

State Data Security Framework Survey

- * The [NAIC Data Security Model Law](#) (“NAIC Model Law”) establishes a framework of generally accepted best practices in information security, as well as a legal framework for requiring insurers and producers to implement such programs.
 - * Outlined below is a comprehensive overview of state laws and their composition relative to the NAIC Model Law. To date, eighteen states—Alabama, Connecticut, Delaware, *Hawaii*, Indiana, *Iowa*, Louisiana, *Maine*, Michigan, *Minnesota*, Mississippi, New Hampshire, *North Dakota*, Ohio, South Carolina, *Tennessee*, Virginia, and *Wisconsin*—have enacted laws that align with the NAIC Model Law. Maryland and New York have enacted their own, distinct data security provisions.
- * Though many states vary in their implementation of the NAIC Model Law (and the specific contours and details of their provisions), most states have incorporated its general framework, including requirements governing:
 - The development/implementation of a written “Information Security Program” (ISP),
 - The contours of an investigation into a cybersecurity event,
 - Notification of the state insurance regulator following a determination that a cybersecurity event has occurred, and
 - Certain limited exceptions.
- * The below survey outlines the varying state approaches to enacting the NAIC Model Law via a comparison of existing statutory text, associated regulatory provisions, and interpretive administrative guidance with respect to these specific provisions. It does not include penalty structures, a complete analysis of the definitional provisions, or discussion of the state regulator’s authority.
- * We envision this survey to be an evergreen document. As updates are put forth—whether through legislative or administrative action—we will update the document and provide a brief overview of the relevant changes in this top box in *bold and italicized blue text*. We ask, therefore, that you continuously review the document for updates to any statutes, regulations, bulletins, or other guidance documents. That said, if you see laws enacted, regulations finalized, bulletins issued, or enforcement actions undertaken that are not reflected in this survey, please let us know.
- * *Please note, we have compiled more detailed analyses on specific questions raised by Council members on how states have implemented the NAIC Model Law. In particular, we have reviewed the application of the attestation requirements and certain exceptions. To the extent that such materials are of interest, they can be found at the close of this survey. See [Appendix 1: Application of NAIC Model Law Attestation Requirements and Exceptions](#).*

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p>NAIC Model Law</p>	<p>Requires implementation of a written ISP (as overseen by the board of directors), details its objectives, and dictates how the ISP should be developed.</p> <p>Requires licensees to undertake a risk assessment and then design their ISPs so as to mitigate the identified risks, including a determination as to whether certain security measures (e.g., placement of access controls, identification and management of data, restriction of access at physical locations, etc.) are appropriate given the risks identified.</p> <p>Further requires:</p> <ul style="list-style-type: none"> • Due diligence and oversight of third-party service providers (TPSP). • Implementation of program adjustments, as needed. • Establishment of an incident response plan that addresses—among other things—the internal processes for responding to/recovering from a cybersecurity event. • Submission of an annual certification of compliance to the state regulator by February 15. 	<p>If the licensee learns/determines that a cybersecurity event has occurred, requires the licensee (or an outside vendor) to conduct a prompt investigation to:</p> <ul style="list-style-type: none"> • Determine whether a cybersecurity event occurred. • Assess the nature and scope of the event. • Identify any nonpublic information that may have been involved. • Perform and oversee reasonable measures to restore security. 	<p>Once it is determined that a cybersecurity event has occurred, requires each licensee to notify the state regulator within 72 hours that either of the following criteria has been met:</p> <ul style="list-style-type: none"> • The state is the licensee’s home state <u>or</u> • The licensee reasonably believes that the nonpublic information involved affects over 250 resident-consumers <u>and</u> is either (1) a cybersecurity event impacting the licensee of which notice is required to be provided pursuant to state/federal law <u>or</u> (2) a cybersecurity event that has a reasonable likelihood of materially harming any consumer in the state or any material part of the licensee’s normal operations. <p>Dictates the information that must be provided to the Commissioner (e.g., the date of the cybersecurity event, a description of how the information was exposed/breached, how the event was discovered, etc.); requires notification to consumers comport with the state’s data breach notification law; addresses how notice should be handled if the cybersecurity event occurs in a system maintained by a TPSP, etc.</p>	<p>Sets forth three primary exceptions which, if applicable, exempt licensees from the requirement that they develop and implement an ISP. These exemptions apply to:</p> <ul style="list-style-type: none"> • Licensees with fewer than 10 employees. • Licensees subject to HIPAA that have established and currently maintain an ISP pursuant to such statutes, rules, regulations, guidelines, etc., provided the licensee submits a written statement certifying its compliance with the state regulator. • An employee, agent, representative, or designee of a licensee (i.e., such individuals need not develop their own ISPs to the extent that they are covered by the licensee’s ISP). 	<p>N/A</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p>Alabama</p> <p>Ala. Code §§ 27-62-1 et seq.</p>	<p>Mirrors the NAIC Model Law, except does <u>not</u> require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.</p> <p>Sets a state-specific deadline, giving licensees until May 1, 2021 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs.</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Alabama <u>and</u> the breach has a “reasonable likelihood” of harming a resident or the licensee’s normal operations). Requires licensees to notify the Commissioner if a TPSP is breached, <u>unless</u> the TPSP provides the required notice to the Commissioner. 	<p>Expands exemptions in the NAIC Model Law to include those with:</p> <ul style="list-style-type: none"> Fewer than 25 employees (rather than 10). Less than \$5 million in gross annual revenue. Less than \$10 million in year-end total assets. ISPs in accordance with the Gramm-Leach-Bliley Act (GLBA). 	<p>Unlike the NAIC Model Law, does <u>not</u> include in the definition of “nonpublic information” “business related information” the tampering of which would cause a material adverse impact to the licensee.</p>
Alaska					
Arizona					
Arkansas					
California					
Colorado					
<p>Connecticut</p> <p>Conn. Gen. Stat. § 38a-38</p>	<p>Mirrors the NAIC Model Law, except sets two state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until October 1, 2020 to develop, implement, and maintain an ISP. 	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the state regulator within 3 business days (rather than 72 hours) of a cybersecurity event (rather than from the 	<p>Expands exemptions in the NAIC Model Law to include those with:</p> <ul style="list-style-type: none"> Before October 1, 2021, fewer than 20 employees (rather than 10, 	<p>N/A</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	<ul style="list-style-type: none"> Gives licensees until October 1, 2021 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. 		<p>determination that a cybersecurity event occurred).</p> <ul style="list-style-type: none"> Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Connecticut <u>and</u> 250+ residents are affected). 	<p>which will take effect on October 1, 2021).</p> <ul style="list-style-type: none"> ISPs in accordance with statutes, rules, and regulations of a jurisdiction approved by the state regulator (e.g., compliance with NYDFS’ cybersecurity regulation), though an annual statement certifying compliance must be filed with the state regulator. 	
<p><i>Delaware</i></p> <p>Del. Code Ann. tit. 18, §§ 8601 et seq.</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Delaware <u>and</u> the cybersecurity event results in a reasonable likelihood of 	<p>Expands exemptions in the NAIC Model Law to include those with fewer than 15 employees (rather than 10).</p>	<p>N/A</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
			<p>materially harming consumers, a reasonable likelihood of materially harming any material part of the licensee’s normal operations, or the licensee is required to provide notice to a government, agency, or other body under state or federal law).</p> <ul style="list-style-type: none"> Imposes industry-specific requirements governing consumer notice (e.g., notification within 60 days unless certain exceptions are met, appropriate forms of notice, etc.). 		
<i>D.C.</i>					
<i>Florida</i>					
<i>Georgia</i>					
<p><i>Hawaii</i></p> <p>Haw. Rev. Stat. Ann. § 431: -101 et seq.</p> <p>Effective July 1, 2021</p>	<p>Mirrors the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by March 31 (rather than February 15).</p> <p>Sets two state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until July 1, 2022 to implement the ISP requirements. Gives risk retention groups chartered and licensed in Hawaii until July 1, 2023 to implement the ISP requirements. 	MIRRORS NAIC MODEL LAW	<p>Mirrors the NAIC Model Law, except requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.</p>	MIRRORS NAIC MODEL LAW	N/A

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<i>Idaho</i>					
<i>Illinois</i>					
<p>Indiana</p> <p>Ind. Code Ann. §§ 27-2-27-16 et seq.</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Does <u>not</u> require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee. Does <u>not</u> affirmatively require the licensee to adjust the ISP. <p>Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by April 15 (rather than February 15).</p>	MIRRORS NAIC MODEL LAW	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Indiana <u>and</u> the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in Indiana or any material part of the normal operations of the licensee). Does <u>not</u> contain language dictating how notice should be given regarding cybersecurity events of TPSPs. 	<p>Expands exemptions in the NAIC Model Law to include those with:</p> <ul style="list-style-type: none"> Fewer than 50 employees (rather than 10). Less than \$5 million in gross annual revenue. Less than \$10 million in year-end total assets. ISPs in accordance with GLBA. <p>Does <u>not</u> apply to financial institutions as defined under federal law.</p>	<p>Entitles compliant licensees to an affirmative defense to any tort action that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information.</p>
<p>Iowa</p> <p>Iowa Code Ann. §§ 507F.4 et seq.</p>	<p>Mirrors the NAIC Model Law, except sets two state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until January 1, 2023 to develop, implement, and maintain an ISP. 	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	<p>Unlike the NAIC Model Law, exempts those with:</p> <ul style="list-style-type: none"> Fewer than 20 employees, including independent contractors. 	N/A

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p>Effective January 1, 2022</p>	<ul style="list-style-type: none"> Gives licensees until January 1, 2024 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. <p>Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by April 15 (rather than February 15).</p>			<ul style="list-style-type: none"> Less than \$5 million in gross annual revenue. Less than \$10 million in year-end total assets. ISPs in accordance with HIPAA, provided that a certification of compliance can be submitted, upon request. ISPs in accordance with GLBA or comparable federal law and corresponding regulations. 	
<i>Kansas</i>					
<i>Kentucky</i>					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p>Louisiana</p> <p>La. Rev. Stat. §§ 22:2501 et seq.</p>	<p>Mirrors the NAIC Model Law, except sets two state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until August 1, 2021 to develop, implement, and maintain an ISP. Gives licensees until August 1, 2022 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. 	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Louisiana <u>and</u> the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in Louisiana or any material part of the normal operations of the licensee). Provides that the licensee has a continuing obligation to update and supplement notifications. 	<p>Expands exemptions in the NAIC Model Law to include those with:</p> <ul style="list-style-type: none"> Fewer than 25 employees (rather than 10). Less than \$5 million in gross annual revenue. Less than \$10 million in year-end total assets. ISPs in accordance with GLBA, provided that a certification of compliance can be submitted, upon request. ISPs in accordance with statutes, rules, and regulations of a jurisdiction approved by the state regulator, though an annual statement certifying compliance must be filed with the state regulator. 	<p>Entitles compliant licensees to an affirmative defense to any tort action that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information.</p>
<p>Maine</p>	<p>Mirrors the NAIC Model Law, except clarifies that licensees have until January 1, 2023 to</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except requires notification of the state regulator within 3 business</p>	<p>Mirrors the NAIC Model Law, except expands exemptions in</p>	<p>N/A</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
Me. Rev. Stat. Ann. tit. 24-A, §§ 2261 et seq. Effective January 1, 2022	comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by April 15 (rather than February 15).		days (rather than 72 hours) of a determination that a cybersecurity event has occurred.	the NAIC Model Law to include those with ISPs in accordance with HIPAA and GLBA, provided that a certification of compliance can be submitted, upon request.	
Maryland Md. Ins. Code § 4-406(b); Md. Bus. Code § 14-3504; Bulletin 19-14			<u>Does not mirror the NAIC Model Law.</u> Requires carriers to notify the state regulator within 45 days of determining that a breach occurred if the carrier: <ul style="list-style-type: none"> • Conducts an investigation required under the state’s data breach notification law; <u>and</u> • Determines that the breach creates a likelihood that personal information has been or will be misused. 		
Massachusetts					
Michigan Mich. Code Ann. §§ 553 et seq.	Mirrors the NAIC Model Law, except sets two state-specific deadlines: <ul style="list-style-type: none"> • Gives licensees until January 20, 2022 to develop, implement, and maintain an ISP. 	Mirrors the NAIC Model Law, except does <u>not</u> contain language governing how a licensee should respond if they learn that a cybersecurity	Mirrors the NAIC Model Law, except: <ul style="list-style-type: none"> • Requires notification of the state regulator within 10 business days (rather than 72 hours) of a determination that 	Expands exemptions in the NAIC Model Law to include those with fewer than 25 employees (rather than 10).	Clarifies that a cybersecurity event will <u>not</u> be deemed to have occurred in the event of unauthorized

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p>Effective January 20, 2021</p>	<ul style="list-style-type: none"> Gives licensees until January 20, 2023 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. 	<p>event has occurred in a system maintained by a TPSP.</p>	<p>a cybersecurity event has occurred.</p> <ul style="list-style-type: none"> Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Michigan and the cybersecurity event has a reasonable likelihood of materially harming consumers or the licensee’s normal operations). Imposes industry-specific requirements governing notification to consumers (e.g., dictates appropriate forms of notice). 		<p>access by a person who acted in good faith and the access was related to the person’s activities.</p>
<p>Minnesota</p> <p>Minn. Stat. §§ 60A.9851 et seq.</p> <p>Effective August 1, 2021</p>	<p>Mirrors the NAIC Model Law, except sets two state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until August 1, 2022 to develop, implement, and maintain an ISP. Gives licensees until August 1, 2023 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. <p>Like the NAIC Model Law, requires annual certification to the state regulator, but such</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except expands exemptions to include those with:</p> <ul style="list-style-type: none"> Fewer than 25 employees. ISPs in accordance with HIPAA and GLBA, provided that a certification of compliance can be submitted, upon request. 	<p>N/A</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	certification must be submitted by April 15 (rather than February 15).				
<i>Mississippi</i> Miss. Stat. §§ 83-5801 et seq.	Mirrors the NAIC Model Law, except does <u>not</u> require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.	MIRRORS NAIC MODEL LAW	Mirrors the NAIC Model Law, except: <ul style="list-style-type: none"> • Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Mississippi <u>and</u> the cybersecurity event has a reasonable likelihood of materially harming consumers residing in Mississippi or the licensee’s normal operations). 	Expands exemptions in the NAIC Model Law to include those with: <ul style="list-style-type: none"> • Fewer than 50 employees (rather than 10). • Less than \$5 million in gross annual revenue. • Less than \$10 million in year-end total assets. • Producer and adjuster licenses from the ISP requirements and the investigation and notice requirements (but only to the extent they concern cybersecurity events at TPSPs). <p>Exempts licensees affiliated with a depository institution that maintains an ISP in accordance with GLBA from the ISP requirements.</p>	N/A
<i>Missouri</i>					
<i>Montana</i>					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<i>Nebraska</i>					
<i>Nevada</i>					
<p><i>New Hampshire</i></p> <p>N.H. Rev. Stat. §§ 420-P:1 et seq.</p>	<p>Mirrors the NAIC Model Law, except does <u>not</u> require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.</p> <p>Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by March 1 (rather than February 15).</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except:</p> <ul style="list-style-type: none"> Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in New Hampshire <u>and</u> the cybersecurity event has a reasonable likelihood of materially harming consumers residing in New Hampshire or the licensee’s normal operations). 	<p>Expands exemptions in the NAIC Model Law to include:</p> <ul style="list-style-type: none"> Licensees with fewer than 20 employees (rather than 10). Licensees operating in compliance with New York’s cybersecurity regulation. Continuing care retirement communities. Life settlement providers. Licensees that are banks or credit unions <u>and</u> that maintain an ISP in accordance with GLBA. Motor vehicle retail sellers/sales finance company. “Vendors” engaged in the sale of portable electronics insurance. 	<p>Unlike the NAIC Model Law, does <u>not</u> include in the definition of “nonpublic information” “business related information” the tampering of which would cause a material adverse impact to the licensee.</p>
<i>New Jersey</i>					
<i>New Mexico</i>					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p><i>New York</i></p> <p>23 NYCCR 500</p> <p><i>Note, the New York rules pre-date the NAIC Model Law</i></p>	<p>Requires implementation of a “Cybersecurity Program” and dictates its “core cybersecurity functions” (e.g., identifying and assessing internal and external cybersecurity risks, using defensive infrastructure to protect the licensee’s information systems, detecting cybersecurity events, etc.).</p> <p>Requires implementation and maintenance of a written “Cybersecurity Policy” based on the licensee’s risk assessment that addresses information security, data governance and classification, asset inventory and device management, etc.</p> <p>Like the NAIC Model Law, requires the Cybersecurity Program to:</p> <ul style="list-style-type: none"> • Be based on a risk assessment. • Include continuous monitoring, penetration testing, or vulnerability assessments; include audit trails designed to detect and respond to cybersecurity events; limit access privileges; address the secure disposal of information, etc. 	<p>N/A</p>	<p>Requires notification of the state regulator within 72 hours of a determination that a cybersecurity event has occurred that is either:</p> <ul style="list-style-type: none"> • A cybersecurity event impacting the licensee for which notice is required to be provided to any government, self-regulatory agency, or other supervisory body; <u>or</u> • A cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operations of the licensee. 	<p>Offers several exemptions (to varying sections) for:</p> <ul style="list-style-type: none"> • Licensees with fewer than 10 employees <u>located in New York</u>. • Licensees with less than \$5 million in gross annual revenue <u>in each of the last three fiscal years from New York business operations</u>. • Licensees with less than \$10 million in year-end total assets. • Employees, agents, representatives or designees of licensees. • Licensees that do not directly/indirectly operate, maintain, utilize, or control any information systems. • Licensees that do not directly/indirectly control, own, access, etc. 	<p>Requires designation of a “Chief Information Security Officer” to oversee and implement the Cybersecurity Program, report annually to the licensee’s board of directors, etc.</p> <p>Requires the licensee to utilize qualified cybersecurity personnel to manage their cybersecurity risks/oversee the core cybersecurity functions.</p> <p>Unlike the NAIC Model Law, provides for specific requirements concerning TPSP security policies.</p>

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	<ul style="list-style-type: none"> Establish a written incident response plan. Submit an annual certification to the state regulator by February 15. <p>Unlike the NAIC Model Law, requires the Cybersecurity Program to include written procedures, guidelines, etc. to ensure the use of secure development practices for in-house developed applications.</p>			<p>nonpublic information.</p> <p>Requires licensees that qualify for exemptions to file a Notice of Exemption.</p>	
<i>North Carolina</i>					
<p><i>North Dakota</i></p> <p>N.D. Cent. Code Ann. §§ 26.1-02.2-01 et seq.</p> <p>Effective August 1, 2021</p>	<p>Mirrors the NAIC Model Law, except sets three state-specific deadlines:</p> <ul style="list-style-type: none"> Gives licensees until August 1, 2022 to develop, implement, and maintain an ISP. Gives licensees with less than 50 employees until August 1, 2022 to develop, implement, and maintain an ISP. Gives licensees until August 1, 2023 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. <p>Like the NAIC Model Law, requires annual certification to</p>	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	<p>Mirrors the NAIC Model Law, except expands exemptions to include those with:</p> <ul style="list-style-type: none"> Between August 1, 2021 and July 31, 2023, fewer than 50 employees. After July 31, 2023, fewer than 25 employees. Less than \$5 million gross revenue. Less than \$10 million in year-end assets. ISPs in accordance with HIPAA, provided that a 	N/A

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	the state regulator, but such certification must be submitted by April 15 (rather than February 15).			certification of compliance can be submitted, upon request.	
Ohio Ohio Rev. Stat. §§ 3965.01 et seq.	<p>With respect to the annual certification, permits an insurer domiciled in Ohio and licensed exclusively to conduct business in Ohio (and no other state) to submit a written statement to the state regulator certifying that the insurer is in compliance with the ISP requirements as part of their corporate governance annual disclosure.</p> <p>Provides that a licensee that is compliant with the ISP requirements will be deemed to have implemented a cybersecurity program that “reasonably conforms to an industry-recognized cybersecurity framework” for the purposes of the state’s Uniform Commercial Code.</p>	MIRRORS NAIC MODEL LAW	<p>Mirrors the NAIC Model Law, except requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.</p> <p>Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Ohio <u>and</u> the cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the license).</p>	<p>Mirrors the NAIC Model Law, except expands exemptions to include those with:</p> <ul style="list-style-type: none"> • Fewer than 20 employees (rather than 10). • Less than \$5 million in gross annual revenue. • Less than \$10 million in year-end total assets. • ISPs in accordance with GLBA. 	Entitles compliant licensees to an affirmative defense to any tort action that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information.
Oklahoma					
Oregon					
Pennsylvania					
Rhode Island					
South Carolina	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	N/A

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
S.C. Code Ann. §§ 38-99-10 et seq.					
<i>South Dakota</i>					
Tennessee Tenn. Code Ann. §§ 56-2-1003 et seq. Effective July 1, 2021	Mirrors the NAIC Model Law, except sets three state-specific deadlines: <ul style="list-style-type: none"> • Gives licensees until July 1, 2022 to develop, implement, and maintain an ISP. • Gives licensees until July 1, 2023 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. Mirrors the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by April 15 (rather than February 15).	MIRRORS NAIC MODEL LAW	Mirrors the NAIC Model Law, except requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.	Mirrors the NAIC Model Law, except expands exemptions to include those with: <ul style="list-style-type: none"> • ISPs in accordance with GLBA. • Less than 25 employees, including independent contractors. • Less than \$5 million in gross annual revenue. • Less than \$10 million in year-end total assets. 	N/A
<i>Texas</i>					
<i>Utah</i>					
<i>Vermont</i>					
Virginia Va. Code Ann. §§ 38.2-621 et seq.	Deviates from the NAIC Model Law in that it does <u>not</u> require the licensee to undertake certain steps with respect to the risk assessment (e.g., does <u>not</u> require identification of reasonably foreseeable internal or external threats; assessment of	MIRRORS NAIC MODEL LAW	Mirrors the NAIC Model Law, except requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.	Mirrors the NAIC Model Law, except expands exemptions to include those with ISPs in accordance with GLBA and does <u>not</u> include an exemption for small businesses	Includes within the definition of “non-public information” a consumers’ passport number or military

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	<p>the likelihood and potential damage of the threats; assessment of the sufficiency of policies, procedures, and other safeguards in place to manage these threats, etc.).</p> <p>Does <u>not</u> permit the licensee to determine which security measures to implement (i.e., mandates specific security measures, rather than enumerating several options).</p> <p>Sets two state-specific deadlines:</p> <ul style="list-style-type: none"> • Gives licensees until January 1, 2023 to comply with the annual certification requirement. • Gives licensees until July 1, 2022 to comply with the requirements relating to a licensee’s due diligence and oversight of TPSPs. 		<p>Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Virginia <u>and</u> “the cybersecurity event meets threshold and other requirements prescribed by the Commissioner”; does <u>not</u> require the cybersecurity event to have a reasonable likelihood of materially harming consumers or the licensee’s normal operations).</p> <p>Imposes industry-specific requirements governing notification to consumers (e.g., dictates appropriate forms of notice).</p>	(i.e., those with fewer than 10 employees).	identification number.
<i>Washington</i>					
<i>West Virginia</i>					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
<p><i>Wisconsin</i></p> <p>Wis. Stat. Ann. §§ 601.95 et seq.</p> <p>Effective November 1, 2021</p>	<p>Mirrors the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by March 1 (rather than February 15).</p>	<p>MIRRORS NAIC MODEL LAW</p>	<p>Mirrors the NAIC Model Law, except requires that licensees notify the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.</p> <p>Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Wisconsin <u>and</u> meets certain conditions (e.g., the licensee reasonably believes that the cybersecurity event involves the nonpublic information of at least 250 consumers, etc.).</p>	<p>Mirrors NAIC Model Law, except exempts those with:</p> <ul style="list-style-type: none"> • Less than \$10 million in year-end total assets. • Less than \$5 million in gross annual revenue. • Fewer than 50 employees, including independent contractors, who work at least 30 hours a week for the licensee. 	<p>N/A</p>
<i>Wyoming</i>					

APPENDIX 1: Application of NAIC Model Law Attestation Requirements and Exceptions

- * We have drafted the below survey in response to requests from Council members for supplemental information regarding qualification as a licensee; the application of the annual certification requirements (i.e., the extent they apply to entities beyond domestic insurers); and the obligations associated with eligibility for and compliance with the exception/exemption provisions (e.g., whether filings are required for all licensees).
- * While each state has adopted a slightly nuanced approach, and the below survey outlines the varying approaches in greater detail, there are some general themes worth noting at the outset in response to the questions posed by Council members:
 - **Qualification as a Licensee.** Every state appears to have adopted the NAIC Model Law’s definition of a *licensee* (i.e., a person who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws, excluding a purchasing group or a risk retention group chartered and licensed in another state and/or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction). Though the definition of *person* varies from state-to-state, in every state it includes both an individual and an entity.
 - **Certification Requirements.** Every state requires only domestic insurers/insurers domiciled in the state to annually certify/attest that they are compliant with the ISP requirements. Few states define who qualifies as an insurer in their state’s Insurance Data Security Law; as such—to the extent possible—we have included the definition of *insurer* used throughout the state’s insurance code.
 - **Eligibility for Exceptions.** In general, the majority of states do not specifically address—in available guidance or otherwise—whether *all licensees* (even those that do qualify as insurers/do not need to submit the annual certification) are required to submit a filing that they are eligible for an exception. In such states, it is likely that—to the extent a filing is required to qualify for a given exception—such a filing is required of *all licensees*. It warrants noting, however, that most states only require an affirmative filing that a licensee qualifies for an exception if the licensee is seeking to take advantage of an exception related to compliance with *another regulatory regime* (e.g., HIPAA, GLBA, New York’s cybersecurity regulation, etc.). If a state has issued supplemental guidance providing a different interpretation (e.g., Mississippi, New Hampshire, Ohio, and South Carolina), it is noted in the below survey.
 - **Application of the Licensee-Designee Exception and Associated Certification Requirements.** One question specifically asked if there are circumstances under which a *licensee that is not an insurer* would need to file an annual certification (i.e., if an individual licensee submits qualification for an exception pointing to a business licensee’s ISP, and the business licensee otherwise qualifies for an exception, would the business licensee now need to file an attestation since the individual is operating under the business licensee’s ISP?). It does not appear as though any state specifically addresses this question in available guidance, but it seems unlikely that any state would affirmatively require non-insurers to file an annual certification (unless such a certification was otherwise required by an exception that is applicable to all licensees).
- * Given the limited guidance available, it warrants highlighting that the vast majority of states enacted their respective Insurance Data Security Laws in 2019-2021. As such, available guidance is fairly limited and—in many states—the state regulator is expected/has the authority to promulgate regulations in the coming months and/or years to implement and clarify these provisions.

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Questions	Who qualifies as a <i>licensee</i> ?	Who is required to submit an annual attestation/certification of compliance? Who qualifies as an <i>insurer</i> ?	Are licensees required to submit a filing, written statement, certification, etc. to take advantage of any of the exceptions? If an individual/entity is not required to file an annual certification, will they still be required to submit a filing describing their eligibility for an exception?	If an individual licensee submits qualification for an exception pointing to a business licensee’s ISP, and the business licensee otherwise qualifies for an exception, would the business licensee now need to file a certification since the individual is operating under the business licensee’s ISP?
Alabama Effective May 1, 2019	Applies to <i>licensees</i> , defined to include a person (i.e., an individual or a nongovernmental entity) authorized to operate; registered; <u>or</u> required to be licensed, authorized, or registered under the state insurance laws (including insurance producers and insurance companies that do not meet the size and/or revenue-related exemptions or other exemptions). Bulletin 2019-05 . Does <u>not</u> include: <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer that is 	<i>By February 15, 2021, and unless an exception applies,</i> requires <i>insurers</i> domiciled in Alabama to submit an annual written statement by February 15 certifying that they are in compliance with the statutory requirements. Ala. Code § 27-62-4(i). While Alabama’s Insurance Data Security Law does <u>not</u> define <i>insurer</i> , the state’s Insurance Code defines the term to include “every person engaged as indemnitor, surety, or contractor in the business of entering into contracts of insurance.” Ala. Code § 27-1-2(2).	<i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).</i> Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does <u>not</u> appear to require: <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Ala. Code § 27-62-9(a)(1), (3). Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with: <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits a written statement certifying compliance. Ala. Code § 27-62-9(a)(2). • GLBA, provided that the licensee produces, <u>upon request</u>, documentation that 	<i>Does not explicitly address this question in existing guidance,</i> but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	domiciled in another state or jurisdiction. Ala. Code § 27-62-3(9), (12).		independently validates the depository institution’s adoption of an ISP (<i>applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA</i>). Ala. Code § 27-62-9(a)(4).	
Connecticut Effective October 1, 2020	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual or a nongovernmental entity) authorized to operate; registered; <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Conn. Gen. Stat. § 38a-38(b)(7), (10). 	<p><i>By February 15, 2021 and unless an exception applies,</i> requires <i>domestic insurers and health care centers</i> to submit an annual written statement certifying that they are in compliance with the statutory requirements. Due to COVID-19, permits licensees that fail to file their annual certification by February 15, 2021 to file by April 15, 2021 without risk of sanctions. Bulletin IC-42.</p> <p>While Connecticut’s Insurance Data Security Law does <u>not</u> define <i>domestic insurer</i>, the state’s Insurance Code defines the term to include “any insurer [(i.e., any person or combination of persons doing any kind/form of insurance business other than a fraternal benefit society <u>and</u> includes a receiver of any insurer when the context reasonably permits)] that has been chartered by, incorporated, organized, or constituted within or under the laws of</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).</i> Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification was also required.</p> <p>Does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Conn. Gen. Stat. § 38a-38(c)(10)(A)(i), (iii). <p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • A jurisdiction approved by the Commissioner (pursuant to regulations to be adopted by the Connecticut Insurance Department), provided that the licensee submits an annual written statement certifying compliance. Conn. Gen. Stat. § 38a-38(c)(10)(A)(iv). • HIPAA, provided that the licensee submits a written statement certifying compliance. Conn. Gen. Stat. § 38a-38(c)(10)(A)(ii). 	<p><i>Does not explicitly address this question in existing guidance,</i> but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p> <p>But affirmatively requires licensees taking advantage of the exception applicable to those operating in compliance with other state laws to <u>annually</u> certify compliance. Conn. Gen. Stat. § 38a-38(c)(10)(A)(iv).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
		[Connecticut].” Conn. Gen. Stat. § 38a-1(6), (12).		
Delaware Effective July 1, 2019	Applies to <i>licensees</i> , defined to include a person (i.e., an individual, corporation, company, etc.) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws. Does <u>not</u> include: <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Del. Code tit. 18, §§ 102(11), 8603(10), (14); UA Bulletin No. 5. 	<u>Unless an exception applies</u> , requires <i>insurers</i> domiciled in Delaware to submit an annual written statement by February 15 certifying that they are in compliance with the statutory requirements. Del. Code tit. 18, § 8604(i). Defines <i>insurer</i> to include an insurer, health service corporation, managed care organization, or HMO licensed under the state’s Insurance Code. Del. Code tit. 18, § 8603(9).	<i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable)</i> . Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does <u>not</u> appear to require: <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Del. Code tit. 18, § 8609(a)(1), (3). Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA, provided that the licensee submits a written statement certifying compliance. Del. Code tit. 18, § 8609(a)(2).	<i>Does not explicitly address this question in existing guidance</i> , but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).
Hawaii Effective July 1, 2021	Applies to <i>licensees</i> , defined to include a person (i.e., an individual, corporation, company, etc.) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or	<u>Unless an exception applies</u> , requires <i>insurers</i> domiciled in Hawaii to submit an annual written statement by March 31 certifying that they are in compliance with the requirements associated with developing an ISP, conducting	Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA, provided that the licensee submits a written statement certifying compliance. Haw. Rev. Stat. Ann. § 431: -104.	<i>Does not explicitly address this question in existing guidance</i> , but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	<p>registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Haw. Rev. Stat. Ann. § 431: -101. 	<p>a risk assessment, etc. Haw. Rev. Stat. Ann. § 431: -208.</p> <p>While Hawaii’s Insurance Data Security Law does <u>not</u> define insurer, the state’s Insurance Code defines the term to include every person engaged in the business of making contracts of insurance and includes reciprocal or interinsurance exchanges.” Haw. Rev. Stat. Ann. § 431:1 -202.</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception</i>, but does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the fewer than 10 employees exemption; and • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee. Haw. Rev. Stat. Ann. § 431: -104. 	<p>certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>
<p>Indiana</p> <p>Effective July 1, 2020</p>	<p>Applies to licensees, defined to include a person (i.e., individuals, corporations, associations, etc.) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Ind. Code 	<p><u>Unless an exception applies</u>, requires insurers domiciled in Indiana to submit an annual written statement by April 15 certifying that they are in compliance with the requirements associated with developing an ISP, conducting a risk assessment, etc. Ind. Code § 27-2-27-20(c).</p> <p>While Indiana’s Insurance Data Security Law does <u>not</u> define insurer, the state’s Insurance Code defines the term to include “a company, firm, partnership, association, order, society or system making any kind of insurance,” including associations operating as</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception</i>, but does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; • <i>Licensees</i> that have established and maintain ISPs under HIPAA; • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee; or • <i>Licensees affiliated with financial institutions</i> that maintain an ISP in compliance with GLBA to submit a certification, attestation, or written statement to take advantage of the exception. Ind. Code § 27-2-27-26. 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	§§ 27-2-27-10; 27-1-2-3(h).	Lloyds, reciprocal or inter-insurers, or individual underwriters. Ind. Code § 27-1-2-3(x).		
Iowa Effective January 1, 2022	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual, corporation, company, etc.) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Iowa Code Ann. § 507F.3(13). 	<p><i>By January 1, 2023</i>, and <i>unless an exception applies</i>, requires <i>insurers</i> domiciled in Iowa to submit an annual written statement by April 15 certifying that they are in compliance with the requirements associated with developing an ISP, conducting a risk assessment, etc. Iowa Code Ann. § 507F.4(8).</p> <p>Defines insurer to mean the same as the state’s Insurance Code defines it: “a company qualified and licensed by the insurance division to transact the business of insurance in this state by certificate issued” pursuant to Iowa’s insurance laws, and does <u>not</u> include “agencies, authorities, or instrumentalities of the United States, its possessions and territories, the commonwealth of Puerto Rico, the District of Columbia, or a state or political subdivision of a state.” Iowa Code Ann. §§ 507F.3(12); 521A.1(8).</p>	<p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA, provided that the licensee submits a written statement certifying compliance.</p> <p><i>Does not address whether a licensee that is not required to attest will still need to file an exception</i>, but does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; or • <i>Licensees affiliated with financial institutions</i> that maintain an ISP in compliance with GLBA to submit a certification, attestation, or written statement to take advantage of the exception. Iowa Code Ann. § 507F.13. 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
<p>Louisiana</p> <p>Effective August 1, 2021</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., any natural person or nongovernmental juridical person) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Cybersecurity Guidance.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. La. Rev. Stat. § 22:2503(7), (10). 	<p><i>By February 15, 2022</i>, and <u>unless an exception applies</u>, requires <i>insurers</i> domiciled in Louisiana to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. La. Rev. Stat. § 22:2504(I)(1).</p> <p>While Louisiana’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include “every person engaged in the business of making contracts of insurance, other than a fraternal benefit society,” including a reciprocal, insurance exchange, insurance exchange syndicate, a Lloyds organization, HMOs (for specific purposes), etc. La. Rev. Stat. § 22:46(10).</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable)</i>. Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed.</p> <p>Does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. La. Rev. Stat. § 22:2509(A)(1)-(3), (5). <p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits, <u>upon request</u>, a written statement certifying compliance. La. Rev. Stat. § 22:2509(A)(4). • GLBA, provided that the licensee produces, <u>upon request</u>, documentation that independently validates the depository institution’s adoption of an ISP (<i>applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA</i>). La. Rev. Stat. § 22:2509(A)(6). • A jurisdiction approved by the Commissioner, provided that the licensee submits a written statement certifying compliance. La. Rev. Stat. § 22:2509(A)(7). 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
<p>Maine</p> <p>Effective January 1, 2022</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual, corporation, company, etc.) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Me. Rev. Stat. Ann. tit. 24-A, §§ 2263. 	<p>By January 1, 2023 and <u>unless an exception applies</u>, requires <i>insurance carriers</i> domiciled in Maine to submit an annual written statement by April 15 certifying that they are in compliance with the ISP requirements. Me. Rev. Stat. Ann. tit. 24-A, § 2264(9).</p> <p>Defines insurance carrier to mean the same as the state’s Insurance Code defines it:</p> <ul style="list-style-type: none"> • “Any person or entity required to be licensed by the superintendent to assume risk, including without limitation an insurer, nonprofit hospital, medical or health care service organization, health maintenance organization or multiple-employer welfare arrangement; • A self-funded plan subject to state regulation; • A preferred provider arrangement administrator; or • A TPA that provides administrative services for an entity that is not a carrier.” Me. Rev. Stat. tit. 24-A, §§ 2263(7), 2204(15). 	<p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA, provided that the licensee submits an <u>annual</u> written statement certifying compliance.</p> <p><i>Does <u>not</u> address whether a licensee that is not required to attest will still need to file an exception</i>, but does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee; or • <i>Licensees affiliated with financial institutions</i> that maintain an ISP in compliance with GLBA to submit a certification, attestation, or written statement to take advantage of the exception. Me. Rev. Stat. tit. 24-A, § 2269. 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Michigan Effective January 20, 2021	<p>Applies to <i>licensees</i>, defined to include a licensed insurer, producer, and other persons licensed, authorized, or registered <u>or</u> holding or required to hold a certificate of authority under the state’s insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Mich. Comp. L. Ann. § 500.553(g). 	<p><i>By February 15, 2022</i>, and <i>unless an exception applies</i>, requires <i>insurers</i> domiciled in Michigan to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Mich. Comp. L. Ann. § 500.555(9).</p> <p>While Michigan’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include an individual, corporation, inter-insurer, Lloyds organization, etc., engaged/attempting to engage in the business of making insurance or surety contracts. Mich. Comp. L. Ann. § 500.106.</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable)</i>. Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed.</p> <p>Does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of another licensee; or • <i>Licensees</i> that have established and maintain an ISP in compliance with HIPAA. <p>to submit a certification, attestation, or written statement to take advantage of the exception. Mich. Comp. L. Ann. § 500.565(1)-(3).</p>	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>
Minnesota Effective August 1, 2021	<p>Applies to <i>licensees</i>, defined to include any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered under the state’s insurance laws. Minn. Stat. Ann. § 60A.985(8).</p>	<p><i>By August 1, 2022</i>, and <i>unless an exception applies</i>, requires <i>insurers</i> domiciled in Minnesota to submit an annual written statement by April 15 certifying that they are in compliance with the ISP requirements. Minn. Stat. Ann. § 60A.9851(9).</p> <p>While Minnesota’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s</p>	<p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits, <u>upon request</u>, a written statement certifying compliance. • GLBA, provided that the licensee produces, <u>upon request</u>, documentation that independently validates the depository institution’s adoption of an ISP (<i>applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA</i>). Minn. Stat. Ann. § 60A.9856. 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
		<p>Insurance Code defines the term to include “every insurer, corporation, business trust, or association engaged in insurance as principal, but for purposes of this subdivision does not include a political subdivision providing self-insurance or establishing a [joint] pool under” Minnesota’s insurance laws. Minn. Stat. Ann. § 60A.02(4).</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception</i>, but does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of another licensee. Minn. Stat. Ann. § 60A.9856. 	<p>other things—the certification provisions).</p>
<p>Mississippi Effective July 1, 2019</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., any natural person or nongovernmental juridical person) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Miss. Code Ann. § 83-5-805. 	<p><u><i>Unless an exception applies</i></u>, requires <i>insurers</i> domiciled in Mississippi to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Miss. Code Ann. § 83-5-807(9); Bulletin 2019-4; Mississippi Cybersecurity Law Guidance; Mississippi Insurance Data Security Law ISP Certification Form.</p> <p>While Mississippi’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include “those companies subject to the jurisdiction of the commissioner” (i.e., all indemnity or guaranty companies, all companies,</p>	<p><u><i>Per guidance from the Mississippi Insurance Department, only requires licensees who are insurers and have an NAIC # to complete the exception certification form.</i></u> Mississippi Cybersecurity Law Guidance.</p> <p>Generally, does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee; or • <i>Insurance producers and adjusters</i> to—among other things—submit a certification, attestation, or written statement to take advantage of the exception. Miss. Code Ann. § 83-5-817(a), (c). But indicates via guidance that <i>licensees who are insurers and have an NAIC #</i> are required to complete an exception certification form, even for these exceptions. Mississippi Cybersecurity Law Guidance. 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements. Mississippi Insurance Data Security Law ISP Certification Form.</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
		<p>corporations, etc. transacting the business of insurance in this state). Miss. Code Ann. §§ 83-5-1, 83-6-1(e).</p>	<p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits a written statement certifying compliance. Miss. Code Ann. § 83-5-817(b). • GLBA, provided that the licensee produces, <u>upon request</u>, documentation that independently validates the depository institution’s adoption of an ISP (<i>applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA</i>). Miss. Code Ann. § 83-5-817(d). 	
<p>New Hampshire</p> <p>Effective January 1, 2020</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual or non-governmental entity) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. N.H. Rev. Stat. § 420-P:3(IX), (XII). 	<p><i>Per guidance from the New Hampshire Insurance Department, does <u>not</u> require licensees—other than domestic insurers—to submit the annual attestations or otherwise certify compliance with the ISP requirements</i> (unless required by an exception/safe harbor). Docket No. INS 20-013-AB.</p> <p><i><u>Unless an exception/safe harbor applies</u></i>, requires <i>insurers</i> domiciled in New Hampshire to submit an annual written statement by March 1 certifying that they are in compliance with the ISP requirements. N.H. Rev. Stat. § 420-P:4(IX); Docket No. INS 20-013-AB; Bulletin INS-20-001-AB; New Hampshire</p>	<p><i>Per guidance from the New Hampshire Insurance Department, outlines circumstances in which other licensees (i.e., entities that are not insurers/not required to file an annual attestation) will be required to complete an exception certification form.</i> To the extent a licensee qualifies for a safe harbor (i.e., compliance with HIPAA or New York cybersecurity regulations), requires licensees that are not domestic insurers to submit the exception certification form <i>only once</i> by March 1, 2021. Docket No. INS 20-013-AB; New Hampshire Insurance Data Security Law Exception Certification Form.</p> <p>For insurers who qualify for a safe harbor (i.e., are compliant with HIPAA or New York cybersecurity regulations), permits submission of the exception certification form in place of the ISP certification form annually by March 1. Docket No. INS 20-013-AB; New Hampshire Insurance Data Security Law Exception Certification Form.</p> <p>In general, does <u>not</u> appear to require:</p>	<p><i>Does <u>not</u> explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements under any circumstances (e.g., the exception certification form is only required to be filed by all other licensees <i>once</i> by March 1, 2021; domestic insurers are the only entities required to certify compliance with the ISP requirements either via an annual certification or the exception certification). Docket No. INS 20-013-AB.</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
		<p>Insurance Data Security Law ISP Certification Form (indicates application to domestic insurers).</p>	<ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee; or • <i>Continuing care retirement communities;</i> • <i>Life settlement providers;</i> • <i>Licensees</i> that are bank or credit unions that are compliant with GLBA; • <i>Motor vehicle retail sellers or motor vehicle sales finance companies;</i> or • <i>A portable electronics vendor</i> to submit a certification, attestation, or written statement to take advantage of the exception. N.H. Rev. Stat. § 420-P:9 (exceptions). <p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits a written statement certifying compliance (<i>extends protections to the extent that a licensee maintains other nonpublic information in the same manner as PHI, provided that the licensee submits a written statement that it does maintain and protect other nonpublic information as it does PHI</i>). N.H. Rev. Stat. § 420-P:10 (safe harbor). • New York’s cybersecurity regulations, provided that the licensee submits a written statement certifying compliance. N.H. Rev. Stat. § 420-P:11 (safe harbor). 	
North Dakota	Applies to <i>licensees</i> , defined to include a	<i>By August 1, 2022</i> , and <i>unless an exception applies</i> , requires	Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have	<i>Does not explicitly address this question in</i>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
<p>Effective August 1, 2021</p>	<p>licensed insurer, producer, and other persons licensed, authorized, or registered <u>or</u> holding or required to hold a certificate of authority under the state’s insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. N.D. Cent. Code Ann. § 26.1-02.2-01. 	<p><i>insurers</i> domiciled in North Dakota to submit an annual written statement by April 15 certifying that they are in compliance with the requirements associated with developing an ISP, conducting a risk assessment, etc. N.D. Cent. Code Ann. §§ 26.1-02.2-03(10), 26.1-02.2-11.</p> <p>While North Dakota’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include “any corporation, association, benefit society, exchange, partnership, or individual engaged as principal in the business of insurance.” N.D. Cent. Code Ann. § 26.1-02-01(4).</p>	<p>established and maintain an ISP in compliance with HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH Act). N.D. Cent. Code Ann. § 26.1-02.2-08.</p> <p><i>Does <u>not</u> address whether a licensee that is not required to attest will still need to file an exception, but does <u>not</u> appear to require:</i></p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of another licensee. N.D. Cent. Code Ann. § 26.1-02.2-08. 	<p><i>existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>
<p>Ohio</p> <p>Effective March 20, 2019</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual or business entity) who is licensed, authorized to operate, registered <u>or</u> required to be licensed, authorized, or registered under the state insurance laws.</p>		<p>In general, does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size and/or revenue-related exemptions; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exemption. Ohio Rev. Code § 3965.07(A), (C). <p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with</p> 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (e.g., domestic insurers are the only entities required to file an ISP certification statement or</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	<p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Ohio Rev. Code § 3965.01(M). 		<p>HIPAA’s privacy and security rules, provided that the licensee submits a written statement certifying compliance. Ohio Rev. Code § 3965.07(B); HIPAA Compliance Certification Statement. <i>Note, per guidance from the Ohio Department of Insurance, this certification statement is only required of domestic insurers.</i> ODI ISP Certification Notice of Exemption.</p> <p><i>Additional information on the remaining exemption statuses and their application is forthcoming.</i> Statement of Compliance with HIPAA Privacy & Security Rules Guidance Document.</p>	<p>notice of exemption). FAQs.</p>
<p>South Carolina</p> <p>Effective January 1, 2019</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual or business entity) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Bulletin No. 2018-02.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or 	<p><u><i>Unless an exception applies</i></u>, requires <i>insurers</i> domiciled in South Carolina to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. S.C. Code § 38-99-20(I). Clarifies that such domestic insurers will be contacted directly by the Financial Regulation & Solvency Division with further instructions. SCDOI Cybersecurity Portal.</p> <p>While South Carolina’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include a corporation, fraternal organization, individual, etc.</p>	<p><i>Per guidance from the South Carolina Department of Insurance, does <u>not</u> require licensees to proactively communicate their exemption status, though the Department may conduct random inspections to determine compliance.</i> Bulletin No. 2018-12. Separately, suggests that—to take advantage of the exemptions applicable to entities compliant with HIPAA or the New York cybersecurity regulations—annual certification is required. SCDOI Presentation on Complying with the South Carolina Insurance Data Security Act. Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed.</p> <p>In general, does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • <i>Licensees</i> that qualify for the size-related exemption; or • <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee 	<p><i>Does <u>not</u> explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	jurisdiction. S.C. Code § 38-99-10(9).	engaging/attempting to engage as principals in any kind of insurance or surety business. <i>See</i> S.C. Code § 38-1-20(33).	to submit a certification, attestation, or written statement to take advantage of the exception. S.C. Code § 38-1-70(A)(1)-(2). Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with: <ul style="list-style-type: none"> HIPAA, provided that the licensee submits a written statement certifying compliance. S.C. Code § 38-1-70(A)(3). New York’s cybersecurity regulation, provided that the licensee submits a written statement certifying its compliance. Bulletin No. 2018-12 .	
Tennessee Effective July 1, 2021	Applies to <i>licensees</i> , defined to include a licensed insurer, producer, and other persons licensed, authorized, or registered <u>or</u> holding or required to hold a certificate of authority under the state’s insurance laws. Does <u>not</u> include: <ul style="list-style-type: none"> A purchasing group or a risk retention group chartered and licensed in another state. A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Tenn. Code Ann. § 56-2-1003(10). 	<i>By July 1, 2022, and <u>unless an exception applies</u>, requires insurers</i> domiciled in Tennessee to submit an annual written statement by April 15 certifying that they are in compliance with the ISP requirements. While Tennessee’s Insurance Data Security Law does not define insurer, the state’s Insurance Code defines the term to include “all corporations, associations, partnerships, or individuals engaged as principals in the business of insurance.” Tenn. Code Ann. § 56-1-102(2).	Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA, HITECH Act, and/or GLBA, and submits a written statement certifying its compliance with such acts. Tenn. Code Ann. § 56-2-1009(a)(2), (3). <i>Does <u>not</u> address whether a licensee that is not required to attest will still need to file an exception</i> , but does <u>not</u> appear to require: <ul style="list-style-type: none"> <i>Licensees</i> that qualify for the size-related exemptions; or <i>Employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of another licensee. Tenn. Code Ann. § 56-2-1009(a)(1), (4). 	<i>Does <u>not</u> explicitly address this question in existing guidance</i> , but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
<p>Virginia</p> <p>Effective July 1, 2020</p>	<p>Applies to <i>licensees</i>, defined to include a person (i.e., an individual or business entity) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws.</p> <p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Va. Code Ann. § 38.2-621. 	<p><i>Beginning in 2023</i>, and <i>unless an exception applies</i>, requires <i>insurers</i> domiciled in Virginia to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Va. Code Ann. § 38.2-623(H). Clarifies that such domestic insurers will be contacted directly by the Financial Regulation & Solvency Division with further instructions. SCC Cybersecurity Portal.</p> <p>While Virginia’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include “any company engaged in the business of making contracts of insurance.” Va. Code Ann. § 38.2-100.</p>	<p><i>Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable)</i>. Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed.</p> <p>Does <u>not</u> appear to require <i>employees, agents, representatives, or designees of a licensee that are also licensees</i> that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Va. Code Ann. § 38.2-629(A)(2).</p> <p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • HIPAA, provided that the licensee submits a written statement certifying compliance. Va. Code Ann. § 38.2-629(A)(1). • GLBA, provided that the licensee produces, <u>upon request</u>, documentation that independently validates the depository institution’s adoption of an ISP (<i>applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA</i>). Va. Code Ann. § 38.2-629(A)(3). 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).</p>
<p>Wisconsin</p> <p>Effective November 1, 2021</p>	<p>Applies to <i>licensees</i> defined to include a person licensed, authorized, or registered, or a person required to be licensed, authorized, or registered under the state insurance laws.</p>	<p><i>Beginning in 2023</i>, and <i>unless an exception applies</i>, requires <i>insurers</i> domiciled in Wisconsin to submit an annual written statement by March 1 certifying that they are in compliance with the ISP</p>	<p>Deems <i>licensees</i> to have met the requirements of the state’s Insurance Data Security Law if they have established and maintain an ISP in compliance with:</p> <ul style="list-style-type: none"> • Farm Credit Act, Financial Industry Regulatory Authority (FINRA), or Gramm-Leach-Bliley Act (GLBA), provided that the licensee produces, upon request, documentation that independently validates their compliance; or 	<p><i>Does not explicitly address this question in existing guidance</i>, but appears unlikely that an entity that does <u>not</u> otherwise qualify as an insurer would need to comply with the annual</p>

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	<p>Does <u>not</u> include:</p> <ul style="list-style-type: none"> • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Wis. Stat. Ann. § 601.95 (7). 	<p>requirements. Wis. Stat. Ann. § 601.952(8).</p> <p>While Wisconsin’s Insurance Data Security Law does <u>not</u> define <i>insurer</i>, the state’s Insurance Code defines the term to include “any person or association of persons doing an insurance business as a principal, and includes, but is not limited to, fraternal, cooperative associations, insurers operating under [school benefit plans], and risk retention groups.” Insurer also includes “any person purporting or intending to do an insurance business as a principal on his or her own account.” Insurer does <u>not</u> include “a person that issues only qualified charitable gift annuities.” Wis. Stat. Ann. § 600.03(27).</p>	<ul style="list-style-type: none"> • HIPAA, if the licensee maintains nonpublic information in the same manner as protected health information. Wis. Stat. Ann. § 601.951(2). <p>Does <u>not</u> appear to require:</p> <ul style="list-style-type: none"> • Licensees that qualify for the size and/or revenue-related exemptions; or • Employees, agents, representatives, or designees of a licensee that are also licensees that are covered by the ISP of another licensee to submit a certification, attestation, or written statement to take advantage of the exception. Wis. Stat. Ann. § 601.952(9). 	<p>certification requirements. Bulletin.</p>