FIRST ENGROSSMENT

Sixty-seventh Legislative Assembly of North Dakota

ENGROSSED SENATE BILL NO. 2075

Introduced by

Industry, Business and Labor Committee

(At the request of the Insurance Commissioner)

- 1 A BILL for an Act to create and enact chapter 26.1-02.2 of the North Dakota Century Code,
- 2 relating to insurance data and security; and to provide for a legislative management study.

3 BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

4 **SECTION 1.** Chapter 26.1-02.2 of the North Dakota Century Code is created and enacted

5 as follows:

6 <u>26.1-02.2-01 Definitions.</u>

7 <u>As used in this chapter:</u>

8 <u>1.</u> "Authorized individual" means an individual known to and screened by the licensee
 9 and determined to be necessary and appropriate to have access to the nonpublic

10 information held by the licensee and the licensee's information systems.

- 11 <u>2.</u> <u>"Commissioner" means the insurance commissioner.</u>
- 12 <u>3.</u> <u>"Consumer" means an individual, including an applicant, policyholder, insured,</u>
- beneficiary, claimant, and certificate holder, who is a resident of this state and whose
 nonpublic information is in a licensee's possession, custody, or control.
- 15 <u>4.</u> <u>"Cybersecurity event" means an event resulting in unauthorized access to, disruption,</u>
- 16 <u>or misuse of, an information system or nonpublic information stored on the information</u>
 17 <u>system. The term does not include:</u>
- 18 <u>a.</u> The unauthorized acquisition of encrypted nonpublic information if the encryption,
 19 <u>process, or key is not also acquired, released, or used without authorization; or</u>
- 20b.An event the licensee has determined that the nonpublic information accessed by21an unauthorized person has not been used or released and has been returned or22destroyed.
- 23 <u>5.</u> "Department" means the insurance department.

1	<u>6.</u>	"Encrypted" means the transformation of data into a form that results in a low
2		probability of assigning meaning without the use of a protective process or key.
3	<u>7.</u>	"Information security program" means the administrative, technical, and physical
4		safeguards a licensee uses to access, collect, distribute, process, protect, store, use,
5		transmit, dispose of, or otherwise handle nonpublic information.
6	<u>8.</u>	"Information system" means a discrete set of electronic information resources
7		organized for the collection, processing, maintenance, use, sharing, dissemination, or
8		disposition of electronic nonpublic information, as well as any specialized system,
9		including industrial or process controls systems, telephone switching, private branch
10		exchange systems, and environmental control systems.
11	<u>9.</u>	"Licensee" means any person licensed, authorized to operate, registered, or required
12		to be licensed, authorized, or registered pursuant to the insurance laws of this state.
13		The term does not include a purchasing group or a risk retention group chartered and
14		licensed in another state or a licensee that is acting as an assuming insurer that is
15		domiciled in another state or jurisdiction.
16	<u>10.</u>	"Multi-factor authentication" means authentication through verification of at least two of
17		the following types of authentication factors:
18		a. Knowledge factors, including a password;
19		b. Possession factors, including a token or text message on a mobile phone; or
20		c. Inherence factors, including a biometric characteristic.
21	<u>11.</u>	"Nonpublic information" means electronic information that is not publicly available
22		information and is:
23		a. Any information concerning a consumer which can be used to identify the
24		consumer because of name, number, personal mark, or other identifier in
25		combination with any one or more of the following data elements:
26		(1) Social security number;
27		(2) Driver's license number or nondriver identification card number;
28		(3) Financial account number or credit or debit card number;
29		(4) Any security code, access code, or password that would permit access to a
30		consumer's financial account; or
31		(5) Biometric records.

1		b. Any information or data, except age or gender, in any form or medium created by
2		or derived from a health care provider or a consumer which can be used to
3		identify a particular consumer and relates to:
4		(1) The past, present, or future physical, mental, or behavioral health or
5		condition of any consumer or a member of the consumer's family;
6		(2) The provision of health care to any consumer; or
7		(3) Payment for the provision of health care to any consumer.
8	<u>12.</u>	"Person" means any individual or any nongovernmental entity, including any
9		nongovernmental partnership, corporation, branch, agency, or association.
10	<u>13.</u>	"Publicly available information" means any information a licensee has a reasonable
11		basis to believe is lawfully made available to the general public from: federal, state, or
12		local government records; widely distributed media; or disclosures to the general
13		public which are required to be made by federal, state, or local law. A licensee has a
14		reasonable basis to believe that information is lawfully made available to the general
15		public if the licensee has taken steps to determine:
16		a. The information is of the type available to the general public; and
17		b. Whether a consumer can direct the information not be made available to the
18		general public and, if so, that the consumer has not done so.
19	<u>14.</u>	"Risk assessment" means the risk assessment that each licensee is required to
20		conduct under section 26.1-02.2-03.
21	<u>15.</u>	"Third-party service provider" means a person, not otherwise defined as a licensee,
22		that contracts with a licensee to maintain, process, store, or otherwise is permitted
23		access to nonpublic information through its provision of services to the licensee.
24	<u>26.1</u>	-02.2-02. Exclusive regulation.
25	Notv	vithstanding any other provision of law, this chapter establishes the exclusive state
26	standard	Is applicable to licensees for data security, the investigation of a cybersecurity event,
27	and notif	ication to the commissioner.
28	<u>26.1</u>	-02.2-03. Information security program.
29	<u>1.</u>	Commensurate with the size and complexity of the licensee, the nature and scope of
30		the licensee's activities, including the licensee's use of third-party service providers,
31		and the sensitivity of the nonpublic information used by the licensee or in the

	U		-					
1		lice	nsee's possession, custody, or control, each licensee shall develop, implement,					
2		and	I maintain a comprehensive written information security program based on the					
3		lice	icensee's risk assessment that contains administrative, technical, and physical					
4		<u>safe</u>	safeguards for the protection of nonpublic information and the licensee's information					
5		<u>sys</u>	tem.					
6	<u>2.</u>	<u>A lic</u>	censee's information security program must be designed to:					
7		<u>a.</u>	Protect the security and confidentiality of nonpublic information and the security					
8			of the information system;					
9		<u>b.</u>	Protect against any threats or hazards to the security or integrity of nonpublic					
10			information and the information system;					
11		<u>C.</u>	Protect against unauthorized access to or use of nonpublic information, and					
12			minimize the likelihood of harm to any consumer; and					
13		<u>d.</u>	Define and periodically re-evaluate a schedule for retention of nonpublic					
14			information and a mechanism for destruction if no longer needed.					
15	<u>3.</u>	The	e licensee shall:					
16		<u>a.</u>	Designate one or more employees, an affiliate, or an outside vendor designated					
17			to act on behalf of the licensee which is responsible for the information security					
18			program;					
19		<u>b.</u>	Identify reasonably foreseeable internal or external threats that could result in					
20			unauthorized access, transmission, disclosure, misuse, alteration, or destruction					
21			of nonpublic information, including the security of information systems and					
22			nonpublic information accessible to, or held by, third-party service providers;					
23		<u>C.</u>	Assess the likelihood and potential damage of any threats, taking into					
24			consideration the sensitivity of the nonpublic information;					
25		<u>d.</u>	Assess the sufficiency of policies, procedures, information systems, and other					
26			safeguards in place to manage any threats, including consideration of threats in					
27			each relevant area of the licensee's operations, including:					
28			(1) Employee training and management;					
29			(2) Information systems, including network and software design, as well as					
30			information classification, governance, processing, storage, transmission,					
31			and disposal; and					

1			<u>(3)</u>	Detecting, preventing, and responding to attacks, intrusions, or other
2				systems failures; and
3		<u>e.</u>	<u>Imp</u>	lement information safeguards to manage the threats identified in the
4			licer	nsee's ongoing assessment and assess the effectiveness of the safeguards'
5			<u>key</u>	controls, systems, and procedures on an annual basis.
6	<u>4.</u>	Bas	sed or	n the licensee's risk assessment, the licensee shall:
7		<u>a.</u>	<u>Des</u>	ign the information security program to mitigate the identified risks,
8			<u>com</u>	mensurate with the size and complexity of the licensee, the nature and scope
9			<u>of th</u>	ne licensee's activities, including the licensee's use of third-party service
10			<u>prov</u>	viders, and the sensitivity of the nonpublic information used by the licensee or
11			<u>in th</u>	ne licensee's possession, custody, or control.
12		<u>b.</u>	Dete	ermine which security measures as provided under this subdivision are
13			<u>app</u>	ropriate and implement the security measures:
14			(1)	Place access controls on information systems, including controls to
15				authenticate and permit access only to an authorized individual to protect
16				against the unauthorized acquisition of nonpublic information;
17			<u>(2)</u>	Identify and manage the data, personnel, devices, systems, and facilities
18				that enable the organization to achieve business purposes in accordance
19				with the business' relative importance to business objectives and the
20				organization's risk strategy;
21			<u>(3)</u>	Restrict physical access to nonpublic information only to an authorized
22				individual;
23			<u>(4)</u>	Protect by encryption or other appropriate means, all nonpublic information
24				while being transmitted over an external network and all nonpublic
25				information stored on a laptop computer or other portable computing or
26				storage device or media;
27			<u>(5)</u>	Adopt secure development practices for in-house developed applications
28				utilized by the licensee;
29			<u>(6)</u>	Modify the information system in accordance with the licensee's information
30				security program;

1			(7)	Utilize effective controls, which may include multi-factor authentication
2				procedures for employees accessing nonpublic information;
3			<u>(8)</u>	Regularly test and monitor systems and procedures to detect actual and
4				attempted attacks on, or intrusions into, information systems;
5			<u>(9)</u>	Include audit trails within the information security program designed to
6				detect and respond to cybersecurity events and designed to reconstruct
7				material financial transactions sufficient to support normal operations and
8				obligations of the licensee;
9			<u>(10)</u>	Implement measures to protect against destruction, loss, or damage of
10				nonpublic information due to environmental hazards, including fire and
11				water damage or other catastrophes or technological failures; and
12			<u>(11)</u>	Develop, implement, and maintain procedures for the secure disposal of
13				nonpublic information in any format.
14		<u>C.</u>	Incl	ude cybersecurity risks in the licensee's enterprise risk management process.
15		<u>d.</u>	<u>Stay</u>	y informed regarding emerging threats or vulnerabilities and use reasonable
16			sec	urity measures if sharing information relative to the character of the sharing
17			and	the type of information shared; and
18		<u>e.</u>	Prov	vide cybersecurity awareness training to the licensee's personnel which is
19			<u>upd</u>	ated as necessary to reflect risks identified by the licensee in the risk
20			ass	essment.
21	<u>5.</u>	<u>lf t</u>	he lice	nsee has a board of directors, the board or an appropriate committee of the
22		boa	ard at	a minimum shall:
23		<u>a.</u>	Rec	uire the licensee's executive management or the licensee's delegates to
24			dev	elop, implement, and maintain the licensee's information security program;
25		<u>b.</u>	Rec	uire the licensee's executive management or the licensee's delegates to
26			repo	ort the following information in writing on an annual basis:
27			<u>(1)</u>	The overall status of the information security program and the licensee's
28				compliance with the provisions of this chapter; and
29			<u>(2)</u>	Material matters related to the information security program, addressing
30				issues, including risk assessment, risk management and control decisions,
31				third-party service provider arrangements, results of testing, cybersecurity

1		events, or violations, and management's responses and recommendations
2		for changes in the information security program.
3		c. If executive management delegates any responsibilities under this section, the
4		executive management delegates shall oversee the development,
5		implementation, and maintenance of the licensee's information security program
6		prepared by the delegate and shall receive a report from the delegate complying
7		with the requirements of the report to the board of directors.
8	<u>6.</u>	A licensee shall exercise due diligence in selecting its third-party service provider; and
9		a licensee shall require a third-party service provider to implement appropriate
10		administrative, technical, and physical measures to protect and secure the information
11		systems and nonpublic information accessible to, or held by, the third-party service
12		provider.
13	<u>7.</u>	The licensee shall monitor, evaluate, and adjust, as appropriate, the information
14		security program consistent with any relevant changes in technology, the sensitivity of
15		its nonpublic information, internal or external threats to information, and the licensee's
16		own changing business arrangements, including mergers and acquisitions, alliances
17		and joint ventures, outsourcing arrangements, and changes to information systems.
18	<u>8.</u>	As part of the licensee's information security program, a licensee shall establish a
19		written incident response plan designed to promptly respond to, and recover from, any
20		cybersecurity event that compromises the confidentiality, integrity, or availability of
21		nonpublic information in the licensee's possession. The incident response plan must
22		include the licensee's plan to recover the licensee's information systems and restore
23		continuous functionality of any aspect of the licensee's business or operations.
24	<u>9.</u>	A licensee's incident response plan must address:
25		(1) The internal process for responding to a cybersecurity event;
26		(2) The goals of the incident response plan;
27		(3) The definition of clear roles, responsibilities, and levels of decisionmaking
28		authority;
29		(4) External and internal communications and information sharing:
30		(5) Identification of requirements for the remediation of any identified
31		weaknesses in information systems and associated controls;

1		<u>(6)</u>	Documentation and reporting regarding cybersecurity events and related
2			incident response activities; and
3		<u>(7)</u>	The evaluation and revision as necessary of the incident response plan
4			following a cybersecurity event.
5	<u>10.</u>	Annually,	an insurer domiciled in this state shall submit to the commissioner, a written
6		statemen	t by April fifteenth, certifying the insurer is in compliance with the
7		requirem	ents set forth in this section. An insurer shall maintain for examination by the
8		departme	ent all records, schedules, and data supporting this certificate for a period of
9		five years	s. To the extent an insurer has identified areas, systems, or processes that
10		require m	naterial improvement, updating, or redesign, the insurer shall document the
11		identifica	tion and the remedial efforts planned and underway to address the areas,
12		<u>systems,</u>	or processes. The documentation must be available for inspection by the
13		<u>commiss</u>	ioner.
14	<u>26.1</u>	-02.2-04.	Investigation of a cybersecurity event.
15	<u>1.</u>	If a licens	see learns a cybersecurity event has or may have occurred, the licensee, an
16		<u>outside v</u>	endor, or service provider designated to act on behalf of the licensee, shall
17		conduct a	a prompt investigation.
18	<u>2.</u>	During th	e investigation, the licensee or an outside vendor or service provider
19		designate	ed to act on behalf of the licensee, at a minimum shall:
20		<u>a.</u> Dete	ermine whether a cybersecurity event has occurred;
21		<u>b.</u> <u>Ass</u>	ess the nature and scope of the cybersecurity event;
22		<u>c.</u> Ider	tify any nonpublic information that may have been involved in the
23		cybe	ersecurity event; and
24		<u>d.</u> Perf	orm or oversee reasonable measures to restore the security of the
25		info	mation systems compromised in the cybersecurity event in order to prevent
26		<u>furth</u>	ner unauthorized acquisition, release, or use of nonpublic information in the
27		licer	nsee's possession, custody, or control.
28	<u>3.</u>	If a licens	see learns a cybersecurity event has or may have occurred in a system
29		maintaine	ed by a third-party service provider, the licensee shall complete the
30		<u>requirem</u>	ents provided under subsection 2 or confirm and document that the
31		third-part	v service provider has completed the requirements.

1	<u>4.</u>	<u>The</u>	licen	see shall maintain records concerning all cybersecurity events for a period of			
2		<u>at le</u>	east fi	ve years from the date of the cybersecurity event and shall produce the			
3		reco	records upon demand of the commissioner.				
4	<u>26.1</u>	-02.2	-05.	Notification of a cybersecurity event.			
5	<u>1.</u>	<u>A lic</u>	ense	e shall notify the commissioner as promptly as possible, but no later than			
6		<u>thre</u>	e bus	iness days from a determination that a cybersecurity event involving			
7		non	public	c information that is in the possession of a licensee has occurred if:			
8		<u>a.</u>	<u>This</u>	s state is the licensee's state of domicile, in the case of an insurer, or this state			
9			<u>is th</u>	e licensee's home state, in the case of a producer as defined in chapter			
10			<u>26.1</u>	-26, and the cybersecurity event has a reasonable likelihood of materially			
11			<u>harr</u>	ning a consumer residing in this state or reasonable likelihood of materially			
12			harr	ning any material part of the normal operations of the licensee; or			
13		<u>b.</u>	<u>The</u>	licensee reasonably believes the nonpublic information involved is of two			
14			hun	dred fifty or more consumers residing in this state and is:			
15			<u>(1)</u>	A cybersecurity event impacting the licensee for which notice is required to			
16				be provided to any government body, self-regulatory agency, or any other			
17				supervisory body pursuant to any state or federal law; or			
18			<u>(2)</u>	A cybersecurity event that has a reasonable likelihood of materially harming			
19				any consumer residing in this state or materially harming any part of the			
20				normal operations of the licensee.			
21	<u>2.</u>	<u>The</u>	licen	see shall provide the notice required under this section in electronic form as			
22		<u>dire</u>	cted I	by the commissioner. The licensee shall update and supplement the initial			
23		and	any s	subsequent notifications to the commissioner regarding material changes to			
24		prev	viousl	y provided information relating to the cybersecurity event. The licensee's			
25		<u>noti</u>	<u>ce rec</u>	quired under this section must include:			
26		<u>a.</u>	<u>The</u>	date of the cybersecurity event;			
27		<u>b.</u>	<u>Des</u>	cription of how the information was exposed, lost, stolen, or breached,			
28			<u>inclu</u>	uding the specific roles and responsibilities of third-party service providers, if			
29			any;				
30		<u>C.</u>	<u>How</u>	v the cybersecurity event was discovered;			

1		<u>d.</u>	Whether any lost, stolen, or breached information has been recovered and if so,
2			<u>how;</u>
3		<u>e.</u>	The identity of the source of the cybersecurity event;
4		<u>f.</u>	Whether the licensee has filed a police report or has notified any regulatory,
5			government, or law enforcement agencies and, if so, when the notification was
6			provided;
7		<u>g.</u>	Description of the specific types of information acquired without authorization.
8			Specific types of information means particular data elements, including medical
9			information, financial information, or any other information allowing identification
10			of the consumer;
11		<u>h.</u>	The period during which the information system was compromised by the
12			cybersecurity event;
13		<u>i.</u>	The total number of consumers in this state affected by the cybersecurity event.
14			The licensee shall provide the best estimate in the initial report to the
15			commissioner and update the estimate with a subsequent report to the
16			commissioner pursuant to this section;
17		<u>j.</u>	The results of any internal review identifying a lapse in either automated controls
18			or internal procedures, or confirming that all automated controls or internal
19			procedures were followed;
20		<u>k.</u>	Description of efforts being undertaken to remediate the situation that permitted
21			the cybersecurity event to occur;
22		<u>l.</u>	A copy of the licensee's privacy policy and a statement outlining the steps the
23			licensee will take to investigate and notify consumers affected by the
24			cybersecurity event; and
25		<u>m.</u>	Name of a contact person that is both familiar with the cybersecurity event and
26			authorized to act for the licensee.
27	<u>3.</u>	<u>The</u>	e licensee shall comply with chapter 51-30, as applicable, and provide a copy of the
28		<u>not</u>	ice sent to consumers to the commissioner, when a licensee is required to notify
29		<u>the</u>	commissioner under subsection 1.
30	<u>4.</u>	<u>In t</u>	he case of a cybersecurity event in a system maintained by a third-party service
31		pro	vider, of which the licensee has become aware, the licensee shall treat the event in

1		accordance with subsection 1 unless the third-party service provider provides the			
2		<u>noti</u>	notice required under chapter 26.1-02.2 to the commissioner.		
3		<u>a.</u>	a. The computation of licensee's deadlines under this subsection begin on the day		
4			after the third-party service provider notifies the licensee of the cybersecurity		
5			event or the licensee otherwise has actual knowledge of the cybersecurity event,		
6			whichever is sooner.		
7		<u>b.</u>	Nothing in this chapter prevents or abrogates an agreement between a licensee		
8			and another licensee, a third-party service provider, or any other party to fulfill		
9			any of the investigation requirements imposed under section 26.1-02.2-04 or		
10			notice requirements imposed under subsection 1.		
11	<u>5.</u>	<u>lf a</u>	cybersecurity event involving nonpublic information that is used by a licensee that		
12		<u>is a</u>	cting as an assuming insurer or in the possession, custody, or control of a licensee		
13		<u>that</u>	is acting as an assuming insurer and that does not have a direct contractual		
14		<u>rela</u>	tionship with the affected consumers, the assuming insurer shall notify the		
15		<u>ins</u> ı	insurer's affected ceding insurers and the commissioner of the insurer's state of		
16		<u>don</u>	nicile within three business days of making the determination that a cybersecurity		
17		<u>eve</u>	nt has occurred.		
18	<u> <u> </u></u>	– <u>The</u>	e ceding insurer that has a direct contractual relationship with affected consumers		
19		<u>sha</u>	Il fulfill the consumer notification requirements imposed under chapter 51-30 and		
20		<u>any</u>	other notification requirements relating to a cybersecurity event imposed under		
21		<u>sub</u>	section 1.		
22	<u>7.6.</u>	<u>lf a</u>	cybersecurity event involving nonpublic information that is in the possession,		
23		<u>cus</u>	tody, or control of a third-party service provider of a licensee that is an assuming		
24		<u>ins</u>	irer, the assuming insurer shall notify the insurer's affected ceding insurers and the		
25		<u>con</u>	missioner of the insurer's state of domicile within three business days of receiving		
26		<u>noti</u>	ce from its third-party service provider that a cybersecurity event has occurred.		
27	<u> <u> </u></u>	– <u>The</u>	e ceding insurers that have a direct contractual relationship with affected		
28		<u>con</u>	sumers shall fulfill the consumer notification requirements imposed under chapter		
29		<u>51-3</u>	30 and any other notification requirements relating to a cybersecurity event		
30		<u>imp</u>	osed under subsection 1.		

	-0	
1	9. 7.	Any licensee acting as assuming insurer does not have any other notice obligations
2		relating to a cybersecurity event or other data breach under this section or any other
3		law of this state.
4	<u> 10.8.</u>	If a cybersecurity event involving nonpublic information that is in the possession,
5		custody, or control of a licensee that is an insurer or the insurer's third-party service
6		provider for which a consumer accessed the insurer's services through an
7		independent insurance producer, and for which consumer notice is required by chapter
8		51-30, the insurer shall notify the producers of record of all affected consumers of the
9		cybersecurity event no later than the time at which notice is provided to the affected
10		consumers. The insurer is excused from the obligation imposed under this subsection
11		for any producers that are not authorized by law or contract to sell, solicit, or negotiate
12		on behalf of the insurer, and those instances in which the insurer does not have the
13		current producer of record information for an individual consumer.
14	<u>26.1</u>	1-02.2-06. Power of commissioner.
15	<u>1.</u>	The commissioner may examine and investigate the affairs of any licensee to
16		determine whether the licensee has been or is engaged in any conduct in violation of
17		this chapter. This power is in addition to the powers the commissioner has under
18		chapter 26.1-03. Any investigation or examination must be conducted pursuant to
19		<u>chapter 26.1-03.</u>
20	<u>2.</u>	If the commissioner has reason to believe a licensee has been or is engaged in
21		conduct in this state which violates this chapter, the commissioner may take action
22		that is necessary or appropriate to enforce the provisions of this chapter.
23	<u>26.1</u>	1-02.2-07. Confidentiality.
24	<u>1.</u>	Any documents, materials, or other information in the control or possession of the
25		department which are furnished by a licensee, or an employee or agent thereof acting
26		on behalf of a licensee pursuant to this chapter, or that are obtained by the
27		commissioner in an investigation or examination pursuant to section 26.1-02.2-06 are
28		confidential, not subject to chapter 44-04, not subject to subpoena, and are not subject
29		to discovery or admissible in evidence in any private civil action. The commissioner
30		may use the documents, materials, or other information in the furtherance of any
31		regulatory or legal action brought as a part of the commissioner's duties. The

1		<u>con</u>	nmissioner may not otherwise make the documents, materials, or other information			
2		pub	public without the prior written consent of the licensee.			
3	<u>2.</u>	The	e commissioner or any person that received documents, materials, or other			
4		<u>info</u>	rmation while acting under the authority of the commissioner may not be permitted			
5		<u>or r</u>	equired to testify in any private civil action concerning any confidential documents,			
6		mat	terials, or information subject to subsection 1.			
7	<u>3.</u>	<u>In o</u>	order to assist in the performance of the commissioner's duties the commissioner:			
8		<u>a.</u>	May share documents, materials, or other information, including the confidential			
9			and privileged documents, materials, or information subject to subsection 1, with			
10			other state, federal, and international regulatory agencies, with the national			
11			association of insurance commissioners, its affiliates or subsidiaries, and with			
12			state, federal, and international law enforcement authorities, provided the			
13			recipient agrees in writing to maintain the confidentiality and privileged status of			
14			the document, material, or other information;			
15		<u>b.</u>	May receive documents, materials, or information, including otherwise			
16			confidential and privileged documents, materials, or information, from the national			
17			association of insurance commissioners, its affiliates or subsidiaries, and from			
18			regulatory and law enforcement officials of other foreign or domestic jurisdictions,			
19			and shall maintain as confidential or privileged any document, material, or			
20			information received with notice or the understanding that it is confidential or			
21			privileged under the laws of the jurisdiction that is the source of the document,			
22			material, or information;			
23		<u>C.</u>	May share documents, materials, or other information subject to this section, with			
24			a third-party consultant or vendor provided the consultant agrees in writing to			
25			maintain the confidentiality and privileged status of the document, material, or			
26			other information; and			
27		<u>d.</u>	May enter agreements governing sharing and use of information consistent with			
28			this subsection.			
29	<u>4.</u>	<u>A w</u>	aiver of any applicable privilege or claim of confidentiality in the documents,			
30		mat	terials, or information does not occur as a result of disclosure to the commissioner			
31		und	ler this section or as a result of sharing as authorized in subsection 3.			

1	<u>5.</u>	Do	ocuments, materials, or other information in the possession or control of the national
2		as	sociation of insurance commissioners or a third-party consultant or vendor pursuant
3		<u>to</u>	this chapter are confidential, not subject to chapter 44-04, not subject to subpoena,
4		ar	id not subject to discovery or admissible in evidence in any private civil action.
5	<u>26.1-02.2-08. Exceptions.</u>		
6	<u>1.</u>	<u>T</u> h	ne following exceptions apply to this chapter:
7		<u>a.</u>	A licensee with less than five million dollars in gross revenue or less than ten
8			million dollars in year-end assets is exempt from section 26.1-02.2-03.
9		<u>b.</u>	During the period beginning on August 1, 2021, and ending on July 31, 2023, a
10			licensee with fewer than fifty employees, including independent contractors and
11			employees of affiliated companies having access to nonpublic information used
12			by the licensee or in the licensee's possession, custody, or control, is exempt
13			from section 26.1-02.2-03.
14		<u>C.</u>	After July 31, 2023, a licensee with fewer than twenty-five employees, including
15			independent contractors and employees of affiliated companies having access to
16			nonpublic information used by the licensee or in the licensee's possession,
17	1		custody, or control is exempt from section 26.1-02.2-03.
18		<u>d.</u>	A licensee that is subject to and governed by the privacy, security, and breach
19			notification rules issued by the United States department of health and human
20			services, title 45, Code of Federal Regulations, parts 160 and 164, established
21			pursuant to the federal Health Insurance Portability and Accountability Act of
22			1996 [Pub. L. 104-191], and the federal Health Information Technology for
23			Economic and Clinical Health Act [Pub. L. 111-5], and which maintains nonpublic
24			information concerning a consumer in the same manner as protected health
25			information is deemed to comply with the requirements of this chapter except for
26			the commissioner notification requirements under subsections 1 and 2 of section
27			<u>26.1-02.2-05.</u>
28		e.	An employee, agent, representative, or designee of a licensee, that also is a
29			licensee, is exempt from section 26.1-02.2-03 and is not required to develop an
30			information security program to the extent the employee, agent, representative,
31			or designee is covered by the information security program of the other licensee.

- 1 <u>2.</u> If a licensee ceases to qualify for an exception, the licensee has one hundred eighty
- 2 <u>days to comply with this chapter.</u>
- 3 26.1-02.2-09. Penalties.
- 4 In the case of a violation of this chapter, a licensee may be penalized in accordance with
- 5 <u>section 26.1-01-03.3.</u>
- 6 <u>26.1-02.2-10. Rules and regulations.</u>
- 7 <u>The commissioner may adopt reasonable rules necessary for the implementation of this</u>
- 8 chapter.
- 9 <u>26.1-02.2-11. Implementation dates.</u>
- 10 <u>A licensee shall implement:</u>
- 11
 1.
 Subsections 1, 2, 3, 4, 5, 8, and 9 of section 26.1-02.2-03 no later than August 1,

 12
 2022; and
- 13 2. Subsections 6 and 7 of section 26.1-02.2-03 no later than August 1, 2023.
- 14 SECTION 2. LEGISLATIVE MANAGEMENT STUDY CYBER VULNERABILITIES OF
- 15 ENTITIES LICENSED BY THE INSURANCE DEPARTMENT. During the 2021-22 interim, the
- 16 legislative management shall consider, with the assistance of the insurance department,
- 17 studying the North Dakota laws and practice of insurers making property and casualty
- 18 insurance policies and related information available to insureds by electronic means; the
- 19 feasibility and desirability of prohibiting insurers from restricting the conditions in which insureds
- 20 may access such information, including through software and agents of their choosing; and the
- 21 extent to which insurers conducting business in this state have sought to limit access to policies
- 22 and related information made available to insureds, whether such restrictions restrain
- 23 competition in the marketplace, balance with an analysis of the impact of such access on
- 24 potential cyber breaches, and loss of trade secret or proprietary information resulting from
- third-party usage and software applications, and how the two competing considerations can be
- 26 safely and fairly reconciled. The legislative management shall report its findings and
- 27 recommendations, together with any legislation required to implement the recommendations, to
- 28 the sixty-eighth legislative assembly.