Health Plan Cybersecurity

Presentation before the U.S. Department of Labor ERISA Advisory Council

September 9, 2022

About AHIP

AHIP is the national association whose members provide coverage for health care and related services to hundreds of millions of Americans every day. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities, and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access, and well-being for consumers.

ahip.org

Our Mission Statement

We are champions of care.

Health insurance providers, working together as one.

Making health care better and coverage more affordable for every American.

Listening. And guiding the conversation on care.

We are advancing mental and physical health.

Always improving how and where we help others.

Harnessing the power of our collective expertise.

Turning healthy insights into helpful innovations.

All for the greater good.

So everyone can thrive in good health.

Together.

That’s what care does.

AHIP

Guiding Greater Health

AHIP Members Lead in Cybersecurity

- Cybersecurity and protecting the data, privacy, and protected health information of all of our members is a top priority for AHIP and the industry, as articulated in a recent Priorities Statement from AHIP's Board of Directors
- We believe government policies should support efforts by entities to develop consistent, secure mechanisms to share information with other entities and consumers to accommodate digital solutions but avoid delays or cyber security risks.
- Health insurance providers implement multi-dimensional safeguards – physical, technical, and administrative – to protect members' personal information.
- As cybersecurity risks become more commonplace, public and private entities should take reasonable and prudent steps to protect individually identifiable, proprietary, corporate, and other information held electronically and in physical form.
- In health care specifically, patient safety and access issues are of primary concern.

AHIP Board of Directors' Core Privacy, Confidentiality, and Cybersecurity Priorities

- Everyone deserves the peace of mind of knowing that their personal health information is private and protected.
- Every person should have access to their data and be able to know easily how their health information may be shared.
- Personal health information should be protected no matter who holds the data.
- Demographic data should be leveraged to improve health equity and outcomes.
- Entities offering digital tools should be required to embed consumer privacy and security protections within those tools.
- The commercial sale of identifiable health information should be prohibited without the agreement of the individual.

AHIP Engagement

- **AHIP is an active participant in the Health / Public Health Sector Coordinating Council (HSCC)**
  - The HSCC is recognized by the U.S. Department of Health and Human Services (HHS) as the critical infrastructure industry partner for coordinating strategic, policy and operational approaches to prepare for, respond to, and recover from significant cyber and physical threats to the ability of the sector to deliver critical assets and services to the public. These threats include natural, technological and human-made disasters, and national or regional health crises. The HSCC represents the primary healthcare subsectors of direct patient care; public health; health plans and payers; pharma, blood and labs; medical technology; health information technology; and funeral homes and mass fatality managers.
- **AHIP has a standing Cybersecurity Work Group**
  - Participants include Chief Information Security Officers, Policy Experts, Government Affairs representatives, and others who are interested in security and cybersecurity topics. Participants in that Work Group address all cyber and security topics, including cyber alerts and threats, industry guidance, and responding to legislative and regulatory issues involving cybersecurity.
- **AHIP also participates in a number of external engagements, including the**
  - **Confidentiality Coalition**, a diverse group of healthcare stakeholders with an interest in privacy, confidentiality, security, cybersecurity and related topics;
  - the **Workgroup for Electronic Data Interchange (WEDI**), which acts as an advisory body to the Secretary of HHS as mandated by HIPAA;
  - the **Chamber of Commerce Privacy Working Group**; and
  - the **American Benefits Council**, which focuses on issues important to health and welfare plans.

Federal and State Activity

- National Cyber Director appointed by the President
- HHS-OCR Cybersecurity Guidance
- 405(d) Program and Task Group
- Cybersecurity and Infrastructure Security Agency (CISA) advisories
- FBI reports and investigations
- FDA guidance for medical devices
- FTC guidance
- NAIC Insurance Data Model Act #668

Recommendations for the ERISA Advisory Council

RECOMMENDATION #1

We encourage the Council to consider the existing work that has taken place so that the Department can leverage the work products in this space so as not to duplicate Federal and State work in this area.

- As the Council engages in work in this area, we recommend clarifying whether the focus of cybersecurity guidance will be on employer-sponsored self-funded plans, employer-sponsored fully insured plans, both, or some other structure (e.g., Multiple Employer Welfare Arrangements [MEWAs]).
- As our statement illustrates, we believe that employer-sponsored health and welfare plans that comply with HIPAA, the HITECH Act, and other federal and State laws and regulations understand cybersecurity risks and the importance of implementing reasonable and appropriate protections.

Recommendations for the ERISA Advisory Council

RECOMMENDATION #2

The Council should clarify the scope of its cybersecurity recommendations and focus recommendations on any "gaps" or current concerns that may not be commonplace today or covered by the existing legal protections.

- For context, employer-sponsored health and welfare plans that are fully-insured will rightly rely on health insurance providers to protect information from a cybersecurity perspective. The employer itself cannot legally access protected health information held by a health insurance provider under HIPAA and should not be expected to prepare for, respond to or remediate a cyber-attack. The health insurance provider is and should be the entity to plan for, respond to and remediate cybersecurity attacks.

Recommendations for the ERISA Advisory Council

RECOMMENDATION #3

The Advisory Council should consider working with HHS/OCR to issue guidance explaining any cybersecurity concerns and the existing roles and responsibilities between employers and health insurance providers in fully insured plans.

For employer-sponsored health and welfare plans that are self-funded, often these arrangements involve an Administrative Services Only (ASO) agreement through which an entity handles the administrative services for the plan. Anecdotal information received is that cybersecurity is a common contractual provision in modern ASO contracts and entities have been proactive in arranging cyber planning and response in these arrangements. As some entities may be accustomed to planning for cybersecurity risks and protections, it is not known whether all ASO arrangements have consistently and routinely prepared for cybersecurity risks.

Recommendations for the ERISA Advisory Council

RECOMMENDATION #4

The Council should consider asking the Department to conduct a limited and concentrated informal inquiry to research and discover whether ASO contracts have adequate provisions for cybersecurity. If such provisions are not commonplace, the Department should issue guidance setting forth expectations between employers and ASO providers in self-funded health and welfare plans. If no ASO contract exists and the employer functions as the administrator, the Council should recommend ways (using the resources highlighted above) for self-funded health and welfare plans to address cybersecurity risks in their business environments and operations.

Despite the funding arrangement of a health and welfare plan, in our assessment, smaller or mid-sized companies frequently find cybersecurity guidance helpful as their resources are often limited when compared to larger, more robust operations.

Recommendations for the ERISA Advisory Council

RECOMMENDATION #5

The Council could recommend that the Department begin educational outreach to help smaller and mid-sized self-funded health and welfare plans understand the risks and benefits to promote building cyber protections into their business operations. This should include an inventory of work performed by federal agencies to date so that resources and priorities and be focused on areas not currently addressed by existing educational and guidance documents. Where possible, the Department should partner with other agencies or leverage the cybersecurity guidance and materials that have been developed to date.

As the Council explores this important topic, we caution the Council from prescribing recommendations, guidance, or future regulations that are prescriptive or that would remain static and create an inability to keep pace with new cyberthreats, industry trends for protections and new technological developments that promote better detection, response, and remediation.

It is also important for the Council to consider the costs and benefits of any recommended cybersecurity activity. Companies need the ability to conduct their own risk assessments based on their unique operating environments and to develop risk management programs that are scalable to their business operations and that take into account available resources. In

Recommendations for the ERISA Advisory Council

RECOMMENDATION #6

Future recommendations, guidance, or regulations should be flexible and allow for technology-neutral, scalable solutions based on an entity's business operations, risk assessment, available resources, and new developments that promote better detection, response, and remediation. A cost-benefit analysis should be an essential part of the process.

A key function for public and private entities to combat cyber-attacks is to share information when possible as a campaign or infiltration is detected. Federal laws have attempted to help in this regard, but oftentimes information cannot be shared (i.e., classified, confidential, proprietary), or if it is shared, it is "watered down" to a point where it becomes generic and unhelpful.

Recommendations for the ERISA Advisory Council

RECOMMENDATION #7

We support increased information sharing between public and private sector entities. We also support international efforts are important for migrating threats and campaigns, particularly from nation states and part of global "infection" processes as can occur with malicious code and viruses.

Questions and Answers

- Marilyn Zigmund Luke, AHIP
- Adam Beck, AHIP
- Alan Thierfeldt, Cigna