

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 undertake 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? <i>(If NO for any item, interview the appropriate responsible personnel to discuss the reason(s) such measures were not implemented.)</i>	
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?	

DRAFT

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