SB 207 2022 MIA Pre-Filed Testimony Final.pdf
Uploaded by: Kathleen Birrane
Position: FAV

LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lt. Governor

KATHLEEN A. BIRRANE
Commissioner

GREGORY M. DERWART
Deputy Commissioner

Maryland
INSURANCE ADMINISTRATION

200 St. Paul Place, Suite 2700, Baltimore, Maryland 21202
Direct Dial: 410-468-2471 Fax: 410-468-2020
Email: kathleen.birrane@maryland.gov
www.insurance.maryland.gov

TESTIMONY OF
THE
MARYLAND INSURANCE ADMINISTRATION
BEFORE THE
SENATE FINANCE COMMITTEE

JANUARY 19, 2022

SENATE BILL 207 – INSURANCE CARRIERS - CYBERSECURITY STANDARDS

POSITION: SUPPORT

Thank you for the opportunity to provide written comments regarding Senate Bill (SB) 207.

SB 207 is a departmental bill that establishes data security and incident response requirements for segments of the insurance industry, including insurance companies. While the Insurance Article, Annotated Code of Maryland, currently addresses data privacy, there are no specific regulatory requirements related to data security or the establishment of a data security program within an insurer. Likewise, legislation passed in 2019 requires certain licensees of the Maryland Insurance Administration (MIA) Commissioner to notify the Commissioner of a data security breach at the same time and in the same manner the licensee is required to provide a breach notice to the Office of the Attorney General (OAG), there are no comprehensive regulatory requirements specific to the insurance industry related to incident response plans or notice to the Commissioner. The MIA believes that these are significant gaps in regulatory oversight and in protection for Maryland residents, as well as for the industry itself. SB 207 will fill these gaps by establishing reasonable, proportionate requirements for data security and incident response programs and for regulatory notice.

SB 207 adopts key provisions of the National Association of Insurance Commissioners' (NAIC) Model Act #668 - Insurance Data Security Law (the Model), which was adopted by the NAIC in 2017. The Model was developed in response to several major data breaches involving large insurers that exposed and compromised the sensitive personal information of millions of insurance consumers. The Model requires carriers licensed by a department of insurance to

develop, implement, and maintain an information security program, investigate any cybersecurity events, and notify the state insurance commissioner of such events. As of this writing, 18 jurisdictions, including the neighboring states of Delaware and Virginia, have adopted the Model. Facilitating adoption of the Model is a strategic priority for the NAIC to ensure and formalize insurance data security protections in a reasonably uniform manner across U.S. insuring jurisdictions and to avoid risking federal preemption of state laws in this area if states fail to act.

SB 207 requires insurers and certain other licensees of the Commissioner to develop, implement, and maintain an information security program based on its risk assessment, with a designated employee in charge of the information security program. Requirements for compliance with the information security program and oversight of third-party service providers are phased in over time. Covered licensees determine the appropriate security measures to implement based on their own ongoing risk assessment for internal and external threats. If a cybersecurity event occurs, a covered licensee is required to investigate the cybersecurity event and notify the Commissioner of a cybersecurity event. SB 207 also grants the Commissioner the power to examine and investigate covered licensees to determine compliance with the law and to require that deficiencies be remedied.

For context, insurance is a 1.28 trillion dollar industry in the U.S. and a 41 billion dollar industry in Maryland, with approximately 1,600 licensed insurers conducting business in the state. Nearly every resident provides some level of personally identifiable information to an insurer, including protected health and financial information, either directly or through claims. Hackers are aware of this and the profitable opportunity for disruption it engenders. Consequently, insurers are frequent targets of hacking, phishing schemes, and ransomware.

As noted above, under legislation passed in 2019, carriers are required to notify the MIA of a security system breach at the same time that the carrier is required to notify the OAG under the Commercial Law Act. The circumstances in which a business must provide notice to the OAG are narrowly defined and not tailored to the insurance industry. However, even under those very narrow circumstances, since the law went into effect on October 1, 2019, there has been a significant increase in the frequency and severity of confidential data breaches as to which notice has been given.

Date Range	Number of Breaches	Total Impacted MD Residents	Number of Residents Impacted in a **single** breach
10/1/2019 - 12/31/2019 (3 months)	7	783	517
1/1/2020 - 12/31/2020 (12 months)	31	18,454	9,753
1/1/2021 - 8/8/2021 (8 months)	52	38,535	15,556

This limited data demonstrates the need to ensure that carriers have data security systems in place, are actively assessing and acting to mitigate their data security risk, have incident response plans in place, and keep the Commissioner informed of cyber incidents.

The standards and reporting requirements reflected in the Model and incorporated into SB 207 are consistent with current business standards and practices for the industry and its vendors. The Model was developed iteratively over the course of 2 years with extensive input from the insurance industry, other state insurance regulators and consumer representatives. Given that, it reflects a reasoned effort to assure reasonable and coherent regulatory uniformity of standards across states and reporting platforms. In addition, the existence and depth of carriers' cybersecurity protection programs are already evaluated by credit rating agencies and cybersecurity risk analysis and are part of each carrier's triennial financial examination and other risk reporting requirements.

Requiring an insurer to have a written data security and incident response reporting program is also consistent with other types of operational risk program standards imposed by the Insurance Article. For example, carriers are required to maintain disaster recovery and business interruption plans that meet certain standards.

While based on the Model, SB 207 takes an incremental approach to addressing data security in the Maryland insurance market. While the Model imposes requirements on essentially all licensees, including producers, SB 207 is limited to risk-bearing entities and the health claim administrators for those entities. In addition, while most large national and regional insurers have programs in place that meet and far exceed the standards in the Model, this legislation considers the needs of smaller, regional insurers in that it phases in requirements for compliance with the information security program and oversight of third-party service provider obligations set forth in the Model.

Adopting SB 207 is necessary to protect the integrity of consumer and insurer data against security breaches and to assure that the Commissioner has the tools needed to enforce protection standards and to mitigate the potential damage of a carrier's data breach. Therefore, the MIA respectfully requests a favorable report on SB 207.

CPD Written Testimony SB 207.pdf
Uploaded by: Hanna Abrams
Position: FWA

BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief
Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

January 17, 2022

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Hanna Abrams, Assistant Attorney General

RE: Senate Bill 207 – Insurance Carriers – Cybersecurity Standards – SUPPORT WITH AMENDMENTS

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 207 ("SB 207") with the amendments discussed below. SB 207 establishes cybersecurity standards for insurance carriers, which the Division agrees is critical. However, based on the Division's experience investigating cybersecurity breaches, we believe the two amendments discussed below are essential.

First, for the purpose of clarity, SB 207 should reinstate the requirement that insurers comply with federal law and the Maryland Personal Information Protection Act (Md. Com. Law §14-3501 *et seq*.) currently set forth in § 4-406:

> **Compliance with this section does not relieve a carrier from a duty to comply with any other requirements of federal law or Title 14 of the Commercial Law Article relating to the protection and privacy of personal information.**

The compliance requirement is implicit in the cross references contained in § 33-105, but the Division strongly believes the requirement should be incorporated explicitly in SB 207.

Second, the definition of a "cybersecurity event" includes exclusions in § 33-101(E)(2). This exclusion must contemplate potential misuse in the future. In addition, in recent ransomware attacks, companies pay the attacker in exchange for access to their systems and the promise that the information will be destroyed after payment is received. This promise is nothing more than the word of a thief that has already breached their system and held information hostage. The Consumer Protection Division urges the committee to add language providing an objective standard for a determination that the information has been destroyed or returned. To that end, we propose the following additional language to § 33-101(E)(2)(II) (bolded language added):

"CYBERSECURITY EVENT" DOES NOT INCLUDE: . . .

(II) AN EVENT WITH REGARD TO WHICH THE CARRIER HAS DETERMINED **with reasonably high degree of certainty** THAT THE NONPUBLIC INFORMATION ACCESSED

BY AN UNAUTHORIZED PERSON HAS NOT BEEN **and will not be** USED OR RELEASED AND HAS BEEN RETURNED OR DESTROYED.

The Consumer Protection Division urges a favorable report with amendments discussed.

Cc: Members, Finance Committee
Kathleen Birrane, Insurance Commissioner

AHIP Comments_Cyber SB 207_1_17_22.pdf
Uploaded by: Kris Hathaway
Position: UNF

F 202.331.7487
ahip.org

January 17, 2022

The Honorable Delores G. Kelley
Chair, Senate Finance Committee
Maryland General Assembly
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Dear Senator Kelley:

I am writing on behalf of AHIP to request revisions and clarifications to SB 207 which parallels the National Association of Insurance Commissioner's (NAIC) Insurance Data Security Model Law (Model) as proposed in SB 207. AHIP is the national association whose members provide insurance coverage for health care and related services. We are committed to solutions and partnerships that improve affordability, value, access, and well-being for consumers.

The NAIC voted to adopt the Model in December of 2017, and health insurance providers agree with the three core elements of the model law:

1. To require carriers to protect consumer data;
2. To require carriers to promptly investigate a suspected Cybersecurity Event; and
3. Upon determining there has been an actual Cybersecurity Event, to notify the Commissioner.

However, there remain specific areas where the industry, including AHIP, has concerns with the Model from a legal and administrative perspective. A coalition of 10 national trade groups (ACLI, AHIP, AIA, BCBSA, IIABA, IRI, NAIFA, NAMIC, PCI and RAA) began a series of meetings to develop changes to state legislation based on the Model. Several of those concerns were addressed and included in SB 207. The remaining revisions to the Model are outlined in the recommendations below. Over a dozen states have adopted these proposed edits.

Recommendation 1 – Include a HIPAA Safe Harbor Exemption: Since 1996, health insurance providers across the country have been subject to the sweeping requirements of HIPAA and subsequent HITECH amendments. As federal law, it provides uniform requirements as well as consistent terminology and definitions which are pervasive throughout the entire health care community. HIPAA and HITECH are applicable to entities which handle protected health care information, including commercial health insurers as well as Medicare and Medicaid plans, and doctors, hospitals, pharmacists, etc.

Over 40 states have cyber breach legislation enacted, and nearly all have a "HIPAA Exemption" provision to avoid entities being subjected to overlapping and often conflicting definitions and requirements of state law, and state-to-state laws. HIPAA addresses all the significant elements of the model law and more, except for the Commissioner notification. The edits clarify if a health insurance provider meets HIPAA standards, they are in compliance with this law; and they must also notify the Commissioner of a

Cybersecurity Event.This recommendation is of the most important concern of health insurance providers, and strongly request the addition of the following language in SB 207:

> Carriers subject to Pub.L. 104-191.110 Stat.1936 enacted August 21, 1996 (Health Insurance Portability and Accountability Act) will be considered to meet the requirements of this Act except those pertaining to Commissioner Notification [insert section]

Recommendation 2 - Exclusivity, Section 33-102 (A)(1) pg 6: A clarification is needed in this section as the bill only states it is intended to create cyber "standards" for carriers but does not seem to avoid overlapping or conflicting existing state laws. Deleting this section and replacing with the langage below would ensure the law is the exclusive state law on the subject it covers, so that licensees are not exposed to multiple and different state law requirements and definitions should they occur.

> Notwithstanding any other provision of law, this Act establishes the exclusive state standards applicable to Licensees for data security, the investigation of a Cybersecurity Event as defined in Section 33-101, and notification to the Commissioner

Recommendation 3 - Electronic Information, Section 8603(l) pg 8: These revisions limit the information protected to only *electronic* information to align with the overall concept of electronic data and cybersecurity. Also, by including this deletion, we clarify the goal is to protect consumers, not corporate entities.

> (A) The purpose of this tile is to establish standards for:
> (1) Electronic data security;

Thank you very much for the opportunity to provide AHIP's minor revisions to SB 207 as based on the NAIC Insurance Data Security Model Law. As additional background, further information on HIPAA provisions is attached. If you have any questions, please do not hesitate to reach out and contact me at your convenience.

Sincerely,

Kris Hathaway
Vice President, State Affairs
America's Health Insurance Plans
khathaway@ahip.org / (202) 870-4468

cc Commissioner Kathleeen Birrane
Maryland Insurance Administration

HIPAA Privacy and Security Summary

The 1996 Health Insurance Portability and Accountability Act, Pub. L. 104-191 (**HIPAA**), resulted in the promulgation of the **Privacy Rule**[1] and the **Security Rule**.[2] These rules were impacted by the passage in 2009 of the Health Information Technology for Economic and Clinical Health Act (**HITECH**), a part of the American Recovery and Reinvestment Act of 2009.

Who Must Comply with HIPAA Rules?

Covered entities and business associates, as applicable, must follow HIPAA rules. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA rules.

Covered Entities

Covered entities electronically transmit health information. Covered entities which must follow HIPAA standards and requirements include:

- Covered Health Care Provider: Any provider of medical or health care services who transmits health information electronically. These include doctors, hospitals, pharmacists and others.
- Health Plan: Any individual or group plan that provides or pays the cost of health care, such as: company health plans; government programs that pay for health care (Medicare, Medicaid, and the military and veterans' health care programs); health insurance companies; health maintenance organizations (HMOs).
- Health Care Clearinghouse: A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa, such as billing services, community health management information systems, repricing companies, and value-added networks.

Business Associates. If a covered entity enlists the help of a Business Associate, then a written contract or other arrangement between the two must detail the uses and disclosures of PHI the business associate may make and require that the business associate safeguard the PHI.[3]

- Business Associate is a person or organization, other than an employee of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI.
- A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate.
- Business associates provide services to covered entities that include: accreditation, billing, claims processing, consulting, data analysis, financial services, legal services, management administration, and utilization review.
- If a covered entity enlists the help of a business associate, then a written contract or other arrangement between the two must detail the uses and disclosures of PHI the business associate may make and require that the business associate safeguard the PHI.

A covered entity can be a business associate of another covered entity.[4]

---

[1] *45 CFR Part 160 and Part 164, Subparts A and E*; August 14, 2002.
[2] *45 CFR Part 160 and Part 164, Subparts A and C*; February 20, 2003.
[3] *45 C.F.R. 164.502(e) and 164.504(e).*
[4] *45 C.F.R. 160.103.*

The Privacy Rule

The HIPAA Privacy Rule establishes standards for the protection of protected health information (**PHI**) held by covered entities. The Rule also establishes standards for business associates.[5]

The Privacy Rule provides the following protections:

- Gives patients important rights with respect to their health information, including rights to examine and obtain a copy of their health records in the form and manner they request (and to ask for corrections to their information).[6]
- Permits the use and disclosure of health information needed for patient care and other important purposes.[7]

Protected Health Information (PHI): The Privacy Rule protects individually identifiable health information, called PHI, held or transmitted by a covered entity or its business associate, *in any form, whether electronic, paper, or verbal*.

PHI includes many common identifiers, such as name, address, birth date, and Social Security number. PHI also includes information that relates to any of the following:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; and
- The past, present, or future payment for the provision of health care to the individual.[8]

The Security Rule

The HIPAA Security Rule specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of **ePHI**. Covered entities must review and modify security measures to continue protecting ePHI in a changing environment. As a result of HITECH's passage in 2009, business associates must also comply with the Security Rule's requirements.

Covered entities and business associates must develop and implement policies and procedures to protect the security of ePHI they create, receive, maintain, or transmit. Each entity must analyze the risks to ePHI in its environment and create solutions appropriate for its own situation. What is reasonable and appropriate depends on the nature of the entity's business, as well as its size, complexity, and resources.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the ePHI;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.[9]

The Security Rule does not dictate security measures but requires covered entities to consider all of the following:

- Size, complexity, and capabilities;
- Technical, hardware, and software infrastructure;
- The costs of security measures; and

[5] *45 C.F.R. 160.102 and 160.103.*
[6] *45 C.F.R. 164.524 and 164.528.*
[7] *45 C.F.R. 164.502(a).*
[8] *45 C.F.R. 160.103.*
[9] 45 C.F.R 160 306(a).

- The likelihood and possible impact of risks to ePHI.

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI in *electronic, verbal, or paper form.*[10]

- The Rule is detailed in setting out the information which must be contained in the notice.
- Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.
- Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually.

The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Almost all states that have enacted some form of cyber breach legislation also have a "HIPAA exemption" to avoid these entities being subjected to confusing, overlapping, and often conflicting requirements of law, both within and across states.

Enforcement

The HHS Office for Civil Rights and state Attorneys General enforce the HIPAA Privacy, Security, and Breach Notification Rules.

- Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the U.S. Department of Justice may apply.
- Common noncompliance issues include impermissible PHI uses and disclosures, lack of PHI safeguards, lack of patients' access to their PHI, use or disclosure of more than the minimum necessary PHI, and lack of administrative ePHI safeguards.
- Enforcement efforts have grown steadily, most noticeably since the passage of the HITECH updates in 2009 and have ranged from corrective action plans to multi-million-dollar penalties.

[10] 45 C.F.R. 164.400 - 414.