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.