AHIP

Statement for the Record

before the

U.S. Department of Labor

ERISA Advisory Council

September 9, 2022

Cybersecurity in the Context of Health and Welfare Benefit Plans

AHIP[1] appreciates the opportunity to offer our perspectives regarding health and welfare benefit plans and the important topic of Cybersecurity. In the digital age, protection of information from a privacy and security perspective is vital to retain the trust of the consumers we serve.

Everyone deserves the peace of mind of knowing that their personal health information is private and protected. Health insurance providers have long-been committed to instituting privacy and cybersecurity practices to protect every individual's personal health information. We believe that the Advisory Council is focusing on a timely and important topic to further education about and enhanced protections for cyber security of health and related information.

Our statement today is intended to provide a background of our work in this area and the privacy, security and cybersecurity protections that are in place today by health insurance providers. AHIP's members are well accustomed to protecting health information in electronic and physical forms.

Our statement is structured to provide an overview of the existing work taking place for cybersecurity, along with examples of recent cybersecurity attacks that affected many Americans. In addition, AHIP members have been working with a number of federal and state legislators and regulators to advance cybersecurity awareness and related protections. We offer a summary of some of these activities to inform the Council by providing an overview of the work taking place in a broader health ecosystem. We summarize existing legal requirements, and we conclude by offering our recommendations for future focus areas for the Council and the Department, with the goal of advancing cybersecurity as a priority and key focus area for the consumers that we serve.

AHIP Members Lead in Cybersecurity

AHIP recently released our Board's **Guiding Principles** and the Chief Medical Officer's **Roadmap** for protecting consumer information to establish health insurance providers as leaders in privacy and security in which we addressed cybersecurity as a key priority. 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 cybersecurity risks.

Health insurance providers implement physical, technical, and administrative safeguards to protect members' personal information. These security practices are not "one dimensional" and frequently incorporate existing guidance, industry practices,

[1] 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.

vendor and software recommendations, legal and regulatory requirements, practical experiences, and a host of physical, technical, and administrative features that are built into systems architecture, policies, procedures, and business practices.

Cybersecurity risks continue to evolve from a lone hacker to nation-state, complex geopolitical campaigns. 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 addition, we have witnessed ransomware and similar events pose serious threats to conducting ongoing business operations.

In health care specifically, patient safety and access issues are of primary concern. No individual or entity should be harmed because of ransomware or similar cybersecurity events that can interfere with care delivery, services, accessibility, or outcomes. Our members remain steadfast in protecting the consumers they serve and diligently work to stay ahead of trends as they face these real-life situations and potential consequences.

Health insurance providers employ a variety of tools depending on the environment to ensure security practices are in use through various lines of defense, including but not limited to risk management analyses, internal audits, standards controls, ongoing risk assessments, and other confidential and proprietary mechanisms. Private sector cybersecurity programs and certifications offered by HITRUST, the Electronic Health Network Accreditation Commission (EHNAC), MITRE ATTACK, and others help protect and align industry practices.

AHIP Engagement

The healthcare system is one of 17 national critical infrastructures, as identified in a series of presidential Executive Orders (attached in the Appendix) establishing public-private partnerships for critical infrastructure protection. AHIP is an active participant in the Health / Public Health Sector Coordinating Council (HSCC).[2] 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.

The HSCC issues guidance for risk mitigation, develops recommendations, best practices and guidance for enterprise cybersecurity improvements, and advises our government partners about policy and regulatory solutions that facilitate mitigation of

[2] Refer to the website https://healthsectorcouncil.org/ for more information.

cybersecurity threats to the sector. A special subset of the HSCC, the "Cybersecurity Working Group" or "CWG," was established with the mission being to collaborate with HHS and other federal agencies to identify and mitigate systemic risks that affect patient safety, security, and privacy, and thus improve confidence in the healthcare system. AHIP is an active member of the CWG. We also hold an elected seat on the Cybersecurity Executive Committee for the CWG. We find the HSCC information and collaboration very helpful and support its future work in this area.

For ongoing engagement and education of our members, AHIP has an established Cybersecurity Work Group which consists of cyber and security experts from health insurance providers across the nation. 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 members receive Cyber Alerts, including warnings of threats and advice for mitigating them. We respond to federal legislative and regulatory developments on cybersecurity topics.

AHIP also participates in a number of external engagements, including the: (a) Confidentiality Coalition, a diverse group of healthcare stakeholders with an interest in privacy, confidentiality, security, cybersecurity and related topics; (b) the Workgroup for Electronic Data Interchange (WEDI), which acts as an advisory body to the Secretary of HHS as mandated by the Health Insurance Portability and Accountability Act (HIPAA); (c) the Chamber of Commerce Privacy Working Group; and (d) the American Benefits Council, which focuses on issues important to health and welfare plans.

Recent Cyber Events

When cyber-attacks and intrusions occur, they are often disseminated in the media and cause consumer concerns and frustration, particularly when personal information is housed in systems that are the subject of the attack or intrusion. Entities often need time to investigate and assess what has happened and whether personal data has been compromised as a result of the cyber-attack. As discussed below, if a cyber-attack results in a data breach, health insurance providers and other entities covered by the Health Information Portability and Accountability Act (HIPAA) are required to notify consumers, HHS, and the media about the particulars of the data breach.[3] Notably, HHS maintains a public database which summarizes data breaches affecting over 500 individuals, including the entity, type of breach, number of individuals affected, and other information.[4] This database has increased transparency about the "who, what, where and when" of breaches and is an important tool for consumers to get a "big picture" of what has occurred.

[3] 45 C.F.R. §§ 164.400-414.
[4] The HHS database is available on the Internet at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

In 2020, for example, ransomware attacks were responsible for almost 50% of all healthcare data breaches.[5] Our experience supports that ransomware continues to be a prevalent risk and something for which health insurance providers and other entities must be prepared. Some of the more public and far-reaching recent cyber events included:

- Cyber-attacks on the Colonial Pipeline, which disrupted fuel supplies and caused a shut-down of essential functions in the Eastern U.S.
- The SolarWinds campaign, which acted as an unidentified Trojan Horse affecting federal agencies, numerous private-sector companies, and state and local governments across the country. It was one of the most sophisticated cyberattacks ever conducted.
- As a result of the WannaCry Ransomware attack in September 2020, a German hospital was hacked and forced to divert patients, resulting in a woman's death.
- The Apache Log4j event, which was used in a variety of consumer and enterprise services, websites, applications, and operational technology products, affected systems through which an unauthenticated remote actor took control.
- "RagnarLocker," was a group of ransomware actors targeting critical infrastructure sectors, including the health sector.
- Other ransomware attacks on the U.S. and international organizations estimated at more than 1,000 instances included "Trickbot" and "Cobalt Strike."

As the examples illustrate, it is vital to stay abreast of these events and we believe that our efforts have been successful in "getting the word out" to help promote early detection and prevention, remediation, and an overall consistent and thorough industry response.

Summary of Federal Activities

AHIP was pleased to see the appointment of the White House National Cyber Director who has been working with stakeholders from the public and private sectors. The National Cyber Director serves as a principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders and is working on the national "digital ecosystem," with the goals of: (1) ensuring federal coherence; (2) improving public-private collaboration; (3) aligning resources to aspirations; and (4) increasing present and future resilience. We encourage the Council to keep watch of the Director's work, which is expected to inform and affect public and private policy and regulatory initiatives.

[5] CISA issued a Fact Sheet:, "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches" to provide helpful strategies for such scenarios, available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf.

Recognizing that there are many federal agencies that have been addressing cybersecurity topics in a policy, regulatory, and/or guidance perspective, we share some key highlights from 2022 that include:

- The HHS/OCR has issued a series of cybersecurity guidance documents.
- The "405(d)" program[6] and Task Group is a collaborative effort between industry and the federal government, which aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.
- The U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) has issued voluminous materials, including Cybersecurity Advisories which warn of developing and emerging cyber campaigns and actions companies can take to thwart or remediate intrusions or attacks.
- The Federal Bureau of Investigation frequently receives reports and investigates cybercrimes.
- The Food and Drugs Administration (FDA) has been updating guidance for medical devices and cybersecurity.
- The Federal Trade Commission sets out a series of guidance documents for small businesses, privacy and security enforcement, and those with a consumer focus.
  The National Institute of Standards and Technology (NIST) issued a Request for Information in February to re-evaluate its 2018 Cybersecurity Framework and recently updated the CSF, which is widely used by the public and private sectors as a baseline for cyber structure.
- NIST also launched the National Initiative for Improving Cybersecurity in Supply Chains (NIICS), which will be a "wide-ranging public-private partnership [with a] focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology."

While we highlight this ongoing federal work, the list is not exhaustive of the work taking place at the federal level. In fact, many agencies are evaluating their own systems and members of their cybersecurity workforce to ensure that they have the technical and human resources to adequately address cyber risks. Recent federal budget allocations are likely to result in more focused internal and external cybersecurity efforts. [7]

[6] For more information, refer to the website: https:/405d.hhs.gov.

[7] The federal budget included allocations for: the FDA has $6M to address cybersecurity vulnerabilities by improving the safety and security of medical devices, hire cyber experts and develop tools to track vulnerabilities associated with devices; the HHS Administration for Strategic Preparedness and Response (ASPR) received $9 million for Office of National Security which provides strategic all-source information, intelligence, counterintelligence, insider threat, cyber threat intelligence, supply chain risk management, and communication security; DHS obtained $2.5B to CISA (a $486M increase over current budget) to maintain critical cybersecurity capabilities implemented in the American Rescue Plan Act of 2021, expand network protection throughout the Federal Executive Branch, and bolster support capabilities, such as cloud business applications, enhanced analytics, and stakeholder engagement; The U.S. Department of the Treasury has $215M to protect and defend agency's systems; The U.S. Department of Justice was

State Initiatives

The NAIC has been working on improving cybersecurity in the insurance industry, and in late 2017, they adopted the NAIC Insurance Data Security Model Act, #668: **MO-668 (PDF)** (often referred as the "NAIC Cyber Model"). States have been steadily working to enact the Cyber Model, and so far, 21 states have passed some version of it. Of those, two thirds have included an expanded HIPAA Safe Harbor for state insurance department licensees. States also have had broadly applicable cyber breach bills, which illustrates the complexity of the issues and the difficulty in administering the patchwork of State requirements based on the regulation of data type, entity, both or some other construct.

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.

Legal Background and Policy Issues

The HIPAA contains privacy and security provisions for protected health information held by covered entities and business associates. Health insurance providers are well-accustomed to complying with the HIPAA requirements, many of which were designed to protect the privacy and security of health information in electronic and other environments. In 2008, the Health Information Technology for Economic and Clinical Health (HITECH) Act modified HIPAA and promoted the adoption of health information technology through electronic health records (EHRs) for healthcare providers. The Act included key provisions to modify the HIPAA penalties, improve enforcement, and set new protections for health information. Federal regulations were updated to conform to these statutory requirements. As noted above, any data breach resulting from a cybersecurity attack requires notifications to HHS, affected consumers, and the media.

allotted funds to expand the ability to pursue cyber threats and support multi-year efforts to build cyber investigative capabilities at FBI field offices; HHS received an increase of $90M for a resulting $161 Million for HHS Cybersecurity under the Office of the Chief Information Officer; CMS was granted $646 Million for information technology systems, Cybersecurity investments, system upgrades, modernizing payment systems; ONC: $39 Million (increase of $18M from 2022) to implement the Trusted Exchange Framework and Common Agreement (TEFCA). The Common Agreement includes requirements for cybersecurity; OIG: $15 million to increase OIG's cybersecurity efforts, expand digital technology, modernize infrastructure, promote AI workforce.

For cybersecurity-specific laws and regulations, the Cybersecurity Information Sharing Act of 2015[8] created a framework for information sharing between and among the public and private sectors. This framework was enacted in 2021 to amend the HITECH Act by encouraging covered entities and business associates to adopt strong cybersecurity practices.[9] The Cyber Incident Reporting for Critical Infrastructure Act of 2022[10] recognized the importance of establishing a Center within the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) to receive reports from a "critical infrastructure sector" and established timeframes for doing so. We await future regulations from CISA related to the mechanisms of these cyber reporting processes. In addition, specific requirements can apply to governmental benefits programs such as the Federal Employee Health Benefits Program (FEHBP). The FEHBP contracts include a section on procedures for information security incident and data breach reporting.

The DOL Focus

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.

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.

Recommendation 3: The Advisory Council should consider working with HHS/OCR to issue guidance explaining any immediate cybersecurity concerns for health benefit plans and the existing roles and responsibilities between employers and health insurance providers in fully insured plans under HIPAA.

[8] Public Law 116-321.
[9] The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) was directed to consider recognized security practices when imposing penalties or taking other enforcement actions.
[10] Pub. L. No. 117-103.

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. Entities have been proactive in planning for cyber events and responses in agreements. However, without conducting an official survey or inquiry, it is not known whether all ASO arrangements have consistently and routinely prepared for cybersecurity risks.

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.

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 overly 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. As the real-life examples listed above illustrate, cybersecurity is an area that is highly technical and rapidly evolving. Threats that exist today can easily become outdated as new threat actors and nefarious campaigns emerge. Health and welfare plans need the ability to be nimble and respond to these developments in proactive and innovative ways based on market developments and emerging threats.

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 other words, the Council should not recommend a one-size-fits-all approach because each company's consumers and business operations dictate be reasonable and appropriate cyber protections that should be in place.

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. In addition, international alerts for cyber-attacks and emerging campaigns should be publicly disseminated as soon as feasible. Understanding international "lessons learned" can also promote better practices to adopt and threats that are migrating across platforms. International efforts can continue but U.S. agencies and entities should remain the key driver for protection of systems.

Public and private entities should do as much as they can to prevent harm to consumers, particularly if a cyber-attack can result in preventing access to health care services or result in cybercrimes, particularly when direct harm to an individual results (e.g., medical identity theft, being unable to obtain needed healthcare).

Recommendation 7: We support increased information sharing between public and private sector entities via federal channels, through the HSCC, the Health Information Sharing & Analysis Center, and among entities themselves to thwart cyber attacks. This is particularly important when attacks are directed at critical infrastructure such as the health industry. We also support international efforts as they 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.

Appendix

Cybersecurity Executive Orders

Presidential Executive Orders:

March 9, 2022: Ensuring Responsible Development of Digital Assets

September 30, 2021: Continuance or Reestablishment of Certain Federal Advisory Committees and Amendments to Other Executive Orders

May 12, 2021: Improving the Nation's Cybersecurity

January 19, 2021: Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities

May 15, 2019: Securing the Information and Communications Technology and Services Supply Chain

May 2, 2019: America's Cybersecurity Workforce

May 15, 2018: Enhancing the Effectiveness of Agency Chief Information Officers

May 11, 2017: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

May 1, 2017: Establishment of the American Technology Council

September 29, 2016: Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters

February 9, 2016: Commission on Enhancing National Cybersecurity

February 13, 2015: Promoting Private Sector Cybersecurity Information Sharing

February 12, 2013: Improving Critical Infrastructure Cybersecurity

Full text of AHIP **Guiding Priorities** and the Chief Medical Officer's **Roadmap** for protecting consumer information.