WILMERHALE®

Statement of Kirk J. Nahra
Partner, WilmerHale
Kirk.Nahra@wilmerhale.com

Cybersecurity Issues for Group Health Plans

Thank you for the opportunity to present today on the issues involved in cybersecurity for group health plans.

My Background

My name is Kirk Nahra. I am a partner with WilmerHale in Washington, D.C., where I am co-chair of the global Cybersecurity and Privacy Practice Group. I represent companies in virtually all industries and around the world on the full range of privacy and cybersecurity compliance and legal issues. I also teach as an adjunct professor at the Washington College of Law at American University, including a course in Health Care Privacy and Security. I am a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis and a fellow with the Institute for Critical Infrastructure Technology.

I have been advising companies on compliance issues with the HIPAA Privacy and Security Rule since those rules were being drafted in 1999. A significant part of my practice over those years has involved advising health plans, both the insurers that are health plans and the employer sponsored group health plans that are the focus of the discussion today. I also provide advice to health insurers in their relationships with these group health plans (where a health insurer may provide "insurance" to a group health plan or may provide administrative services to a self-insured group health plan). In addition I represent various service providers in their relationships with these group health plans.

HIPAA Background

The HIPAA era began in 1996, with the passage of the Health Insurance Portability and Accountability Act of 1996. While "HIPAA" now means many things to many people, at its foundation, the HIPAA law itself focused on "portability," the idea that individuals could "take" their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions.

When Congress passed HIPAA, it also added into the mix a variety of other topics related to the health care industry (such as creating large funding for what has now become an extended fight against health care fraud). One of the policy mandates adopted in HIPAA was to move toward standardized electronic transactions for the health care industry. The core idea was that certain "standard transactions"—such as the submission of a health insurance claim and the payment of that claim—could be "standardized" in mandatory electronic formats, and thereby create efficiency savings and more effective results. With these standardized transactions came a concern about privacy and security associated with health care information being put into electronic form, with the resulting requirements for the creation of the HIPAA Privacy Rule and the HIPAA

Security Rule. So, now, for most people and in most situations, HIPAA has become shorthand for health care privacy and security.

- Who Needs to Care about HIPAA?

First and foremost, the HIPAA privacy and security rules are designed to protect individuals, generally patients of health care providers and members of insurance or government health insurance benefit programs. From a policy perspective, lots of attention is paid to whether individual rights are protected appropriately under the HIPAA rules, balancing privacy interests with the overall operation of the health care system and significant public benefits that arise from the use and disclosure of health care information in a variety of contexts.

From a compliance perspective, however, the focus is on those businesses that must comply with these HIPAA principles, and face potential enforcement if compliance problems arise.

So, who does need to comply with the HIPAA rules? HIPAA's history leads to much of this answer. Initially, driven by the primary focus of the HIPAA law on portability and standard transactions, the HIPAA privacy and security rules applied only to specifically designated "covered entities," health care providers, health plans, and health care clearinghouses. The category of "covered entities" includes a full range of health care providers, generally physicians, hospitals, pharmacies, and a wide variety of entities that provide direct health care services to patients. Coverage also reaches various "health plans," including government health care programs, private health insurers, and significantly, the health care benefit plans offered by employers.

However, even from the start, HIPAA was not a general medical privacy law. It applied to certain entities in certain situations, for certain information. That meant that a large number of companies that obtain or use health care information were not within the scope of these rules, such as consumer-facing entities, many health care web sites, life and disability insurers, employers in their employment role, etc. These "gaps" increasingly lead to challenges in today's environment. (See, e.g., Nahra, "A public service announcement about the HIPAA Privacy Rule," (IAPP), June 21, 2021, available at https://www.wilmerhale.com/en/insights/publications/20210621-a-public-service-announcement-about-the-hipaa-privacy-rule).

Because of this limitation to covered entities, the U.S. Department of Health and Human Services (HHS) developed a creative solution to respond to a key fact about the health care system. While the covered entities are core participants in the industry, such covered entities rely on tens of thousands of vendors to provide them services, with many of these services involving protected patient information. Therefore, the concept of a "business associate" was born, i.e., an entity that provides services to the health care industry where the performance of those services involves the use or disclosure of patient information.

Because HHS originally had no direct jurisdiction over these "business associates," HHS imposed an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that the covered entity violated the HIPAA rules. A business associate's failure to meet a contractual privacy standard would be a breach of that contract, but would not

subject the business associate to government enforcement, because the business associate was not regulated under the HIPAA rules.

Now, as a result of the 2009 Health Information Technology for Economic and Clinical Health ("HITECH") law, and HHS regulations issued in 2013, "business associates" must comply directly with significant portions of the HIPAA rules. Accordingly, while these vendors have had contractual obligations since the beginning of the HIPAA era, they now must meet many of the same standards as the covered entities, and face the same risks associated with government enforcement. Although this legislation does not turn business associates into covered entities, it does impose—for the first time—direct accountability on these business associates, with potential civil and criminal liability for a failure to meet these requirements.

In addition, the HITECH regulations extended "business associate" compliance obligations "downstream," to service providers of a business associate, and to service providers of that downstream business associate, on indefinitely. These "subcontractors" face the same compliance obligations as a first-tier business associate that contracts directly with a hospital or a health insurer.

Therefore, the following kinds of entities need to be concerned directly with compliance obligations and potential enforcement as a result of the HIPAA rules:

- Health care providers, such as hospitals, physicians, and pharmacies (if they utilize standard electronic transactions as defined by the HIPAA statute, such as submitting claims) (Note that this can mean, for example, that an onsite employer medical clinic that does not bill insurance would not be a covered entity health care provider under HIPAA);
- Health insurers and government health care programs;
- Any employer that provides health care benefits to its employees (with the employer's "health plan" being the covered entity);
- A service provider to any of these entities; and
- A service provider to a service provider of any of these entities (and on downstream, indefinitely).

Consequently, while HIPAA does not cover all health care information, it certainly applies to a large range of entities, many of whom may not realize that they face legal obligations and enforcement risks as a result of the HIPAA rules.

And, to be clear, the HIPAA rules also affect an enormous range of other entities that collect, rely on, use, and/or disclose health care information, because the HIPAA rules have an impact on how information can flow, even if the entities are not covered directly. For example, entities conducting medical research are typically not subject to the HIPAA rules directly, but may need to ensure appropriate compliance with HIPAA procedures when seeking information from those entities covered by HIPAA, such as a doctor who was involved in prior treatment of a clinical trial participant.

However, it also is important to note that HIPAA, even with its recent expansion from the HITECH Act aside, is still not a general medical privacy law. It does not protect all health information, of employees or anyone else. While its scope has broadened, its protections still depend on where

health care information starts, with a health care provider or health plan. That leaves enormous gaps in protection, particularly given recent technological and philosophical developments that are encouraging consumer involvement in their own health care and providing the technology to make this goal a reality.

- HIPAA and Employers

This history and the resulting scope of the HIPAA Privacy and Security Rules drives the challenges today for employers and their health plans. HHS had authority to impose obligations on employer sponsored group health plans because such group health plans were defined as "health plans" in the HIPAA statute – because of their involvement with "portability." However, based on the same definitions, HHS did not have the authority to regulate employers directly. So the group health plan (essentially a benefits contract) is a HIPAA covered entity, but the employer is not. From an employer perspective, one important consequence is that much of the health information collected by an employer about its employees actually is not in any way subject to the HIPAA rules. This includes disability and workers compensation claims information, Family and Medical Leave Act information, doctor's notes about worker absences, COVID vaccine information and a wide range of other information about the health of employees collected in the normal course of business. This is "health information" as we normally think of that term, but it is not "protected health information" covered by the HIPAA rules and subject to HIPAA's protections and obligations.

On the flip side, what HIPAA does mandate in most circumstances is that these "group health plans" comply with some or all of the HIPAA Privacy Rules (depending on a variety of specific details), even though the "group health plan" typically has no independent existence outside of the definition of the benefits contract. In short, the benefits contact now has operational compliance obligations. That legal fiction (or sorts) drives much of the complication and confusion about how HIPAA applies to group health plans. (Remember that the application of this issue in most circumstances is to companies outside of the health care industry who otherwise have no involvement with HIPAA).

When HHS was writing the rules for these group health plans, one of the government's primary concerns in structuring the rule was its recognition that employers provide much of the health insurance in this country. With this background, the goal of HHS with employers is quite clear- to ensure, as much as possible, that protected health information (as defined by HIPAA) is not used by employers for employment-related decisions nor used against an employee in connection with its employment (meaning that an employee couldn't be fired because it - or its spouse or child – had an expensive medical condition or, from today's news, that employee or spouse or child obtained an abortion in a state that prohibited it or where the employer might object to this).

However, because of the tortured history of the HIPAA statute, which was driven by health insurance portability and "standard transactions" rather than privacy, HHS had no authority to regulate employers directly. If it had been given such authority, the law could have included a provision that said, "no employee health information can be used for employment related purposes." However, this is not the case.

While HHS could not regulate employers directly, HHS did have authority to regulate group health plans, which are the employee welfare benefit plans that provide actual health care benefits to employees and define the scope of these benefits.

These group health plans are "covered entities" under the HIPAA Privacy Rule. They are in the larger category of “health plans,” meaning that for the most part, they must comply with the HIPAA Privacy Rule to the same extent that a typical health insurer or large hospital must, even though virtually no employer group health plan acts in the same way as a health insurer. (Note that at one point in time some large employers administered their own group health plans but to my knowledge that practice has largely disappeared).

Under the HIPAA Privacy Rule as written, employers must place stringent conditions on the flow of employee health information from the group health plan, which is the formal entity providing health care benefits to employees, and to the employer itself as the health plan's sponsor.

And therein lies the problem. HHS established a regulatory framework, covering virtually every employer that provides any kind of health benefits to its employees, which is based on the idea that there is a distinction between this "group health plan" and the "plan sponsor" of that health plan. And, throughout the employer community, there simply is no such distinction. The group health plan is a piece of paper, a formal contract required by the Employment Retirement Income Security Act (“ERISA”) statute (the federal law governing employee benefits and pension plans), but typically nothing more. So, HHS has created a complicated set of regulatory provisions based on this fiction that there is today an actual or conceptual separation between a plan sponsor and a group health plan.

In addition, because of the gaps in HIPAA's scope, there have always been large areas where employers obtained health care information about employees outside the reach of the HIPAA rules. For example, disability claims, workers' compensation claims, Family and Medical Leave Act data, information obtained as a result of employment applications, and general information obtained through the course of being an employer all are outside the scope of HIPAA.

Accordingly, the key application of HIPAA generally works as follows. There are certain group health plans that are exempted from HIPAA’s coverage – but this exemption is written to – as a practical matter – exclude virtually no group health plan.

At that point the primary focus of attention turns to whether a group health plan is insured or self-insured. The rules provide the possibility that an insured health plan could receive so little information about the group health plan details that it can avoid some – but not all – of HIPAA’s obligations. There is meaningful ambiguity about what obligations remain if an insured group health plan avoids all HIPAA obligations. Moreover, as employers have been involved more actively in managing their costs, even this potential exemption creates issues. For example, if an insured group health plan receives no employee protected health information (“PHI”) at all (and therefore triggers the exemptions for some obligations), but their “business associate” (a consulting firm for example who needs specific details to shop the coverage) does receive the PHI, does that trigger a loss of this exemption? Does the insured group health plan ever get an exemption from the obligation to have business associate agreements? So this possibility of an exemption exists, but may not really apply in many circumstances. (My expectation is that few insured group health

plans would be able to demonstrate compliance with the HIPAA rules even if they needed to be in compliance as a technical matter).

For self-insured group health plans, this possibility of an exemption disappears, no matter what information is obtained by the self-insured group health plan. That means that the self- insured group health plan for, for example, a mid- size employer in your home town in the manufacturing or retail industry, now has to comply with the HIPAA privacy and security rule in the same way that Aetna or Blue Cross Blue Shield does.

Many of the challenges that arise for these group health plans relate to "privacy" – how data is protected and used and segregated so that it is only used for appropriate purposes and not in violation of the HIPAA rules. This issue is becoming increasingly complicated as employers look to "holistic" wellness programs for example. I am happy to discuss these privacy challenges but they are not the focus of our discussion today.

On cybersecurity, the primary problems are clear. A self-insured group health plan (and many insured health plans) must comply in full with the HIPAA Security Rule. That group health plan typically has no independent existence. Therefore, how the group health plan complies would of necessity involve the company's entire information system, most of which has nothing whatsoever to do with HIPAA. The large bank who has a self- insured group health plan now must meet HIPAA's obligations for the bank's systems – but those systems are the same across the business. That is the challenge.

So, as we think about these rules, there are a variety of questions that come to mind. Does it make sense to have a standard that is the same for the bank group health plan as it is for Aetna or Blue Cross Blue Shield or the Mayo Clinic? How does a bank (or any employer, essentially, outside of itself being a HIPAA covered entity for its business) "comply" with HIPAA when the group health plan – to the extent it does anything – uses all the same systems? Is this a standard that basically requires all employers who provide health benefits to employees to raise the level of their security to the HIPAA standard for everything? Few (no?) group health plans operate their own computer systems. What does it actually mean to "comply" with the HIPAA Security Rule in this context? (Please note that there is a much broader discussion about how anyone can comply with the HIPAA Security Rule, but that is a discussion for another day).

How does the group health plan "segregate" HIPAA PHI in its systems, when the same IT team (and finance and legal) all advise the group health plan and the employer generally?

How does this group health plan "oversee" the business associates? Presumably, the health insurer who is hired to administer the health plan knows the HIPAA rules – but what about the cloud vendor for the employer, or the accounting firm, or the human resources support firm? Does the group health plan contract separately with these entities (rather than with the employer)? What about the wellness plan (if it is even subject to HIPAA)?

So, with this background and this sense of the main issues, I am happy to take your questions.