses MHPAEA disclosure requirements with disclosures of relevant documents made in a request submitted during an appeal. MHPAEA requires disclosure of: 1. the Reason for denial (adverse benefit determination); 2. The medical necessity criteria used. In the context of an appeal, members may request disclosures for relevant documents, regardless of whether the claim is for a mental health service. Because of this, we recommend that the language be amended to clearly articulate the disclosure requirements derived from MHPAEA. To the extent that the requirement to disclose relevant documents is noted, we suggest that the notation make clear the requirement is derived from ERISA/ACA and generally applies to all claims, and so we are submitting these for your Working Group's consideration.

While in part the NAIC Summer Meetings have conflicted with our offering additional substantive comments, we have reached out to your Working Group and wish to reiterate our expectation and wish to offer what assistance we can provide as you develop appropriate and effective examination standards to assist state examiners in completing their parity reviews and examinations.

Marty Mitchell
AHIP

G:\MKTREG\DATA\D Working Groups\D WG 2018 MCES (PCW)\Docs_WG Calls 2018\Mental Health Parity\Comments Received\AHIP 8-08-18 Comments.docx

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?	

G:\MKTREG\DATA\D Working Groups\D WG 2018 MCES (PCW)\Docs_WG Calls 2018\Ins Data Security\Current Drafts\IDS Pre&PostBreach Checklists 7-16-18.doc

August 15, 2018

Director Bruce R. Ramge, Chair
Market Conduct Examination Standards (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Attn: Petra Wallace
Via e-mail: pwallace@naic.org

Re: Insurance Data Security Pre- and Post-Breach Checklists

Dear Director Ramge:

We, the undersigned, appreciate this opportunity to offer comments on the recently exposed Insurance Data Security Pre- and Post-Breach Checklists (the Checklists). As you and your Working Group consider your next steps, we offer these points:

- We question the necessity or advisability of making additions to the broadly-used Market Regulation Handbook that are based on a Model Law that is not an accreditation standard and has not been enacted in a majority of states. In fact, the Model has been enacted in only one state, and industry has expressed concern with the Model Law as adopted by the NAIC. Making additions to the Market Regulation Handbook based on the new Model Law is premature at this point.

- If the Working Group is intent on making the additions, it should at least place an advisory sentence at the beginning of the checklists, reading as follows:

  > **These checklists should be used only in states that have enacted the *NAIC Insurance Data Security Model Law (#668)* or legislation which is substantially similar to the Model**.

  We are aware that generic advisories of a similar nature appear at the beginning of each chapter in the Handbook, but we believe the brief advisory set out above would be prudent and well-placed guidance to assist examiners as they prepare their tasks.

- We are aware of the multiple, detailed revisions made in the past two years to the IT portions of the Financial Examiners Handbook. We recommend a careful comparison between those provisions and the checklists here to avoid needless duplication of work by examiners and to promote regulatory efficiency.

- We strongly recommend that the Pre-Breach Checklist, and to a lesser extent, the Post-Breach Checklist, be preceded by a reminder to Examiners that the Model Law specifies these requirements are to be based on a licensee's particular risk profile.

We thank you and other Working Group members for your consideration of our comments, and we look forward to discussing them further with you at your convenience.

Organization	Name	Phone Number	E-mail Address
American Bankers Association	Sarah Ferman	202-663-5510	sferman@aba.com
American Council of Life Insurers	Jigar Gandhi	202-624-2019	jigargandhi@acli.com
America's Health Insurance Plans	Bob Ridgeway	501-333-2621	bridgeway@ahip.org
American Land Title Association	Justin Ailes	202-261-2937	Justin@ALTA.org
Blue Cross Blue Shield Association	Joe Zolecki	312-297-5766	Joseph.Zolecki@bcbsa.com
Delta Dental Plan Association	Frank Kolb	202-525-3836	fkolb@deltadental.com
Independent Insurance Agents and Brokers of America	Wes Bissett	202-302-1607	Wes.bissett@iiaba.net
Insured Retirement Institute	Jason Berkowitz	202-469-3014	jberkowitz@irionline.org
National Association of Health Underwriters	Jessica Waltman	703-496-0796	jessica@forwardhealthconsulting.com
National Association of Insurance and Financial Advisors	Gary A. Sanders	703-770-8192	gsanders@naifa.org
National Association of Mutual Insurance Companies	Paul Tetrault	978-969-1046	PTetrault@namic.org

National Association of Professional Insurance Agents	Lauren Pachman	703-518-1344	Laurenpa@pianet.org
Property Casualty Insurers Association of America (PCI)	Robert W. Woody Alex Hageli	202-639-0496 847-553-3656	Robert.Woody@pciaa.net Alex.Hageli@pciaa.net
Reinsurance Association of America	Adam Kerns	202-783-8381	Kerns@reinsurance.org

American Insurance Association

555 12th Street, NW
Suite 550
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

August 15, 2018

Director Bruce R. Ramge, Chair
Mr. Jim Mealer, Vice Chair
Market Conduct Examination Standards (D) Working Group
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

Attn: Petra Wallace, Market Regulation Specialist

VIA Electronic Mail: pwallace@naic.org

RE: New Insurance Data Security Pre- & Post-Breach Checklists for Inclusion in the Market Regulation Handbook

Dear Director Ramge and Mr. Mealer:

The American Insurance Association (AIA) appreciates the opportunity to provide comments on the National Association of Insurance Commissioners' (NAIC) draft Insurance Data Security Pre- & Post-Breach Checklists (Checklists) for inclusion in the Market Regulation Handbook (Handbook). AIA was very active in the development of the Insurance Data Security Model Law (Model Law) and it is with that background that we provide the comments outlined below.

Consistency with the IT Examination

As a threshold matter, we are unclear as to the objective for including these Checklists in the Market Conduct Examination Handbook. In our experience, this issue has been primarily an IT Examination issue. Over the past few years, the NAIC's IT Examination Working Group has updated the IT Examination Handbook Guidance and we believe intends to also do so with regard to the Model Law. There is some overlap conceptually with the proposed Checklist items. Additionally, the IT Examiners have the expertise that market conduct examiners may not have to review the issues identified in the checklist.

We strongly urge consistency in the Examination frameworks and to avoid duplication that would unnecessarily complicate an already robust review. We believe that identifying the objectives of the Market Conduct review will assist in a more complete assessment as to the appropriate tool for reviewing a Licensee's Information Security Program and the substantive contents of the Checklist.

Advisory Language

We understand the Working Group's desire to proactively develop the Checklists, but respectfully urge the Working Group to wait to incorporate the Insurance Data Security Model Law until there is a better understanding of the role of the Market Conduct review and how states are going to incorporate the Model

Law into their state statutes. For example, Appendix B identifies 72-hr notice to the Commissioner or Director of Insurance as a criterion for review. At this time, the 72-hr requirement is only in 2 states; however, there are a handful of other states with existing laws that have varying timing requirements for notifying the Commissioner.

We acknowledge that throughout the Handbook there are references to compliance with NAIC Model Laws and that the Instructions and specific Handbook wording advise jurisdictions that they should closely review the handbook to determine the standards that reflect the statutes and regulations of the given jurisdiction and those that do not. We believe that it is important for the Working Group to reinforce this advisory language in this section as well and encourage jurisdictions to remove Appendix A and B from their individual jurisdiction's procedural manuals, if they have not adopted the Model Law.

Risk-Based

An important element of the model law is that the measures and practices identified in the Model Law are to be implemented based on the individual Licensee's risk assessment. This is a critical element of the Model Law that should be identified in the Review Guidelines and Instructions sections, because every item identified in the checklist may not be appropriate for every Licensee and will not be implemented in the same manner as other companies. In many instances a "yes" or "no" response may not be a good indicator of compliance. Additionally, this is another reason that the IT Examination may be a better resource for regulators.

Specific Recommendations

We have also identified the following criteria in the proposed Checklists that are not part of the Model Law. Notably, some of the specifics identified below are not specified in the Model Law because they depend on an individual company risk analysis and implementation decision and are not conducive to the prescriptive approach some of these criteria take. These are our initial observations and look forward to providing additional insight, as appropriate.

Exhibit A - Pre-Breach Checklist

- Criteria 3, 4 and 5: The Model Law requires that an Information Security Program be developed, implemented and maintained by the Licensee's Executive Management and reported on annually. Nowhere in the Model Law is there a requirement that the Board, IT Steering Committee, or Executive Management approve of the Information Security Program. Additionally, there is no reference in the Model Law to an IT Steering Committee. The Board can delegate some of its authority to a committee; however, it should not be assumed that such delegation is to an IT Steering Committee.

  As such, we recommend the following amendments.
  3. Has the ISP been reviewed ~~and approved~~ by the Licensee's executive management?
  4. Has the overall status of the ISP been ~~reviewed and approved by~~ reported to the Licensee's Board of Directors?
  ~~5. Has the ISP been reviewed and approved by the Licensee's IT Steering Committee?~~

- Criterion 6: The Model Law does not identify a specific timing requirement for review. As such this question is beyond the scope of the Model Law and given the risk-based nature of the Model Law will not be meaningful.

- Criterion 7: This criterion suggests that a description is required of the roles and responsibilities of any function of the information security program that is outsourced to a third party and how the Licensee will oversee such third party. This is not required by the Model Law. Rather, the Model Law requires that the Licensee designate persons/third parties who are responsible for the information

security program, and separately requires that the Licensee oversee third party service provider arrangements, generally. Requiring that Licensees include this detailed information about third party responsibilities for the Information security program functions potentially puts Licensees at risk of having such information exploited by bad actors. This is another example of where a "yes" or "no" answer is not always appropriate, but at the same time a detailed description may also be concerning. Careful consideration should be given as to how the IT Examination handles this type of question and whether there is any unnecessary and troublesome duplication.

- Criterion 10: Again, there is no requirement in the model to regularly communicate to the employees. If this is intended to assess training, that issue seems to be addressed in criterion 12.

- Criterion 13: There is no requirement as to the specific intervals at which cyber-awareness training should occur.

- Criteria 21 and 22: Importantly, due to a risk-focused approach, the Model does not require the Licensee to include information security standards as part of its contracts with third-party services providers. It also does not require inspections or reviews of the Third Party's Information Security Practices. Instead the Model Law requires the Licensee to exercise due diligence and, under the overarching umbrella of risk analysis, as applicable, require the Third Party to implement appropriate administrative, technical, and physical measures. A more consistent criterion would be to ask if the Licensee has a process to conduct due diligence according to the risk of the third party.

- Criterion 24: It is not a bad practice for a company to have guidance in place as to when to institute a Cybersecurity Event investigation, but again this is beyond the scope of the model and should be implemented based on the Licensee's risk assessment.

- Criterion 27: Section 4(H)(2)(f) generally requires that the Response Plan address the documentation and reporting of a Cybersecurity Event. This is a very different requirement than what is identified in the Checklist as requiring a written assessment of the nature and scope of the event. As appropriately identified in the Model Law, it should be the Licensee's decision as to how the Response Plan addresses documenting and reporting the Events. A company may not want to have a written assessment of the nature and scope of the Cybersecurity Event for security reasons. Therefore, the Criterion could inadvertently add a requirement to the Model Law that hinders rather than promotes security.

- Criterion 29: Similarly, Section 4(H)(2)(e) has a general requirement that Response Plan address remediation efforts. This is very different then identifying clear steps to be taken to restore the security of a compromised information system. Cyber events are not always the same and again having clear steps to be taken may lessen corporate resiliency.

- Criterion 30: We cannot find any obligation in the Model Law for the incident Response Plan to address steps to be taken when a Cybersecurity Event occurs at a Third Party Service Provider.

- Criterion 31: This criterion adds a requirement that incident Response Plan provide *detailed* instructions for the external and internal communications and information sharing. Nowhere in Section 4 is there a requirement for detailed instructions.

- Criteria 33 and 34: These criteria should be in the incident Response Plan section only. Additionally, the requirement identified in 34 is not reflective of the Model Law. The Model Law states that the incident Response Plan should address "the evaluation and revision, *as necessary,* of the incident Response Plan following a Cybersecurity Event.

Post-Breach Checklist

- Criterion 3: As stated earlier, the timing requirement for notifying a regulator of a breach varies among states and as such this criterion should be more generic.

- Criterion 4i: The notification does not need to include an estimate of the number of customers globally affected.

- Criterion 4j: Not all internal reviews of automated controls need to be included, but rather those identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.

- Criterion 6: Currently, not every state requires a Licensee to provide a copy of the notice to the Commissioner/Director.

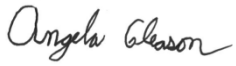
- Criterion 8: This criterion appears to distinguish between independent producers and producers of record, the Model Law does not appear to do this.

- Criterion 10: This Criterion appears to make what is a discretionary "make available" provision in the Model Law a requirement. Additionally, there may be some security concerns associated with including this type of information.

****

AIA appreciates the opportunity to provide feedback and remains committed to a constructive and collaborative dialogue. We respectfully ask that the Working Group consider whether the Checklists are the appropriate vehicle for regulatory review at this time and welcome the opportunity to provide additional substantive feedback, as appropriate. Please let us know if you have any questions or if we can be of any further assistance.

Respectfully submitted,



Angela Gleason
Senior Counsel

