Segal

Michael Stoyanovich
VP, Senior Consultant
mstoyanovich@segalco.com

180 Howard Street
Suite 1100
San Francisco, CA 94105-6147
segalco.com

Memorandum

To: 2022 Advisory Council on Employee Welfare and Pension Benefit Plans

From: Michael Stoyanovich

Date: July 13, 2022

Re: Cybersecurity Issues Affecting Group Health Plans

Segal is an over 80-year-old global, full-service employee benefit and Human Resources (HR) consulting firm. Our clients include multiemployer health and pension funds, corporations, higher education institutions and their health systems, nonprofits, church plans, and public sector entities, among many others. Within Segal there are many areas of service expertise. I am part of a group of professionals dedicated to enhancing the quality, service and productivity of benefits service groups and larger service organizations – Administration and Technology Consulting (ATC). Additionally, we provide support for the governance, risk, and compliance (GRC) efforts of these organizations. I personally have been an executive at two multiemployer third-party benefits administrators and since joining Segal some years ago, one focus of my work is to support the GRC initiatives of many different organizations (especially multiemployer). It is from this perspective I offer the following comments.

Introduction

Cybersecurity risks, their management and mitigation, are among the most discussed topics of concern for all group health plans, including those Segal supports. Plan fiduciaries have a heightened awareness of the cybersecurity risk environment within which they operate. This is in addition to having preexisting unique statutory and regulatory responsibilities on behalf of plan participants.

Group health plans already comply with various laws protecting the sensitive data for which they are responsible. Cybersecurity, privacy, security, and administrative obligations exist under both the Employee Retirement Income Security Act (ERISA) and the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Employers and group health plans are also subject to confidentiality obligations under the Genetic Information Nondiscrimination Act (GINA)[1] and the Americans with Disabilities Act (ADA).[2]

[1] https://www.eeoc.gov/laws/guidance/fact-sheet-genetic-information-nondiscrimination-act
[2] https://www.ada.gov/ada_intro.htm

HIPAA and HITECH provide a robust statutory and regulatory framework for protection of both Protected Health Information (PHI) and Electronic PHI (e-PHI) used, maintained, and disclosed by group health plans and their partners (known as "Business Associates.") Congress has recognized this regulatory structure and enhanced it in 2021, when it passed legislation encouraging plans to utilize standards and practices established by the National Institute of Standards and Technology (NIST). HIPAA's privacy and security rules and HITECH's breach rules set forth a mature and complete set of guidelines for protection and enforcement of how ERISA group health plans use and disclose PHI and e-PHI.

HIPAA and HITECH are enforced by the Centers for Medicare & Medicaid Services (CMS), which regularly monitors breach reports and complaints. CMS's Office for Civil Rights (OCR) has a detailed enforcement process, and it frequently publishes enforcement data including case examples and resolution agreements.[3] Guidance is frequently issued on special topics such as cloud storage, ransomware, and the use of remote devices. Thus, based on current regulatory guidance (in particular, HIPAA) there is already sufficient protection and oversight of ERISA group health plans. There exists sufficient guidance on what group health plans need to do to protect the valuable data and information with which they are entrusted.

Additionally, the sub-regulatory guidance published by the Department of Labor (DOL) in 2021[4] closely mirrored existing HIPAA and HITECH guidance, so its principles were already being used by group health plans to enhance their cybersecurity stance. More so, significant internal risk mitigation concerns coupled with external commercial pressures have also resulted in most group health plan sponsors reviewing and enhancing their cyber risk management practices (via NIST, ISO or other cybersecurity risk frameworks).

Based on the existing robust regulatory structure for group health plans, we do not recommend additional guidance from the DOL. Yet if it were to be contemplated it should be carefully coordinated with CMS, and if then produced, be done within the context of further clarifying the existing guidelines published by the DOL. Even then, it would be valuable for the DOL to acknowledge, as HIPAA's security rule currently does, the wide variety of group health plan sponsors and the data with which they are entrusted. Hence any clarifications to the guidance offered by the DOL should allow for flexibility, recognizing the many differences in group plan sponsors (size, financial resources, human resources, etc.) and be technology neutral.

Group Health Plans and Cybersecurity

Health benefit plans already have taken significant steps within existing statutory, regulatory, and legal frameworks to protect the cybersecurity of regulated, confidential, sensitive, or nonpublic employee and participant data and information. As noted, some of these frameworks are dictated by regulatory requirements (HIPAA and HITECH). Other non-regulatory cybersecurity frameworks have been embraced by fiduciaries as a part of their commitment to fulfill their obligations to participants, as well (e.g., the Department of Labor's cybersecurity guidance which applied to fiduciaries for all ERISA plans[5]). Additionally, cybersecurity frameworks are embraced by plans on their own initiative (or in some cases due to external

[3] https://www.hhs.gov/hipaa/for-professionals/index.html
[4] https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414
[5] IBID

commercial stimulus). These include frameworks published by NIST[6] or the International Organization for Standardization (ISO)/IEC [7] just to name a few.[8]

Additionally, Congress amended the HITECH Act in 2021 to encourage health plans and business associates under HIPAA to follow "recognized security practices" as a defense or to mitigate penalties that could be assessed for violations of the HIPAA security rule.

The law defines these "recognized security practices" as:

- Standards, guidelines, best practices, methodologies, procedures, and processes developed under the NIST Act;
- Approaches promoted by the Cybersecurity Act of 2015;
- Other programs and processes that address cybersecurity and that are developed, recognized, or announced though regulations under other statutory authorities.

When enforcing the HIPAA security rule, CMS will now consider the extent to which a covered entity (or business associate) has followed "recognized security practices" for (at least) the previous 12 months. The requirements of the security rule itself have not changed. It appears that the HITECH amendment took effect on January 5, 2021, when it was signed into law (Public Law 116-321).

One can visualize a concentric circle of the cybersecurity practices of health plans with HIPAA at the core.

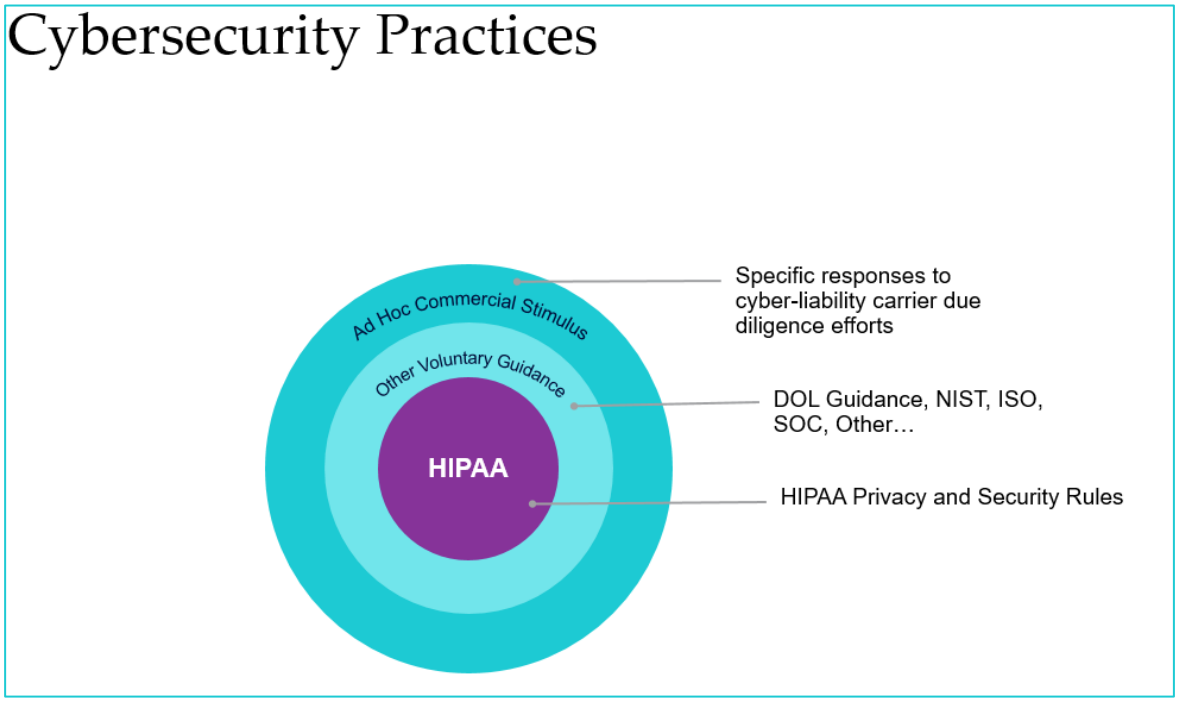

Illustration 1

[6] https://www.nist.gov/cyberframework/getting-started
[7] https://www.iso.org/isoiec-27001-information-security.html
[8] Besides NIST and ISO frameworks, other widely used frameworks include SOC2, HITRUST and many others.

HIPAA Privacy and Security Rules

HIPAA applies to both covered entities and business associates. A covered entity is any healthcare provider that electronically transmits health information. A business associate is a person or an entity that has access to patient information and provides certain services to a covered entity. Covered entities and business associates must meet HIPAA compliance. ERISA group health plans are typically covered entities.

For discussion today it is important to note the difference between HIPAA privacy and HIPAA security. The HIPAA Privacy Rule protects all types of PHI: electronic; written and oral. The HIPAA Security Rule applies to electronic protected health information (ePHI). ePHI is PHI that is transmitted electronically or stored electronically. That is: sent or received via e-mail; stored on a computing network; stored on a computer (including laptops, notebooks or tablets, or other mobile devices); stored on electronic media such as CDs, disks, flash drives, tapes, or memory cards (including those in smartphones).

Health plans already must take actions to protect ePHI per the HIPAA Security Rule. The HIPAA/HITECH Final Rule was published by the Department of Health and Human Services (HHS) in January 2013 modifying the Privacy, Security, Breach Notification and Enforcement Rules under HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). *These Rules are very complex and beyond today's discussion, or my expertise.*

However, it is important to note that health plans already must meet HIPAA-HITECH standards from that Rule. Group health plans must perform regular HIPAA security assessments to ensure that how they "...store, transmit, and protect, and eventually destroy ePHI..." follows the rules.

These HIPAA security assessments are recommended to occur every two (2) to three (3) years, at a minimum, or when a particular event could trigger prudence dictating an organization seek an updated HIPAA security assessment (e.g., changes in the information technology (IT) ecosystem that directly affects the storage or transmission of ePHI, etc.).

HITECH also makes business associates (such as third-party administrators and pharmacy benefit managers, among others) directly liable for compliance with the Security Rule's administrative, physical, and technical safeguards, and documentation requirements. The HITECH final rule also expands the definition of "business associate" to include the following types of entities:

- Subcontractors: Under the final rule, if a business associate delegates or outsources services or functions for a group health plan that involve the creation, receipt, use or disclosure of PHI to a subcontractor (individual or entity), that subcontractor becomes a business associate. Business associates (not group health plans) are required to enter into business associate agreements with *their* subcontractors. If subcontractors then delegate or outsource any of their services or functions to other subcontractors, those subcontractors also become business associates and the original subcontractor must enter a business associate agreement with those subcontractors. These obligations flow downstream through all individuals or entities using, creating, receiving, or disclosing PHI to perform services or functions.

- Additional Types of Business Associates: The definition of business associate is expanded to include additional types of entities, including vendors retained by group health plans to provide personal health records services to participants.
- Expanded Liability for Storage Providers: The final rule clarifies that entities that store PHI, either electronically or in hardcopy, such as storage providers, document storage vendors, co-location vendors, and e-mail and Web hosting providers, are business associates even if they do not access, use, or disclose that information. These storage provider entities may include vendors that host ePHI that plans access and use as part of their routine business practices and vendors that store ePHI for backup and disaster recovery, or archival purposes. Entities that merely transport PHI (e.g., courier services, the United States Postal Service (USPS), United Parcel Service (UPS) and their electronic equivalents, Internet service providers that provide mere data transmission services) are not business associates.

HIPAA Security Risk Analysis

HIPAA's Security Rule does not proscribe a one-size-fits-all blueprint for compliance with specific security procedures, protocols, or technology. Rather, under the Security Rule an organization must determine the most appropriate way to achieve security goals, considering the characteristics of the organization and its environment. This flexibility is important to reflect the fact that there are small and large health plans that are a part of diverse types of organizations (corporations, multiemployer benefits administration offices, or third-party administrators, etc.) and they may find different methods of compliance appropriate. Additionally, this technology agnostic approach has ensured that the Security Rule stays relevant. With ever evolving threats, and constantly changing technology and tools used to defend against those threats, the Security Rule is not stale, or out of date.

Technical safeguards are noted in the Security Rule, as well. They too are flexible. Therefore, organizations are free to select whichever controls are adequate to their operating environment, including inventorying their PHI; email security; cloud security; network segmentation; role-based access control; securing remote access; enabling multi-factor authentication (MFA); continuous monitoring and log management. *Moreover, HITECH's requirements concerning security mandate that for ePHI to be considered "secure," it must be encrypted. Thus, the one defined requirement is that ePHI – whether at rest or in transit – must be encrypted to ensure the information is unreadable, undecipherable, and unusable should a data breach occur. If PHI is not encrypted and a privacy breach occurs, that breach must be reported to CMS and in most cases is published on CMS's public website.*

Segal's experience is that group health plans (and the larger organizations they may be a part of) embrace many if not all the above different controls (where relevant and appropriate).

Physical safeguards are also discussed in the Security Rule. The physical safeguards focus is on physical access to ePHI, regardless of its location. ePHI could be stored in a remote data center, in a commercial cloud service, or on-premises. The safeguards also dictate how workstations and mobile devices should be secured against unauthorized access by employing: facility access controls; policies for the use and positioning of workstations; policies and procedures for mobile devices; and the inventorying of hardware.

Not least, administrative safeguards are also included in the Security Rule. The administrative safeguards are the policies and procedures which bring the Privacy Rule and the Security Rule together. They are the pivotal elements of a HIPAA compliance checklist and require that a HIPAA Security Officer (and a HIPAA Privacy Officer) be assigned to put the measures in place to protect ePHI, while they also govern the conduct of the workforce.

DOL Guidance

In addition to the above noted technical, physical, and administrative safeguards within HIPAA to which group health plans are subject, many group health plans – and in my own recent, personal experience, multiemployer health plans particularly – are also seeking to act in accord with the DOL's recently published cybersecurity guidance.

Although the guidance does not specifically use the language or jargon of ERISA group health plans, there appears to be no reason why the logic of the approach, the suggested best practices and participant educational tips identified could not apply to such group health plans. Hence, many of these plans (and their broader organizations) have sought to enhance their existing HIPAA-centric cybersecurity practices by seeking to act in accord with the DOL's 2021 guidance, as well.

Additional Cybersecurity Efforts

Some group health plans also seek to use additional cybersecurity frameworks of their own initiative, beyond their HIPAA security efforts (and for some, in addition to the voluntary effort to act in accord with the DOL's guidance referenced above).

These efforts include the use of comprehensive security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[9]. Still other benefit plans are within entities that have embraced other security frameworks such as ISO/IEC 27001, also a well-known international set of standards for information security management. Still others use a Service Organization Control (SOC)[10] report in combination with one or more of the above efforts (HIPAA mandatory security efforts, NIST or ISO voluntary efforts).

These additional voluntary efforts by many group health plans (or the organizations of which they are a part) are even more comprehensive in their scope than a) HIPAA security and b) the DOL's recently published cybersecurity guidance.

Yet those are not all the potential spurs to cybersecurity risk management efforts for many group health plans. For many such plans and / or the organizations they are a part of, cyber-liability insurance providers are seeking enhanced assurances via detailed and specific due diligence efforts, prior to underwriting policies. In many cases these group health plans and/or the organizations they are within have had to dedicate significant effort to provide data and information regarding specific technical solutions and / or information about their IT ecosystem to the cyber-liability insurance providers; and in some cases, have been asked to take steps to enhance parts of their cybersecurity stance to reassure their cyber-liability carrier(s). This is all

[9] "…The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders."

[10] Often the preferred SOC report is a SOC2: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

in the service of obtaining the coverage fiduciaries think is relevant and appropriate for the plans and their participants. This coverage helps fiduciaries manage cyber-liability risk and provides access to expertise that comes with these policies.

In Closing

Thank you for the opportunity to be a part of this process.