NORTH CAROLINA LAW REVIEW

Volume 98 | Number 6 Article 6

9-1-2020

The Debilitating Scope of Care Coordination Under HIPPA

Frank Qin

The Debilitating Scope of Care Coordination Under HIPAA*

Care coordination aims to achieve personalized, high-quality, safe, and efficient patient care through the deliberate organization of patient care activities and sharing of information among all entities providing care. Care coordination utilizes a broad spectrum of tools, combining traditional healthcare clinical services and social welfare service approaches. Implementing care coordination strategies has been shown to improve long-term health outcomes of patients with a variety of health issues, including chronic diseases and conditions, acute health problems, and rehabilitation or long-term care.

However, HIPAA's regulatory framework—which involves the minimum necessary principle, security and technical requirements, limitations based on the services provided, and lack of guidance in regards to care coordination—severely limits the ability of entities to share medical information with social welfare services. As such, healthcare entities are essentially crippled in delivering proper care coordination and high-quality medical care.

This is especially stark for people suffering from chronic diseases and the medically indigent, who rely on social welfare services and nonmedical entities in underserved communities. This Comment argues that unless HIPAA regulations are redefined by adding an express provision to allow use and disclosure of electronic protected health information (PHI) for care coordination purposes or expansion of the minimum necessary principle, care coordination cannot help the patients who need it most.

INTRODUCTION

While the Health Information Portability and Accountability Act ("HIPAA")[1] protects the privacy of an individual's health information, it also prevents providers from providing comprehensive medical care. Comprehensive medical care takes all aspects of a person—physical, psychological, social, and spiritual—into consideration in the management of a patient's well-being.[2] As such, providers must consider information regarding a patient's medical history, family history, and socioeconomic situation throughout all phases of treatment. On one hand, HIPAA's stringent regulations on healthcare providers and payers ensures that health information is exchanged securely and only as necessary to treat an immediate problem. However, at the same time, these regulations deter providers from sharing additional patient information that might be useful for treating a patient in a more holistic and comprehensive manner. HIPAA's regulatory framework allows—and even encourages—healthcare providers to remain hesitant in disclosing information because HIPAA merely permits, but does not require,

1. Health Information Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2018)).

2. This term is also known as holistic medicine or alternative medicine; however, I chose not to use these terms since they typically connote a practice that aims to heal, but lacks plausibility and is generally untested, untestable, or proven ineffective. *See generally* ROSE SHAPIRO, SUCKERS: HOW ALTERNATIVE MEDICINE MAKES FOOLS OF US ALL (2008) (chronicling the "epidemic" of alternative medicine); Wallace Sampson, *Antiscience Trends in the Rise of the "Alternative Medicine" Movement*, 775 N.Y. ACAD. SCI. 188 (1995) (describing "alternative" as a noneffective alternative to medical treatment); Gina Kolata, *On Fringes of Health Care, Untested Therapies Thrive*, N.Y. TIMES (June 17, 1996), https://www.nytimes.com/1996/06/17/us/on-fringes-of-health-care-untested-therapies-thrive.html [https://perma.cc/7NLQ-DGWN] (detailing the business of alternative medicine, despite doubts regarding efficacy and lack of regulation). Instead, I address the necessity for medicine to treat not just the immediate physical health problem but also the broader well-being of the patient.

them to share such information for much of their medical treatment activities.[3] In certain situations, such as sharing patient information to nonregulated entities, covered providers are altogether banned from sharing patient information absent express authorization,[4] which can delay medical care.

In the context of care coordination, which involves a broad spectrum of tools that combine traditional healthcare clinical services with social welfare service approaches,[5] HIPAA's regulatory framework hampers adequate and effective medical care. Care coordination requires substantial organization between various entities such as primary care providers, physical therapists, long-term nursing staff, and welfare services in order to achieve high-quality, safe, and effective patient care.[6] Above all, care coordination depends on reliable communication between entities with minimal filtering, so that each entity may assess a patient's complete situation as they provide treatment.

For people who suffer from chronic diseases[7] but have minimal resources and no health insurance, this poses an especially troublesome situation. Many of the social welfare services that third-party organizations provide are not subject to HIPAA, so they do not have the capability to send or receive patient information securely. In these situations, HIPAA serves as a serious obstacle for care coordination.

More than 60% of adults in the United States suffer from at least one chronic disease, with more than 40% having two or more chronic diseases.[8] Health-care costs associated with chronic conditions account for approximately 90% of total health-care spending, including both private insurance and Medicare spending,[9] which amounts to $3.15 trillion in health-care spending

3. *See* 45 C.F.R. § 164.502(a)(1) (2019).

4. *See id.* § 164.502(a).

5. *See Care Coordination*, AGENCY FOR HEALTHCARE RES. & QUALITY, https://www.ahrq.gov/ncepcr/care/coordination.html [https://perma.cc/RV95-V6DV] (last updated Aug. 2018). The Agency for Healthcare Research and Quality is a federal agency that functions as a research arm of the Department of Health and Human Services. For a more precise definition of care coordination, see *infra* Section I.B.

6. *See Care Coordination*, *supra* note 5.

7. Examples of chronic diseases include heart disease, cancer, chronic lung disease, stroke, Alzheimer's disease, diabetes, and chronic kidney disease. *See* Nat'l Ctr. for Chronic Disease Prevention & Health Promotion, *Chronic Diseases in America*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/chronicdisease/resources/infographic/chronic-diseases.htm [perma.cc/8CXK-KASK].

8. *Id.*

9. CHRISTINE BUTTORFF, TEAGUE RUDER & MELISSA BAUMAN, MULTIPLE CHRONIC CONDITIONS IN THE UNITED STATES 10 (2017), https://www.rand.org/content/dam/rand/pubs/tools/TL200/TL221/RAND_TL221.pdf [https://perma.cc/MQ69-2Y8Z]. Total healthcare spending is the amount spent on all outpatient and inpatient healthcare services—prescriptions, ER visits, inpatient stays, and outpatient visits—across all payers and includes out-of-pocket payments. *Id.* at 10.

per year.[10] On average, individuals with chronic conditions spend nearly $8,000 annually in total health-care expenditures—six times as much as individuals without chronic conditions.[11] In terms of out-of-pocket spending, individuals with chronic diseases spend almost twice as much as those without—approximately $1,100 each year.[12]

These statistics suggest that insurance payers bear much of the costs associated with chronic diseases. However, individuals still pay a significant portion of their healthcare costs out-of-pocket. The financial impact associated with having a chronic disease is high, and it is even higher for uninsured patients with minimal resources. Proper care coordination involves a multitude of entities, many of whom require some form of payment. Individuals who are unable to access paid services may need to rely on low cost or free community-based efforts—many of which are privately sponsored, fall outside traditionally subsidized insurance programs, and are not required to follow HIPAA regulations.[13] Services outside of traditional healthcare treatment, such as meal-delivery services, support groups, or temporary housing, require charity or private funding. As such, primary care providers are reluctant to share patient

10. *See* Nat'l Ctr. for Chronic Disease Prevention & Health Promotion, *Health and Economic Costs of Chronic Diseases*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/chronicdisease/about/costs/index.htm#ref1 [https://perma.cc/DW9R-Y55J] ("90% of the nation's $3.5 trillion in annual healthcare expenditures are for people with chronic and mental health conditions.").

11. *See* BUTTORFF ET AL., *supra* note 9, at 10. Statistics are based on approximate spending per group (any chronic condition versus no condition) compiled by the Rand Corporation in 2014. The Centers for Disease Control and Prevention ("CDC") cites this data in its broad assertions in *supra* note 10. These figures were calculated by the author using data from Rand and the CDC.

12. *See* PATRICK RICHARD, REGINE WALKER & PIERRE ALEXANDRE, THE BURDEN OF OUT OF POCKET COSTS AND MEDICAL DEBT FACED BY HOUSEHOLDS WITH CHRONIC HEALTH CONDITIONS IN THE UNITED STATES 5–7 (2018), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0199598&type=printable [https://perma.cc/2GCD-5E9C]. For a breakdown of the cost of each chronic disease, both in terms of direct healthcare costs and indirect costs (such as lost income and reduced economic productivity), see generally HUGH WATERS & MARLON GRAF, THE COST OF CHRONIC DISEASES IN THE U.S. (2018), https://assets1b.milkeninstitute.org/assets/Publication/Viewpoint/PDF/Chronic-Disease-Executive-Summary-r2.pdf [https://perma.cc/JS9A-YCKP].

13. *See* Lynn A. Blewett, Jeanette Ziegenfuss & Michael E. Davern, *Local Access to Care Programs (LACPs): New Developments in the Access to Care for the Uninsured*, 86 MILBANK Q. 459, 459 (2008) (discussing the emergence of locally-based health-care-access programs in response to the growing number of uninsured); Erin Fries Taylor, Peter Cunningham & Kelly McKenzie, *Community Approaches to Providing Care for the Uninsured*, 25 HEALTH AFFS 173, 173 (2006), https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.25.w173 [https://perma.cc/T3AZ-ZD2C] (tracking community strategies in response to rising rates of uninsured individuals). A public alternative is safety net providers who provide patient care regardless of a patient's ability to pay. *See Practice Facilitation Handbook*, *Module 2. Working with Safety Net Practices*, AGENCY FOR HEALTHCARE RES. & QUALITY, https://www.ahrq.gov/ncepcr/tools/pf-handbook/mod2.html [https://perma.cc/G7E4-X4Q7]. However, this approach is limited to providers that receive government funding and does not encompass the full scope of actors that might be necessary for care coordination.

information to these community-based programs for fear of violating HIPAA, which creates a break in the care coordination network.

HIPAA clearly covers actors who perform certain health-care-related functions, such as billing an insurance company for medical care or making a patient referral to another healthcare specialist.[14] But HIPAA does not clearly define the scope of care coordination, instead making a mere mention of it as part of a definition for another term.[15]

Accordingly, HIPAA needs to be clarified for care coordination purposes through the Administrative Procedure Act ("APA") rulemaking process.[16] Modifying HIPAA through rulemaking is the only effective method of ensuring that healthcare entities understand the contours of permissible patient health information sharing and utilization for care coordination. However, agencies are relatively reluctant to create legally binding regulations given the complicated, time-consuming nature of the APA rulemaking procedure. Instead, they are more willing to provide administrative guidance—a nonbinding clarification that provides an administrative agency's interpretation of law. But administrative guidance falls far short in defining care coordination in the proper scope for effective healthcare delivery.

This Comment proceeds in four parts. Part I provides a background of HIPAA and how care coordination currently fits into that regulatory scheme. Care coordination requires a holistic approach between healthcare providers, health plans, social workers, and other third parties to provide adequate and effective personalized healthcare. I argue that, given the current HIPAA regulatory structure, care coordination is limited in its scope and unable to reach its full potential. Part II offers a brief overview of the APA rulemaking process and explains why issuing administrative guidance is a much easier process. Although administrative guidance is not legally binding, regulated entities generally respect guidance as if it had the same precedent as an administrative ruling. Part III analyzes the recent Office for Civil Rights ("OCR") guidance on care coordination and predicts how HIPAA-covered entities will interpret the guidance. The recent OCR guidance clarifies specific instances of patient data sharing between health plans for care coordination purposes but does not clarify care coordination generally. In Part IV, I argue that guidance from OCR is not capable of clarifying care coordination to the degree needed for effective healthcare. Instead, the Department of Health and Human Services ("HHS") should relax HIPAA restrictions surrounding sharing health information for care coordination purposes, which can only be accomplished by changing federal regulation.

14. *See* 45 C.F.R. § 160.103 (2019). For a discussion of HIPAA regulations and entities subject to HIPAA, see *infra* Section I.A.

15. *See infra* Section I.A.

16. *See infra* Section II.A.

I. HIPAA AND CARE COORDINATION BACKGROUND

HIPAA regulates the use and transmission of a patient's healthcare information by healthcare providers, healthcare plans, healthcare clearinghouses, and related business associates.[17] HIPAA regulations loosely and vaguely define care coordination, which leads to a lack of continuity of care between actors involved in care coordination. Without a clear, robust definition of which care coordination related transactions are allowed under HIPAA, actors remain hesitant to provide more than scant patient information to other actors involved in care coordination.[18] This lack of certainty leads to worse health outcomes for patients because service providers do not share the necessary information to comprehensively treat patients.[19] This section explains the mechanics of HIPAA and describes how care coordination currently fits within the existing regulatory scheme.

A. *Brief Overview of HIPAA*

1. What Is HIPAA?

Introduced in 1996, HIPAA was intended to facilitate continued insurance coverage for individuals who move between employers that provide health insurance by modernizing the flow of healthcare information.[20] Under HIPAA, HHS established policies and procedures for maintaining privacy and security of individual healthcare information, listed offenses related to healthcare, and established civil and criminal penalties for those offenses.[21]

As part of the policies and procedures, HHS enacted the HIPAA Privacy and Security Rules, establishing security standards for safeguarding protected health information ("PHI")[22] held or transferred electronically through

17. 45 C.F.R. § 164.502 (2019); *see also* Office for Civil Rights, *Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/5GPE-24A5] (listing types of entities regulated by HIPAA).

18. *See infra* notes 155–69 and accompanying text.

19. *See infra* Section III.B.

20. *See* Health Information Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.) (introducing the Act's purpose "to improve portability and continuity of health insurance coverage").

21. 42 U.S.C. § 1320a-7c(a) (2018). The statute directs the Secretary of the Department of Health and Human Services to control fraud and abuse with respect to delivery and payment of healthcare through the creation of regulations and enforcement programs. *Id.*

22. PHI refers to all "individually identifiable health information" ("IIHI") held or transmitted by a covered entity or business associate, in any form. 45 C.F.R. § 160.103 (2019) (defining protected health information). IIHI is health information created by a healthcare provider, health plan, employer, or healthcare clearinghouse that identifies the individual or with respect to which there is a "reasonable basis to believe" it can be used to identify the individual. *Id.* (defining individually identifiable health information).

administrative, technical, and physical safeguards.[23] Additionally, HHS published the HIPAA Breach Enforcement Rule which explicitly set out investigatory procedures for HIPAA violations and a civil money penalty ("CMP") schedule for those violations.[24]

In 2009, Congress updated HIPAA through the Health Information Technology for Economic and Clinical Health Act ("HITECH")[25] with the purpose of promoting and developing a nationwide health information technology infrastructure.[26] HITECH built upon the existing HIPAA Privacy and Security Rules and integrated the use of electronic health record ("EHR") systems, resulting in more specific technical requirements for electronic data sharing.[27] As a way of promoting a new health information technology infrastructure, HITECH established a "meaningful use" incentive program to promote EHR adoption and interoperability between hospital systems for the electronic exchange of patient medical records.[28]

Under the HITECH legislation, HHS established the Breach Notification Rule which requires entities subject to HIPAA to provide

23. *See* HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 (2019); HIPAA Security Rule, 45 C.F.R. §§ 160, 164 (2019). For a summary of the Privacy Rule, including a compilation of the relevant code sections, see Office for Civil Rights, *The HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (Apr. 16, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/4EZ7-ZL2W]. For a summary of the Security Rule, including a compilation of the relevant code sections, see Office for Civil Rights, *The Security Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (May 12, 2017), https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/V66U-JDLN].

24. *See* HIPAA Enforcement Rule, 45 C.F.R. § 160 (2019). For a summary of the Enforcement Rule, including a compilation of the relevant code sections, see Office for Civil Rights, *The HIPAA Enforcement Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html [https://perma.cc/D7HC-MM4M]. For a more detailed explanation of PHI and the information that HIPAA covers, see *infra* Section I.A.3.

25. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.). The majority of HITECH rules discussed in this paper are also located in the Code of Federal Regulations.

26. 42 U.S.C. § 300jj-11(b) (2018) ("[HHS] shall perform the duties . . . in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information."); *see also* Office for Civil Rights, *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html [https://perma.cc/5S3A-CNGA]. *See generally* David Blumenthal, *Launching HITECH*, 362 NEW ENG. J. MED. 382 (2010) (providing background information on the healthcare industry leading up to the introduction of HITECH).

27. *See* 42 U.S.C. § 300jj-14(b)(1) (2018) ("[T]he [HHS] shall . . . adopt an initial set of standards, implementation specifications, and certification criteria [consistent with this title].").

28. *See id.* § 1395w-4(o) ("[I]f the eligible professional is a meaningful EHR user . . . for the EHR reporting period . . . [the professional] shall be paid . . . from the Supplemental Medical Insurance Trust Fund."). For a distilled description of the meaningful se incentive program and goals, see also *Public Health and Promoting Interoperability Programs*, *Introduction*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/ehrmeaningfuluse/introduction.html [https://perma.cc/K33X-9DHY].

notification following breaches of PHI.[29] Breaches are generally defined as an impermissible use or disclosure that compromises the security or privacy of PHI.[30] Following breaches, entities are required to provide notification to the individuals affected and report the breach to OCR,[31] which works in collaboration with HHS to enforce HIPAA. In 2013, HHS published the Final Omnibus Rule, which expanded these notification requirements and provided more stringent technical updates to the HIPAA Security Rule.[32] The Breach Notification Rule now requires third parties working with regulated parties to report breaches[33] and tightens the breach standard to a presumed impermissible violation.[34]

OCR, as the HHS enforcement division for HIPAA, is tasked with ensuring that regulated entities understand and comply with HIPAA requirements, increasing the general public's awareness of their HIPAA rights and protections, and investigating potential violations.[35] OCR accomplishes these goals by issuing regulations and guidance that clarify existing HIPAA implementation, conducting outreach to regulated entities, and providing technical assistance to resolve substantial noncompliance.[36] Additionally, OCR pursues investigations based on public complaints of violations and seeks to resolve claims by obtaining voluntary compliance, corrective action, and/or a resolution agreement.[37] In rare cases where the regulated entity fails to take

29. *See* HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414 (2019).

30. *See id.* § 164.402 (defining breach); *see also* Office for Civil Rights, *Breach Notification Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/CTH7-VFRQ].

31. § 164.404 ("A covered entity shall, following the discovery of a breach . . . notify each individual whose unsecured [PHI] has been . . . [compromised] as a result of such breach."); *id.* § 164.408 ("A covered entity shall, following the discovery of a breach . . . , notify the [OCR].").

32. *See* Final Omnibus Rule, 78 Fed. Reg. 5566, 5702 (Jan. 25, 2013) (codified as 45 C.F.R. Parts 160 and 164); *see also* Office for Civil Rights, *Omnibus HIPAA Rulemaking*, U.S. DEP'T HEALTH & HUM. SERVS. (Sept. 13, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html [https://perma.cc/935J-SQEM].

33. § 164.410 ("A [third party] shall, following the discovery of a breach . . . , notify the covered entity of such breach."). The third party here refers to business associates, which is defined in Section I.A.2.

34. *Id.* § 164.402 (defining breach and stating that the unauthorized use of PHI is "presumed to be a breach unless the [entity] . . . demonstrates that there is a low probability that the [PHI] has been compromised").

35. *See* Office for Civil Rights, *About Us*, U.S. DEP'T HEALTH & HUM. SERVS. (Oct. 8, 2019), https://www.hhs.gov/ocr/about-us/index.html [https://perma.cc/92F8-MT9U].

36. *See id.*

37. 45 C.F.R. § 160.312 (2019); *see also* Office for Civil Rights, *How OCR Enforces the HIPAA Privacy & Security Rules*, U.S. DEP'T HEALTH & HUM. SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html [https://perma.cc/X8QA-ZEZ5].

action to resolve a HIPAA violation, OCR may impose CMPs[38] or even refer the case to the Department of Justice ("DOJ") if the complaint implicates a potential criminal violation.[39]

2. Who Does HIPAA Cover?

HIPAA is applicable only to three types of entities: health plans,[40] clearinghouses,[41] and certain healthcare providers.[42] Of those types, "covered" entities are those that perform transactions, which are defined as the transmission of information to carry out "financial or administrative activities related to healthcare."[43] While not every type of entity interacts with health information the same way, all covered entities need to comply with the HIPAA Privacy and Security Rules. Conversely, noncovered entities do not fall within HIPAA's reach and therefore do not have to meet its stringent requirements

38. § 160.402 ("[OCR] will impose a civil money penalty . . . if the [OCR] determines the [entity] has violated [a HIPAA] provision."); *see also* Office for Civil Rights, *supra* note 37.

39. *See* 42 U.S.C. § 1320d-6 (2018) (detailing what constitutes a criminal violation of HIPAA rules); *see also* Office for Civil Rights, *How OCR Enforces*, *supra* note 37 (stating that violations of the criminal provision of HIPAA may be referred to the DOJ).

40. Health plans cover some healthcare costs for their subscribers. Health plans generally receive health information regarding a patient's diagnosis and treatment to determine what portion of those services to cover. Health plans include an individual or group plan that "provides, or pays the cost of, medical care." 45 C.F.R. § 160.103 (2019) (defining health plan). This may come in many forms, including government social services (for example, Medicare and Medicaid); private insurance through employers or educational institutions; private insurance through the Health Insurance Marketplace; and other public and private sources. *See, e.g.*, *Health Insurance Marketplace*, HEALTHCARE.GOV, https://www.healthcare.gov/glossary/health-insurance-marketplace-glossary/ [https://perma.cc/7DE5-3PFM]. The Marketplace provides health plan shopping and enrollment through services based on an individual's or family's income and household information. *Id.* The Marketplace is a federal program, although thirteen states run their own marketplaces. *The Marketplace in Your State*, HEALTHCARE.GOV, https://www.healthcare.gov/marketplace-in-your-state/ [https://perma.cc/L6HG-F4K5].

41. Healthcare clearinghouses are thought of as the middlemen between covered entities that create health information and those that maintain health information. Healthcare clearinghouses are third-party systems that interpret claim data between healthcare providers and insurance companies or health plans, sending encrypted patient information and interpreting said encryptions. § 160.103 (defining healthcare clearinghouse). Specific functions include: receiving a transaction with health information that is "nonstandard format or containing nonstandard data content" and assisting with the conversion into "standard data elements or a standard transaction" for the transmitting covered entity; or receiving a standard transaction and assisting with the conversion into "nonstandard format or nonstandard data content" for the receiving covered entity. *Id.* Examples of healthcare clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches. *Id.*

42. *Id.* § 160.102(a).

43. *Id.* § 160.103 (defining transaction). Examples include healthcare claims, healthcare payment, coordination of benefits, healthcare claim status, enrollment and disenrollment for a health plan, eligibility for a health plan, healthcare premium payments, referral certification and authorization, first report of injury, health claims attachments, and healthcare electronic funds transfers. *Id.*

for handling and storing data, regardless of what type of information they have.[44]

While healthcare plans and clearinghouses do little more than either pay for or convert healthcare information, healthcare providers interact with, create, and maintain health information. Providers fall under the covered entity definition only if they engage in exchanges of information to carry out a financial or administrative activity related to healthcare, or "transactions."[45] Providers can include any person, business, or agency that "furnishe[s], bills, or is paid for, healthcare in the normal course of business."[46] Colloquially, providers can include any healthcare professional who provides health services and bills for those services, ranging from the individual practitioner to the largest hospital systems.

Healthcare providers constitute the largest number of all covered entities and generally interact the most with patients and their health information. As such, they are at greater risk for noncompliance with HIPAA considering the various provisions that healthcare providers need to meet. In 2019 alone, there were 396 violations by healthcare providers, constituting 77.65% of breaches total.[47]

While the covered entities—healthcare providers, plans, and clearinghouses—cover a majority of clinical treatment and billing, many other third-party actors are significantly involved in the medical industry. If the third parties need to handle PHI in any manner, they fall under the business associate definition under HIPAA and are subject to its Security and Privacy Rules.[48] Business associates are third-party persons or organizations that perform activities on behalf of, or provide certain services to, a covered entity that uses or discloses PHI.[49] Business associates might create, receive, maintain, or transmit for or on behalf of a covered entity. When covered entities utilize business associates, HIPAA requires the parties to sign a business associate

44. *Id.*

45. *Id.* § 162 (providing transaction standards established by HIPAA Transactions Rule). Examples of covered transactions include claims, benefit eligibility queries, and referral authorization requests. *Id.* § 160.103.

46. *Id.* (defining healthcare provider).

47. *2019 Healthcare Data Breach Report*, HIPAA J. (Feb. 13, 2020), https://www.hipaajournal.com/2019-healthcare-data-breach-report/ [https://perma.cc/NMV4-ECCD]. Of the total number of breaches in 2019, health plan breaches constituted 11.57% (59 violations), healthcare clearinghouses constituted 0.39% (2 violations), and business associates constituted the remaining 23.3% (53 violations). *Id.* Data pulled from Office for Civil Rights, *Breach Portal*, *Cases Currently Under Investigation*, U.S. DEP'T HEALTH & HUM. SERVS. (updated daily), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [https://perma.cc/Q86D-6ZFG]. HHS keeps a running list of cases currently under investigation, also known in the healthcare community as the "Wall of Shame." *What Is the HIPAA Wall of Shame?*, COMPLIANCY GROUP, https://compliancy-group.com/what-is-the-hipaa-wall-of-shame/ [https://perma.cc/QYC4-9QAK].

48. *See* § 160.103 (defining business associate).

49. *Id.*

agreement that imposes specific written safeguards for their use or disclosure of PHI.[50] Business associate agreements must detail the scope and limitations for use and disclosure by the business associate.[51]

HIPAA's administrative, physical, and technical safeguards are numerous; however, they are merely guidelines and standards for compliance. HIPAA requirements are flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments.[52] What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.[53] In deciding the security standards to use, entities need to take into account their "size, complexity, and capabilities"; "technical infrastructure, hardware, and software security capabilities"; the cost of security measures; and the "probability and cruciality" of risks to PHI.[54]

Given the number of various factors and requirements, HIPAA regulations do not provide a clear determination of what policies each entity needs to employ to be compliant. For example, a large healthcare conglomerate that has hospitals and clinics across multiple states will need to consider how to manage sharing health information within the organization, with insurance companies or Medicare, and with providers outside of the organization, all while ensuring that each location has the appropriate technical capabilities to handle data protection and the appropriate level of access for each employee (such as a physician, nurse, scheduling assistant, or billing professional), contractor, and patient (through patient portals). This type of organization has very complicated needs to ensure that it follows HIPAA requirements, necessitating a multitude of compliance personnel, advanced hardware to handle data storage, and secure methods for sharing health information. Contrast this scenario with a regional hospital that is the only health provider within a 100-mile radius and handles all the healthcare for a rural community. The regional hospital will need far less to comply with HIPAA since there is a smaller need to share PHI outside of the community. Ultimately, HIPAA regulations, while flexible, are numerous and complex in nature, making it hard for covered entities to ensure they comply.

50. *Id.* §§ 164.502(e), 164.504(e) (requiring that covered entities obtain assurance of compliance with HIPAA when contracting with business associates).

51. *Id.*

52. *Id.* § 164.306(b)(1) ("Covered entities and business associates may use any security measures that allow the [entity] to reasonably and appropriately implement the standards and implementation specifications as specified in [the HIPAA Security Rule].").

53. *Id.* § 164.306(b)(2).

54. *Id.*

3. What Information Does HIPAA Cover?

HIPAA protects against unlawful access of patient health data and requires that covered entities and business associates create safeguards that ensure the confidentiality, integrity, and availability of protected health information, or PHI. PHI refers to all "individually identifiable health information" that is related to the past, present, or future health status of an individual that is held or transmitted by a covered entity or its business associate in any form or medium.[55] Additionally, PHI includes health data for which there is a "reasonable basis" to believe that such health information can be used to identify an individual patient.[56] This can include information such as diagnoses, treatment information, hospital bills, medical test results, and prescription information.[57] Nonmedical information including national identification numbers (for example, Social Security numbers), and demographic information such as birth dates, gender, ethnicity, and contact information can also qualify as PHI.[58]

In order for individual data to qualify as PHI, there needs to be some sort of relationship with health information; sharing nonmedical information that is identifying alone without any health information does not necessarily classify the information as PHI.[59] For example, a person's residential address that is part of a public tax database would not be PHI since there is no link to health information. On the other hand, if the same person's residential address was listed on a hospital bill it could then qualify as PHI.

Furthermore, the health information must in some way identify the individual, either directly or via a reasonably possible pathway.[60] Although patient information such as a date of birth does not in itself identify a singular person, the combination of the date of birth and the fact that the patient was treated at a particular outpatient cancer clinic makes it much easier to find the individual; thus, there is a reasonable basis to believe that the date of birth in a specific healthcare context is enough to identify a person.

55. *Id.* § 160.103 (defining protected health information). Health information can still qualify as PHI even if it is not held or transmitted in electronic media. *Id.*

56. *Id.*

57. *See id.*; *see also* Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (Nov. 6, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected [https://perma.cc/37EY-KMZV] (listing examples of PHI). However, there are some examples of individually identifiable health information that do not qualify as PHI, such as education records covered by the Family Education Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 574 (codified as amended at 20 U.S.C. § 1232g (2018)); employment records held by a covered entity in its role as an employer; and data of persons who have been deceased for more than 50 years. § 160.103.

58. *See* § 160.103; *see also* Office for Civil Rights, *supra* note 57.

59. Office for Civil Rights, *supra* note 57.

60. § 160.103.

Conversely, there are no restrictions on sharing PHI that has been de-identified.[61] De-identified information is simply PHI that has been scrubbed or transformed so that the information is no longer individually identifying or there is no longer a reasonable basis to believe that the information can be used to identify an individual.[62] One example of de-identification is the use of aggregate data. Although aggregate data is derived from individual patient records from a particular population set, the aggregation is determined through statistical methods that effectively mask each individual.[63] While HIPAA's security requirements still apply to de-identified PHI, covered entities are no longer subject to normal restrictions for sharing such data.[64]

Finally, HIPAA protections do not necessarily follow PHI once it has left a covered entity or business associate.[65] Under the individual right of access, a patient can request access to their PHI from a covered entity or even direct the covered entity to share it with a third-party.[66] Once the PHI has left the HIPAA-regulated entity to a noncovered entity (including the patient herself), there are no restrictions on using the PHI and there are also no administrative or technical safeguards protecting the privacy of the data.

The regulations surrounding what health information is protected under HIPAA as PHI are complex and further complicated by restrictions on how that PHI is used by covered entities.[67] This can create doubt among HIPAA-regulated entities regarding when it is safe to share PHI outside of their organization and when such sharing will lead to a HIPAA violation.

4. How Can Entities Use and Disclose PHI Under HIPAA?

As entities subject to regulations under HIPAA, covered entities and business associates are restricted in the ways that they can share patient data and the amount they can share. There are four pathways through which PHI can be used and disclosed: (1) required disclosures by law; (2) permitted uses

61. *See Id.* § 164.502(d)(2) (providing standards for using and disclosing de-identified PHI); *see also* Office for Civil Rights, *supra* note 57.

62. *Id.* § 164.514(a) (defining de-identification of PHI). There are two methods for de-identification: the expert determination and safe harbor methods. *See id.* § 164.514(b). The expert determination method applies statistical and scientific principles to render the information not individually identifiable. *See id.* § 164.514(b)(1). The safe harbor method removes particular identifiers from the health data. *See id.* § 164.514(b)(2) (including examples such as names, geographical identifiers, dates, and phone numbers).

63. For example, a health plan report that lists the average age of persons subscribed to the plan would not qualify as PHI. *See id.* § 164.514(a)–(b). Although the report is derived from patient ages from each health plan's subscription records, which each qualify as PHI, the report only shows the aggregated data in which there is no reasonable way to identify any individual patient. *See id.*

64. See *supra* notes 60–61 and accompanying text.

65. *See* 45 C.F.R. § 164.524(a)(1) (2019) (requiring that covered entities and business associates provide patients with access to their health information upon request).

66. *See id.*

67. *See infra* Section I.A.4.

and disclosures; (3) uses and disclosures that require express authorization from an individual;[68] and (4) the individual right of access.[69] Except for the permitted uses and disclosures pathway, the other pathways generally rely on other actors to allow PHI sharing to go forward.[70]

Under the permitted uses and disclosures pathway, covered entities and business associates have the discretion to share PHI without external actors prompting the action.[71] Specifically, covered entities are permitted, but not required, to use and disclose PHI without an individual's authorization for a variety of purposes with the most salient reasons being for treatment, payment, or healthcare operations, also known as "TPO."[72]

Sharing PHI for TPO purposes, however, is also subject to the "minimum necessary" principle, which requires that a covered entity make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose.[73] HIPAA does not precisely define what the minimum necessary principle entails, but instead relies upon the individual covered entity or business associate to determine its proper scope.[74]

68. 45 C.F.R. § 164.508(a) (2019). Excluding certain exceptions, covered entities and business associates may not use or disclose PHI without valid authorization from the patient. *Id.*

69. *Id.* § 164.502(a)(1) (listing permitted uses and disclosures, required disclosures, and prohibited uses and disclosures for covered entities and business associates). The individual right of access itself is a specific instance of a required disclosure. Other required disclosures include to HHS for purposes of compliance investigation or some other legal requirement. *Id.* § 164.502(a)(2).

70. For example, the individual right of access allows a patient to request an entity maintaining her PHI to deliver a copy of that PHI for personal inspection or to send it to a third party, without restriction on what that third-party entity is. *See id.* §§ 164.524(a)(1), 164.528(a). Similarly, required disclosures by law depend on some mandate contained in law (e.g. statute, regulation, or court order) to compel PHI sharing to a particular government authority or other party. *See id.* §§ 164.103, 164.512(a). Finally, of particular note, the pathway requiring express authorization from the patient has very stringent requirements but is essentially a catch-all if the use or disclosure does not fall under another pathway. *See id.* § 164.508 (providing for a general rule and specific instances where authorizations are required). An authorization is a detailed document that gives covered entities permission to use PHI for specified purposes, typically other than for TPO (treatment, payment, or healthcare operations) purposes. *See id.* § 164.508(c); *see also* Office for Civil Rights, *What Is the Difference Between "Consent" and "Authorization" Under the HIPAA Privacy Rule?*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html [https://perma.cc/8XRL-6352].

71. § 164.502(a)(1).

72. Additionally, covered entities are allowed to provide PHI: (1) to the individual, (2) where the individual has an opportunity to agree or object, (3) incident to an otherwise permitted use and disclosure, (4) for public interest and benefit activities, and (5) limited data set for purposes of research, public health, or healthcare operations. *Id.*

73. *Id.* §§ 164.502(b), 164.514(d)(1)–(4).

74. *See id.* § 164.514(d)(3) ("[A] covered entity must implement policies and procedures . . . that limit the [PHI] disclosed to the amount reasonably necessary to achieve the purpose of the disclosure."); *see also* Office for Civil Rights, *Minimum Necessary Requirement*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html [https://perma.cc/3VAW-FESS] (requiring covered entities to evaluate their practices and enhance safeguards to protect against inappropriate PHI access).

Unfortunately, there is scarce judicial clarification for what the minimum necessary principal entails,[75] and HHS has only provided clarification through a series of FAQs[76] and explicit carveouts in its regulations.

The main regulatory carveout provides that the minimum necessary principle does not apply to transactions between covered healthcare providers for healthcare treatment[77] purposes.[78] Other regulatory carveouts include disclosures to a patient under the individual right of access, disclosure done with express authorization from the patient, disclosures made to HHS, and other disclosures as required by law.[79] As such, most activities for TPO purposes are subject to the minimum necessary principle, except for the particular provider-to-provider situation for treatment purposes.[80] The minimum necessary principle, though seemingly flexible in application, looms over covered entities and business associates in every TPO action they take.

The OCR FAQs cover topics such as the purpose behind the minimum necessary principle, how the principle interacts and conflicts with certain HIPAA regulations and purposes, and specific examples where the principle does or does not apply.[81] While the FAQs are helpful in clarifying many fundamental questions about the minimum necessary principle and why HHS implemented such a restriction, the FAQs provide only a few particular examples of permitted PHI usage and do not provide guidance in many other health-related scenarios. Beyond the restrictions created by the minimum necessary principle, HIPAA-regulated entities have broad authority to use and disclose PHI if done for TPO purposes.

75. *See, e.g.*, Citizens for Health v. Leavitt, 428 F.3d 167, 173 (3d Cir. 2005) (quoting from the regulation but not providing additional clarification); Harrold-Jones v. Drury, 422 P.3d 568, 573 (Alaska 2018) (confirming that minimum necessary does not apply for disclosures for legal proceeding, but not providing general clarification); Stevens *ex rel.* Stevens v. Hickman Cmty. Health Care Servs., Inc., 418 S.W.3d 547, 558 (Tenn. 2013) (directly quoting the regulation without clarification).

76. *See* Office for Civil Rights, *FAQ: Minimum Necessary*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/minimum-necessary/index.html [https://perma.cc/M96U-79MH].

77. Treatment is further defined later in this section. *See infra* note 82 and accompanying text.

78. § 164.502(b)(2)(i). The final rule from HHS removed the minimum necessary principal for uses and disclosures of PHI between providers for treatment purposes. 65 Fed. Reg. 82,461, 82,712–13 (Dec. 28, 2000). Commentators to the proposed rule argued that the application of the principal for providers would be "contrary to sound medical practice, increase medical errors, and lead to an increase in liability." *Id.* at 82,712. Additionally, commentators mentioned that the "complexity of medicine" is such that it would be unreasonable to know exactly what medical information is relevant to another caregiver in developing proper diagnosis and treatment. *Id.* at 82,713.

79. § 164.502(b)(2)(ii), (iv), (v).

80. *See id.* § 164.502(b).

81. Office for Civil Rights, *supra* note 74. Specific examples include whether the minimum necessary principle applies to medical students, for documentation to an external institutional review board, for worker's compensation systems, and for plaintiffs or defendants requesting information in litigation. *Id.*

Treatment encompasses the medical care provided to patients and is the broadest category of TPO. Treatment generally means the "provision, coordination, or management of healthcare and related services" between healthcare providers or with a third party, consultation between healthcare providers regarding a patient, or patient referral from one healthcare provider to another.[82] Treatment includes traditional treatment and diagnosis, but also includes making and receiving referrals as well as coordination or management of healthcare and related services by a provider, even if the action is through a hired third party.

Payment encompasses various activities of healthcare providers to obtain payment or reimbursement for their services in addition to activities of health plans to obtain premiums, fulfill coverage responsibilities, provide benefits under the plan, and provide reimbursement for the provision of healthcare.[83] Examples of this include determining eligibility or coverage under a plan and adjudicating claims; risk adjustments; billing and collection activities; reviewing healthcare services for medical necessity, coverage, justification of charges, and the like; utilization review activities; and disclosures to consumer reporting services.[84]

Healthcare operations constitute certain administrative, financial, legal, and quality improvement activities of a covered entity necessary to run its business and support the functions of treatment and payment.[85] Activities that fall under healthcare operations are specifically enumerated in the regulation.[86] Examples include conducting quality assessments and improvement activities, population-based activities related to improving healthcare or reducing healthcare costs, case management and care coordination,[87] and numerous other activities.[88]

Under the TPO exceptions, covered entities and business associates have relatively broad authority to share PHI without a patient's express authorization. For the purposes of care coordination, this seems beneficial in sharing PHI to healthcare actors at various stages of a patient's treatment. But despite this seemingly broad authority, HIPAA-regulated entities must still consider the minimum necessary principle in their uses and disclosures under TPO. Although the minimum necessary principle is a standard, and as such is flexible in its application, it relies on covered entities and business associates to determine what that "minimum necessary" amount of PHI is. Additionally, the

82. 45 C.F.R. § 164.501 (2019) (defining treatment).
83. *Id.* (defining payment).
84. *See id.*
85. *Id.* (defining healthcare operations).
86. *See id.*
87. *See infra* Section I.C.
88. § 164.501 (defining healthcare operations).

minimum necessary principle has vague wording with little clarification provided by HHS. As such, HIPAA-regulated entities will generally err on the side of sharing as little as possible for fear of violating HIPAA.[89] The minimum necessary principle's interaction with TPO makes fully effective care coordination an insurmountable challenge, as discussed in Section I.C.

B. *Care Coordination and the Medically Indigent*

Care coordination has been defined as intentionally "organizing patient care activities and sharing information among all of the participants concerned with a patient's care to achieve safer and more effective care,"[90] the "management of interdependencies among [healthcare-related] tasks,"[91] and various other definitions.[92] Care coordination may include: (1) functions to "ensure that [a] patient's needs and preferences are met over time"; (2) sharing of information across the "people, functions, and sites" of the care process; and (3) deliberate organization of care activities across participants in the care process, including the patient herself.[93] Care coordination has even been included as part of case management, which is the "activity that assists individuals . . . in gaining access to medical, social, educational or other services"—but it does not consist of the underlying service itself.[94]

While the definition of care coordination is inconsistent, the ultimate goal of care coordination is to meet the needs and preferences of the patient through the delivery of high-quality and high-value healthcare.[95] This means communicating a patient's particular needs and preferences at the right time to the right people involved in guiding safe, appropriate, and effective care. Well-

89. *See infra* notes 155–60 and accompanying text.

90. *See Care Coordination*, *supra* note 5.

91. Jody Hoffer Gittell, *Coordinating Mechanisms in Care Provider Groups: Relational Coordination as a Mediator and Input Uncertainty as a Moderator of Performance Effects*, 48 MGMT. SCI. 1408, 1408 (2002).

92. For other state definitions of care coordination, see generally Jane Hyatt Thorpe & Katherine Hayes, *Selected Provisions from Integrated Care RFPs and Contracts: Care Coordination*, INTEGRATED CARE RESOURCE CTR. 3–4 (July 2013), https://www.integratedcareresourcecenter.com/sites/default/files/ICRC_Care_Coordination_FINAL_7_29_13_0.pdf [https://perma.cc/9HNZ-4P8F] (summarizing care coordination definitions from Arizona, Massachusetts, Minnesota, Tennessee, and Texas).

93. AM. NURSES ASS'N, THE VALUE OF NURSING CARE COORDINATION 1–2 (2012), https://www.nursingworld.org/~4afc0d/globalassets/practiceandpolicy/health-policy/care-coordination-white-paper-3.pdf [https://perma.cc/MJ7P-86XM].

94. Medicaid Program; Optional State Plan Case Management Services, 72 Fed. Reg. 68,077, 60,878–79 (Dec. 4, 2007) (codified as 42 C.F.R. §§ 431, 440, 441 (2019)) (internal quotations omitted). For a detailed, nonexhaustive list of case management functions provided by the Centers for Medicare & Medicaid Services ("CMS"), see generally CTRS. FOR MEDICARE & MEDICARE SERVS., INSTRUCTIONS, TECHNICAL GUIDE AND REVIEW CRITERIA: APPLICATION FOR A 1915(C) HOME AND COMMUNITY-BASED WAIVER 105 (2015), http://nasddds.org/uploads/documents/Version3.5InstructionsJan2015.pdf [https://perma.cc/57C6-SUUY].

95. *Care Coordination*, *supra* note 5.

designed and targeted care coordination can improve outcomes for all parties involved—patients, providers, and payers.[96] Care coordination serves to "bend the cost curve downward" by increasing the efficiency of gathering information about a patient and thus reducing costs of medical care through collaboration.[97] Additionally, care coordination can "make providers accountable for quality and outcomes, not just delivering care."[98]

Utilizing care coordination strategies has been shown to improve the health outcomes of patients in several different contexts, including primary care,[99] acute care,[100] and long-term care.[101] Care coordination can reduce the number of hospital days, hospital readmissions, emergency department visits, and home healthcare episodes while also saving significant healthcare costs.[102] Additionally, care coordination can be an incredible tool for improving health outcomes in rural communities, many of which have higher rates of poor physical and mental health, poverty, and unemployment than the state or national average.[103] Furthermore, care coordination can increase patient

96. *See infra* note 102 and accompanying text.

97. Y. Tony Yang & Mark R. Meiners, *Care Coordination and the Expansion of Nursing Scopes of Practice*, 42 J.L. MED. & ETHICS 93, 93 (2014).

98. David Ivers, *Conflict-Free Case Management on Collision Course with Integrated Care*, 28 HEALTH L., Apr. 2016, at 19, 23.

99. Primary care coordination, also known as guided care, aims to care for patients with chronic diseases and conditions such as heart disease and cancer. NEJM Catalyst, *What is Care Coordination?*, MASS. MED. SOC'Y (Jan. 1, 2018), https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0291 [https://perma.cc/ZG7C-HJVE].

100. Acute care coordination is intended for patients who suffer from acute health problems such as a stroke or heart attack, which require critical and emergency care. *Id.*

101. Long-term or post-acute care coordination is intended for patients who are rehabilitating from acute conditions or need long-term healthcare facilities, necessitating movement between facilities based on the patient's progression. *Id.*

102. AM. HOSPITAL ASS'N, THE ROLE OF POST-ACUTE CARE IN NEW CARE DELIVERY MODELS 5–10 (2015) (highlighting case studies where implementing post-acute care coordination has improved hospital readmission rates and improved patient satisfaction when being transferred between healthcare facilities); Bruce Leff et al., *Guided Care and the Cost of Complex Healthcare: A Preliminary Report*, 15 AM. J. MANAGED CARE 555, 555 (2009) (finding, on average, that patients in a guided care subset experienced 24% fewer hospital days, 37% fewer skilled nursing facility days, 15% fewer emergency department visits, 29% fewer home healthcare episodes, and saved $1364 per patient); Dave Russell, Mary VorderBruegge & Suzanne M. Burns, *Effect of an Outcomes-Managed Approach to Care of Neuroscience Patients by Acute Care Nurse Practitioners*, 11 AM. J. CRITICAL CARE 353, 353 (2002) (finding patients in an acute care subset had significantly shorter overall length of stay, shorter mean length of stay in intensive care, and lower rates of infections); Martha Hostetter et al., *Guided Care: A Structured Approach to Providing Comprehensive Primary Care for Complex Patients*, COMMONWEALTH FUND (Oct. 18, 2016), https://www.commonwealthfund.org/publications/case-study/2016/oct/guided-care-structured-approach-providing-comprehensive-primary?redirect_source=/publications/case-studies/2016/oct/guided-care [https://perma.cc/8ND2-Y96B] (finding patients in a guided care subset showed a 15% reduction in hospital admissions, a 48.7% reduction in 30-day readmissions, a 20.7% reduction in hospital days, and a 17.4% reduction in emergency department visits).

103. Pat Conway et al., *Rural Health Networks and Care Coordination: Health Care Innovation in Frontier Communities To Improve Patient Outcomes and Reduce Health Care Costs*, 27 J. HEALTH CARE

confidence in their healthcare team, improve patient engagement, improve health outcomes, and reduce costs.[104] As such, care coordination has proven to be a flexible and vital tool for managing care for people of disparate socioeconomic backgrounds across a variety of health contexts.

While there are many different care coordination models, they all envision a patient's health management through strategic and cooperative team care, requiring integration between all medical providers, payers, social service agencies, and community-based support programs.[105] As such, nonclinical services such as social services and community-based support programs are increasingly "associated with better satisfaction with care, quality of care, quality of life, and survival."[106] Effective community health and social workers must have the ability to "work cooperatively with other members of the multidisciplinary treatment team that are directly involved in a patient's care."[107] In this sense, care coordination can be thought of as a "team sport" that requires strong infrastructure, resources, leadership, and culture to effectively

FOR POOR UNDERSERVED 91, 107 (2016) (observing a rural population in Ely, Minnesota and finding some patient quality of life improvement with drastically reduced emergency department use).

104. *See* Sara Heath, *Care Coordination Across Provider Networks Creates Patient Trust*, PATIENT ENGAGEMENT HIT (Nov. 20, 2017), https://patientengagementhit.com/news/care-coordination-across-provider-networks-creates-patient-trust [https://perma.cc/RD2S-CDWA] (describing how care team collaboration directly influences patient and family trust); Mark M. Nunlist et al., *Using Health Confidence To Improve Patient Outcomes*, 23 FAM. PRAC. MGMT, Nov./Dec. 2016, at 21, 21–22 (mentioning care coordination interventions as improving patient confidence).

105. *See, e.g.*, John D. Burchard, Eric J. Bruns & Sara N. Burchard, *The Wraparound Process*, *in* COMMUNITY TREATMENT FOR YOUTH 1 (2002) (focusing on intensive, individualized care management for youths within complex service delivery approaches); CATHERINE CRAIG, DOUG EBBY & JOHN WHITTINGTON, CARE COORDINATION MODEL: BETTER CARE AT LOWER COST FOR PEOPLE WITH MULTIPLE HEALTH AND SOCIAL NEEDS 1 (2011) (supporting a methodical approach to delivering coordination services); Victoria M. Rozzi et al., *AIMS: A Care Coordination Model to Improve Patient Health Outcomes*, 41 HEALTH & SOC. WORK 191, 191 (2016) (advocating for a social work interventional model); *Community Care Coordination—The Marriage of Health and Social Service Providers*, ECCOVIA SOLUTIONS (July 6, 2017), https://eccoviasolutions.com/community-care-coordination-the-marriage-of-health-and-social-service-providers/ [https://perma.cc/J76F-7UED] (recommending a community-based health neighborhood including health providers and community support providers); *Overview*, NURSE-FAMILY PARTNERSHIP (2020), https://www.nursefamilypartnership.org/wp-content/uploads/2020/03/NFP-Overview.pdf [https://perma.cc/EKL6-UWW4] (creating an evidence-based home visiting program that pairs low income first-time mothers with maternal and child health nurses); *Program of All-Inclusive Care for the Elderly*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.medicaid.gov/medicaid/long-term-services-supports/program-all-inclusive-care-elderly/index.html [https://perma.cc/WB2H-BKGU] (generating a comprehensive service package that allows the elderly to remain in the community rather than in a nursing home).

106. Patricia J. Volland et al., *The Transitional Care and Comprehensive Care Coordination Debate*, GENERATIONS, Winter 2012–13, at 13, 16.

107. Yang & Meiners, *supra* note 97, at 98 (discussing the importance of social services for hospital transition programs).

support the synchronized efforts, communication, and collaboration of multidisciplinary provider teams.[108]

An example of care coordination in action illustrates how important it can be in improving long-term health outcomes. Suppose a patient arrives at the emergency department ("ED") with an unknown health condition and symptoms including frequent urination, increased thirst, and increased hunger. The ED facility triages our patient based on an initial determination of the severity of her condition. Since her symptoms do not seem immediately life-threatening, her ED physician or nurse then evaluates her condition to determine immediate treatments and suggests subsequent labs or tests via the patient's EHR.

Our patient is then transferred out of the ED to another department, possibly an outpatient clinic, where another provider takes over. The provider, typically an attending physician or nurse, views the patient's EHR and, based on the ED provider's recommendation, performs initial treatments and submits imaging, lab, and consult orders. Our patient continues to be shuffled around to other departments, possibly radiology,[109] nephrology,[110] or endocrinology,[111] while a plethora of healthcare providers access the patient's EHR and enter orders, results, and comments.

Finally, our patient's attending physician presents the patient's diagnosis: Type 2 diabetes.[112] The physician develops a care plan around the disease that

108. NEJM Catalyst, *supra* note 99.

109. Radiology uses imaging techniques such as X-ray, computed tomography ("CT"), and magnetic resonance imaging ("MRI") to diagnose and treat diseases. Nat'l Cancer Inst., *Radiology*, NAT'L INST. HEALTH, https://www.cancer.gov/publications/dictionaries/cancer-terms/def/radiology [https://perma.cc/HM2H-NFQ2].

110. Nephrology is a specialty that involves diagnosing and treating kidney disease. Nat'l Cancer Inst., *Nephrologist*, NAT'L INST. HEALTH, https://www.cancer.gov/publications/dictionaries/cancer-terms/def/nephrologist [https://perma.cc/2HGF-KPMU].

111. Endocrinology involves diagnosing and treating disorders of the endocrine system, which contains glands and organs that produce hormones. Nat'l Cancer Inst., *NCI Dictionary of Cancer Terms*, *Endocrinology*, NAT'L INST. HEALTH, https://www.cancer.gov/publications/dictionaries/cancer-terms/def/endocrinology [https://perma.cc/LE3U-CCGH].

112. Diabetes is a chronic disease characterized by elevated levels of blood sugar. *Diabetes: Overview*, WORLD HEALTH ORG., https://www.who.int/health-topics/diabetes#tab=tab_1 [https://perma.cc/A84J-T9JZ]. Type 2 diabetes occurs when the body becomes resistant to insulin, a hormone that reduces blood sugar levels, or fails to make enough insulin. *Id.* Symptoms include those described at the beginning of the scenario: frequent urination, increased thirst, increased hunger, in addition to unintended weight loss, blurred vision, headaches, fatigue, slow healing of cuts, and itchy skin. *Diabetes: Symptoms*, WORLD HEALTH ORG., https://www.who.int/health-topics/diabetes#tab=tab_2 [https://perma.cc/JK4M-4BMK]. Approximately 422 million people worldwide suffer from diabetes, particularly in low- and middle-income countries, with 1.6 million deaths per year attributable to diabetes. *Diabetes: Overview*, *supra*. As of a 2020 Centers for Disease Control and Prevention report, 34.2 million U.S. people—or 10.5% of the U.S. population—suffer from diabetes, with an estimated 7.3 million people undiagnosed. CTRS. FOR DISEASE CONTROL & PREVENTION, NATIONAL DIABETES STATISTICS REPORT, 2020, 2 (2020), https://www.cdc.gov/diabetes/pdfs/data/statistics/national-diabetes-statistics-report.pdf [https://perma.cc/L8YX-XLYB] (providing

involves diabetes education, lifestyle changes to diet and exercise, and insulin medication (for example, metformin[113]). Lastly, the physician recommends a follow-up with a diabetes specialist and discharges the patient.

The patient returns home and initially follows the physician's recommendations, adjusting her diet and increasing exercise, but soon relapses into her old habits, finding it too complicated and emotionally taxing to manage her chronic condition alone.[114] Years later, she suffers from a severe diabetic coma, loses consciousness, and is rushed to the ED again. This time, she is not so lucky and suffers severe long-term health complications.[115]

The above scenario features many aspects of care coordination within a single hospital organization. At the ED, the patient's care team may include the ED physician, nurse, triage provider, and registration staff. Once the patient is transferred to another department, her care team may include general interdisciplinary providers, clinical informatics, radiology, laboratory, and specialty providers. Within a hospital system (a single covered entity) all providers likely have full access to each patient's EHR and can easily view previous treatments, outstanding or completed lab results, and general information about the patient.[116]

estimated percentages as of 2018). Additionally, 88 million people had prediabetes, characterized by consistent elevated blood sugar levels not yet at the threshold to diagnose type 2 diabetes. *Id.* at 8.

113. Metformin is a first-line medication prescribed for patients diagnosed with type 2 diabetes, particularly for patients who are overweight. *See Metformin*, MEDLINE PLUS, https://medlineplus.gov/druginfo/meds/a696005.html [https://perma.cc/7SB9-L9UR] (last updated Mar. 15, 2020). Metformin acts by decreasing blood sugar levels. *Id.*

114. In fact, only sixteen percent of diabetic patients report fully adhering to the recommended lifestyle changes. Joseph C. Kvedar et al., *Digital Medicine's March on Chronic Disease*, 34 NATURE BIOTECHNOLOGY 239, 240–41 (2016).

115. Long-term complications of diabetes include cardiovascular disease, vision loss and eventual blindness, chronic kidney disease (which requires dialysis or kidney transplantation), neuropathy leading to foot ulcers or even amputation, or in severe cases, death. *Diabetes: Symptoms*, *supra* note 112.

116. However, in some hospitals, not all providers operate as a single covered entity. For example, independent physician groups may operate within a hospital through a "timeshare," with hospitals renting out space, equipment, and services on a nonexclusive, "as needed" basis. *See* Kim Stanger, *Physician Timeshare Agreements: New Stark Option for Sharing Space with Visiting Specialists and Others*, HOLLAND & HART (Dec. 17, 2015), https://www.hollandhart.com/physician-timeshare-arrangements-new-stark-option [https://perma.cc/ELU9-34KG]; *see also* 42 C.F.R. § 411.357(y) (2019) (listing requirements for the "timeshare" exception to the anti-kickback and physician self-referral laws). Many specialty functions, such as radiology and lab work, are often contracted out to different organizations that rent space from the hospital. *See* Stanger, *supra*. In an era of increased hospital consolidation, health organizations are dealing with a number of separate legal entities operating within one hospital, likely needing to work through interoperability concerns (due to having different EHR systems) and any potential business associate agreement in order to facilitate easy transmission of PHI. For more information about Stark laws (anti-kickback and physician self-referral laws), see generally Office of Inspector General, *A Roadmap for New Physicians, Fraud & Abuse Laws*, U.S. DEP'T HEALTH & HUM. SERVS., https://oig.hhs.gov/compliance/physician-education/01laws.asp [https://perma.cc/MB8U-8VS6]; *Anti-kickback Statute and Physician Self-Referral Laws (Start Laws)*, AM. SOC'Y ANESTHESIOLOGISTS, https://www.asahq.org/quality-and-practice-management/managing-your-

Outside of the hospital system, primary care providers, specialists, case workers, or other third-party social service workers generally do not have the same type of access to a patient's EHR and therefore cannot make the most educated clinical decisions based on a full picture of the patient's health, social, and psychological situation. In our hypothetical, for example, full access to the patient's EHR for care coordination purposes could have helped her find diabetes support groups or diabetes-friendly meal services to help manage her chronic condition, even without her explicitly seeking those services out. Her providers could securely share her PHI with third-party entities who could then work with the patient to create a plan that she could adhere to. By freely sharing her PHI within a care coordination model, a comprehensive group of actors could support the patient in managing her disease. Chronic diseases, like diabetes, typically have several risk factors that increase a person's chances of either exacerbating the disease or developing significant disease-related health complications.[117] Many risk factors and extraneous conditions might not be detected in a single outpatient clinic visit and require long-term monitoring and frequent check-ins, something that can be properly organized through a fully open care coordination model.

For the medically indigent[118] and those suffering from chronic conditions, coordinated care involves a variety of sources including healthcare providers, social service agencies, and community-based support programs. One approach is through hospitals that support multi-disciplinary teams that coordinate a full spectrum of care—exemplified in many community hospital systems. Community hospitals are governed locally, have the ability to partner with larger systems while maintaining community roots, play a large economic role in the area they serve, and are generally the only acute care provider in the

practice/timely-topics-in-payment-and-practice-management/anti-kickback-statute-and-physician-self-referral-laws-stark-laws [https://perma.cc/U4AQ-BUUG].

117. For example, risk factors for diabetes-related complications include smoking, being overweight and obesity, physical inactivity, high A1C (blood sugar), high blood pressure, and high cholesterol. CTRS. FOR DISEASE CONTROL & PREVENTION, *supra* note 112, at 9.

118. Medically indigent adults are defined as persons who do not have health insurance and are at the same time not eligible for other healthcare coverage such as Medicare, Medicaid, or private insurance. Beth E. Quill, *Medically Indigent*, *in* ENCYCLOPEDIA OF IMMIGRANT HEALTH (S. Loue & M. Sajatovic eds., 2012) https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5659-0_496 [https://perma.cc/T833-D6MX]; *see also* Robert H. Christmas, *Medically Indigent Adults*, 2 HEALTH MARKETING Q., no. 4, 1985, at 7, 8 (describing the lack of access to care for medically indigent individuals in a two-tiered system). Various agencies including governmental entities and public hospitals have put forth different definitions of medical indigency. For a review of various definitions, see generally Lynn Naliboff & Dorothy T. Lang, *Expanding Access to Health Care: Written Eligibility Standards for the Medically Indigent*, 13 CLEARINGHOUSE REV. 848, 848–50 (1980) (summarizing legal definitions, governmental approaches, and eligibility standards for public hospitals of medical indigency).

area.[119] As such, community hospitals are perfectly placed to act as facilitators of care coordination for healthcare services and other community-based services such as social welfare and charities. Community hospitals routinely provide care to the sickest populations by virtue of being the only accessible provider of healthcare services.[120] Thus, it is imperative for them to develop adequate and comprehensive care coordination models to address the needs of their patient population.

One such example is Hennepin County Medical Center ("HCMC")—a safety-net community hospital featuring a comprehensive academic medical center and public teaching hospital, with multiple hospital systems in Minneapolis, Minnesota and surrounding areas. HCMC is a nationally-recognized Level 1 Adult Trauma Center[121] and Level 1 Pediatric Trauma Center and boasts the largest emergency department in the state.[122] HCMC believes that many clinical interventions are ineffective unless pursued in coordination with other county departments or external social agencies.[123] Thus, HCMC works with many community-based services including organizations that help low-income individuals with housing placements, finding consistent sources of food, and identifying paths to heal families who entered into child protection systems.[124] HCMC is just one hospital system of many that utilize care coordination in a holistic approach for treating individuals by involving external services such as social welfare and charities.

Another such example is Community Care of North Carolina ("CCNC"), which is a public-private partnership sponsored by the North Carolina Department of Health and Human Services and the Division of Health Benefits.[125] CCNC is comprised of fourteen regional networks of physicians, nurses, pharmacists, hospitals, health departments, social service agencies, and

119. *The Modern Definition of a Community Hospital*, BECKER'S HOSP. REV., https://www.beckershospitalreview.com/hospital-management-administration/the-modern-definition-of-a-community-hospital.html [https://perma.cc/QH8W-LR57].

120. *Id.*

121. Level I Trauma Centers provide the highest level of surgical care for trauma patients. These criteria are established by the American College of Surgeons. *See Verification, Review, and Consultation (VRC) Program*, AM. C. SURGEONS, https://www.facs.org/quality-programs/trauma/tqp/center-programs/vrc [https://perma.cc/DTJ6-Z5NG].

122. *HCMC Receives National Award for Population Health*, HENNEPIN CTY. MED. CTR. NEWS (June 21, 2013), https://hcmcnews.org/2013/06/21/hcmc-receives-national-award-for-population-health/ [https://perma.cc/3DSA-7ZEH].

123. *See generally About Hennepin Health Care*, HENNEPIN HEALTHCARE, https://www.hennepinhealthcare.org/about-us/ [https://perma.cc/H3PK-RS2E] ("We partner with our community, our patients and their families to ensure access to outstanding care while improving health and wellness through teaching, patient and community education, and research.").

124. *See id.*

125. *Community Care of North Carolina/Carolina ACCESS (CCNC/CA)*, N.C. DEP'T HEALTH & HUM. SERVS., https://medicaid.ncdhhs.gov/providers/programs-and-services/community-care-north-carolinacarolina-access-ccncca [https://perma.cc/R6FD-M7H2].

other community organizations.[126] These medical professionals utilize care coordination to provide healthcare to individuals with complex health needs through the patient-centered medical home model.[127] In that model, the primary care physician takes lead of the patient's care plan, coordinating across various settings and involving all actors who provide care to the patient.[128]

Furthermore, there is a hodgepodge of third-party services providing nonmedical care that can be involved in care coordination. Such services can include free transport service to hospital facilities,[129] temporary housing facilities intended for families that travel out-of-town to receive medical care,[130] food services for those too sick to shop and cook for themselves,[131] and legal services,[132] to name a few. Unless these services are already partnered with hospital organizations as business associates,[133] there will be delay in communication between the hospital with the third-party services. These communication times can be even further delayed by variations in the nature and volume of information requested, whether or not the data is held by a standardized EHR, the third party's capabilities for receiving such data, and any state law regulations that further restrict data sharing.[134] These delays could

126. NCIOM, UNDERSTANDING COMMUNITY CARE OF NORTH CAROLINA 1, http://nciom.org/wp-content/uploads/2018/04/CCNC-Primer-FINAL-4-26-18.pdf [https://perma.cc/BF78-QXQV].

127. *Id.*

128. *Defining the PCMH*, AGENCY FOR HEALTHCARE RES. & QUALITY, https://pcmh.ahrq.gov/page/defining-pcmh [https://perma.cc/4CWY-XQNG].

129. *See, e.g.*, Chris Webber, *Introducing Uber Health*, *Removing Transportation as a Barrier to Care*, UBER (Mar. 1, 2018), https://www.uber.com/newsroom/uber-health/ [https://perma.cc/HVD6-XLP8] (promising "reliable, comfortable transportation for patients"); WINGS OF HOPE, https://wingsofhope.ngo/ [https://perma.cc/U5JA-SVYK] ("[T]he Medical Relief & Air Transport (MAT) program serves patients throughout the Midwest.").

130. *See, e.g.*, RONALD MCDONALD HOUSE CHARITIES, https://www.rmhc.org/ [https://perma.cc/KB52-QM3H] ("A place for families to rest and regroup right in the hospital"); *Target House*, ST. JUDE CHILDREN'S RES. HOSP., https://www.stjude.org/treatment/patient-resources/while-here/housing/target-house.html [https://perma.cc/7RUG-TSJ9] (providing "an apartment-style housing facility just three miles from the hospital"); *Tri Delta Place*, ST. JUDE CHILDREN'S RES. HOSP., https://www.stjude.org/treatment/patient-resources/while-here/housing/tri-delta-place.html [https://perma.cc/39U3-CEPV] (providing "comfortable, fun and patient safe housing . . . on the St. Jude campus").

131. *See, e.g.*, PROJECT ANGEL FOOD, https://www.angelfood.org/ [https://perma.cc/DFA5-S52T] ("Project Angel Food prepares and delivers healthy meals to feed people impacted by serious illness."); MEALS ON WHEELS AM., https://www.mealsonwheelsamerica.org/ [https://perma.cc/X3KQ-KETY] (helping seniors "age with dignity and without fear of hunger").

132. *See, e.g.*, LEGAL AID N.C., http://www.legalaidnc.org/get-help/self-help-library/health-insurance [https://perma.cc/L5Z6-633E] (offering to help health insurance applicants "understand . . . options," access financial help, and complete enrollment).

133. *See supra* Section I.A.2. Business associates also need corresponding business associate agreements that capture the scope of the information the business associate can share.

134. 45 C.F.R. § 160.203(b) (2019) (allowing state law to have a more stringent requirement than already provided by HIPAA).

jeopardize timely medical care or even deter a potential patient from seeking care altogether.

C. *Care Coordination Under HIPAA*

Although permitted disclosures under HIPAA appear to grant a broad scope for covered entities to share PHI for care coordination purposes, in actuality, this scope is limited by the statutory definitions of permitted disclosures within the "minimum necessary" principle.[135]

Care coordination appears to fall under either the "treatment" or "healthcare operations" prongs of TPO permitted uses and disclosures. As noted earlier, "treatment" means the "provision, coordination, or management of healthcare and related services" by healthcare providers, and can include the coordination or management of healthcare in collaboration with a third party.[136] "Healthcare operations" means the activities of a covered entity related to their HIPAA-covered healthcare functions including "population-based activities relating to . . . case management and care coordination."[137] Population-based activities, or research and medical care activities based on population health, involve looking at activities in order to improve the aggregate health outcome of a particular population of individuals.[138] This could take the form of studying all patients in a given geographic location who suffer from the same chronic disease in order to improve the overall health for these patients. HIPAA

135. *Id.* §§ 164.502(b), 164.514(d).

136. *Id.* § 164.501 (defining treatment); *supra* text accompanying note 82. Other activities that fall under the "treatment" definition are consultation between healthcare providers regarding a patient and patient referral between healthcare providers. *Id.*

137. § 164.501 (defining healthcare operations). Other activities that fall under the "healthcare operations" definition are conducting quality assessment and improvement activities; reviewing competence or qualifications of given healthcare professionals; reviewing health insurance benefit costs; conducting medical review, legal services, and auditing functions; business planning and development; business management; and general administrative activities. *Id.*

138. *See* David Kindig & Greg Stoddart, *What Is Population Health?*, 93 AM. J. PUB. HEALTH 380, 380 (2003); *see also What Is Population Health?*, MILKEN INST. SCH. PUB. HEALTH (Apr. 15, 2015) https://mha.gwu.edu/what-is-population-health/ [https://perma.cc/HA4F-NQBM] (interviewing healthcare leaders to define the term "population health").

permits these activities if a covered entity (healthcare provider or health plan) sends the relevant PHI directly[139] to the requesting covered entity.[140]

While HIPAA generally supports care coordination for either pathway—treatment or healthcare operations—certain restrictions apply concerning the purpose for which covered entities can use patient information. Specifically, a covered entity "may use or disclose [PHI]" for a variety of reasons, two of which are most applicable to care coordination.[141] First and most simply, a covered entity may disclose PHI for the purpose of medical treatment activities performed by a healthcare provider.[142] Second, a covered entity may disclose PHI for the purposes of healthcare operations activities for another covered entity.[143] This second reason is applicable only if three certain conditions are met: (1) both covered entities currently have, or have had, a relationship with the individual whose PHI is being requested; (2) the PHI pertains to that particular relationship; and (3) the disclosure falls under the HIPAA definition of healthcare operations.[144]

Along with the statutory definitional restrictions, covered entities must follow the minimum necessary principle, which requires that a covered entity make reasonable efforts to only use, disclose, and request the minimum amount of PHI needed to accomplish the intended purpose.[145] As mentioned

139. Sharing PHI between covered entities (also known as health information exchange) through their EHR systems requires that both systems comply with HIPAA's Privacy and Security Rules and be interoperable, meaning that the technology enables the secure exchange of PHI without special effort on the part of the user. 42 U.S.C. § 300jj(9) (2018); *see also Interoperability*, HEALTHIT (May 9, 2019), https://www.healthit.gov/topic/interoperability [https://perma.cc/SRZ2-2D2C]. In practice, interoperability is challenging since there are a multitude of EHR software companies with different clinical terminologies, technical specifications, and functional capabilities, all existing without one standard interoperability format. *See* Miriam Reisman, *EHRs: The Challenge of Making Electronic Data Usable and Interoperable*, 42 PHARMACY & THERAPEUTICS 572, 572–73 (2017). Furthermore, EHR interoperability has a significant cultural obstacle, requiring the collaboration between patients, providers, software vendors, legislators, and health information technology professionals. *Id.* at 573. Even within a single hospital system, one EHR system may be used for inpatient services, another system for outpatient services, and other systems for ancillary services such as lab work, oncology services, pharmacy, and patient portals. Interoperability has been steadily improving, especially for acute care hospitals, but is still far from the level necessary to seamlessly use, share, and integrate PHI into EHR systems. *See* Don Rucker & Talisha Searcy, *Acute Care Hospitals Are More Interoperable Than Ever but Challenges Remain*, HEALTHIT (Oct. 25, 2018), https://www.healthit.gov/buzz-blog/interoperability/acute-care-hospitals-are-more-interoperable-than-ever-but-challenges-remain [https://perma.cc/H5ET-FL29].

140. *See* 45 C.F.R. §§ 164.506(c)(1), (4)(i) (2019).

141. *Id.* § 164.506(c). A covered entity may also use or disclose PHI for its own TPO purposes; for disclosure of PHI to another covered entity or healthcare provider for payment activities of entity receiving information; and, if the covered entity participates in an organized healthcare arrangement, for purpose of healthcare operations enumerated in the arrangement. *Id.* § 164.506(c)(1), (3), (5).

142. *Id.* § 164.506(c)(2).

143. *Id.* § 164.506(c)(4); *see also The HIPAA Privacy Rule*, *supra* note 23.

144. § 164.506(c)(4); *see also The HIPAA Privacy Rule*, *supra* note 23.

145. 45 C.F.R. §§ 164.502(b), 164.514(d) (2019).

previously,[146] the minimum necessary principle is a standard that is vaguely worded and requires HIPAA-regulated entities to interpret the appropriate scope of PHI they can share in each scenario. The minimum necessary principle does have explicit carveouts where the principle does not apply, including one for transactions between covered healthcare providers for treatment purposes, including care coordination.[147] However, this exception does not apply when a covered entity shares PHI with parties who are not healthcare providers, such as community support groups or social workers.[148] Likewise, disclosures related to care coordination but for nontreatment activities, such as population-based activities, [149] claims management, [150] review of healthcare services for appropriateness of care,[151] utilization reviews,[152] and formulary development,[153] are still subject to the minimum necessary principle.[154]

The minimum necessary principle, although flexible given a covered entity's actions, also makes those same covered entities reluctant to share more than what is explicitly permitted. Additionally, due to the vagueness and complexity of TPO exceptions, many covered entities are unwilling to share PHI for the purposes of care coordination in fear of violating HIPAA.[155] Since care coordination presumes ready exchange of patient information among healthcare providers, payers, and third parties involved, HIPAA privacy provisions can serve to hinder such coordination. Though HIPAA may allow for such sharing, many covered entities, at least anecdotally, are concerned with violating HIPAA, resulting in instances where covered entities fail to comply with requests to share PHI.[156]

In fact, in a late 2018 Request for Information ("RFI"), OCR admitted that a number of covered entities have expressed reluctance to share information related to care coordination or management of treatment, especially in situations where multi-disciplinary teams are involved. [157] The purpose of

146. *See supra* text accompanying notes 73–81.

147. § 164.502(b)(2)(i).

148. *See id.*

149. *Id.* § 164.501 (defining healthcare operations).

150. *Id.* (defining payment).

151. *Id.*

152. *Id.*

153. *Id.* (defining healthcare operations).

154. *See id.* § 164.502(b)(2).

155. *OCR May Alter HIPAA Rules To Ease Compliance*, *Care Coordination*, RELIAS MEDIA (Mar. 1, 2019), https://www.reliasmedia.com/articles/144044-ocr-may-alter-hipaa-rules-to-ease-compliance-care-coordination [https://perma.cc/7Y3L-WCC5].

156. *Id.*

157. *See* Request for Information on Modifying HIPAA Rules to Improve Coordinated Care, 83 Fed. Reg. 64,302 (proposed Dec. 14, 2018) (to be codified as 45 C.F.R. pts. 160, 164) [hereinafter RFI Coordinated Care]. OCR solicited comments for how to improve HIPAA to promote information sharing for treatment and care coordination, promote parental and caregiver involvement in addressing the opioid crisis and serious mental illness, and account for disclosures by covered entities. *Id.*

OCR's RFI was to solicit public comments to help identify provisions of HIPAA that impede the "transformation to value-based healthcare" or ones that "limit or discourage coordinated care . . . without meaningfully contributing" to privacy and security of an individual's PHI.[158] One area identified as needing comment was the promotion of information sharing in the care coordination context.[159] OCR's comment period for its RFI closed on February 12, 2019 and unfortunately has not yet resulted in the necessary regulation change. Instead, OCR issued a series of guidances, including one directed at care coordination for health plans.[160]

II. ADMINISTRATIVE AGENCY GUIDANCES

Under the Congressional delegation of rulemaking authority under HIPAA, HHS is responsible for promulgating regulations consistent with HIPAA's purpose and guidelines.[161] As an administrative agency, HHS must follow the APA[162] in order to add or modify regulations. While much of the regulatory framework has gone through the APA's formal procedure, OCR, the enforcement division of HHS, also issues periodic guidance that is intended to provide the public with the agency's interpretation of a particular regulation.[163] OCR's guidances are aimed toward clarifying the scope of certain HIPAA rules and delineating what is explicitly permitted. However, many of the guidance released by OCR are notoriously bare in detailing what is permissible.[164]

Additionally, the process for issuing guidance is much less formal than the process for enacting or amending a regulation, and guidance is not legally binding in the same way a regulation is. However, many regulated entities, including those regulated under HIPAA and HHS, treat administrative agency guidance as binding and are rarely willing to stray from them. Regulated entities believe that if the agency releases guidance on a particular topic and does not mention a specific allowance, the agency might not believe the allowance is legal.

158. *Id.*

159. *Id.* In fact, care coordination is the first issue listed in the RFI.

160. *See infra* Part III.

161. *See supra* note 21 and accompanying text.

162. The Administrative Procedure Act, Pub. L. 79-404, 60 Stat. 237 (1946) (codified as 5 U.S.C. §§ 500–596 (2018)).

163. For a list of OCR guidance, see Office for Civil Rights, *HIPAA Guidance Materials*, U.S. DEP'T HEALTH & HUM. SERVS. (Dec. 19, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html [https://perma.cc/5ZG5-K7V5].

164. *See id.* For example, many OCR guidances are merely FAQs that clarify specific questions but do not contemplate similar scenarios outside of the scope of the questions. *Id.*

A. *The APA Rulemaking Process*

In simple terms, agencies are delegated authority to issue regulations from laws enacted by Congress.[165] Agencies are not permitted to take action that goes beyond their statutory authority or violates the Constitution and must follow the APA through an open public process when issuing regulations.[166] The APA requires agencies to follow certain administrative procedures when creating regulations, including publishing notice of both the proposed and final rulemaking in the Federal Register and providing the public an opportunity to comment on the proposed rulemaking, colloquially known as notice-and-comment rulemaking.[167]

In order to publish a regulatory rule,[168] agencies must go through a very long and public process.[169] Many times, an agency will survey its area of legal expertise and decide which issues or goals have priority for rulemaking.[170] Once an agency feels comfortable with an initial rule, it will publish it as a proposed rule which starts the notice-and-comment process.[171] The proposed rule will include a summary of the issues under consideration and invite interested parties to comment on the proposed rule by a certain date.[172] The default

165. *See* U.S. CONST. art. I, § 8, cl. 18; Gundy v. United States, 588 U.S. ___, 139 S. Ct. 2116, 2123 (stating that under the Necessary and Proper Clause, Congress may confer discretion to executive agencies "to implement and enforce the laws"), *reh'g denied* 140 S. Ct. 579 (2019); *see also* Yakas v. United States, 321 U.S. 414, 425 (1944) (finding the Constitution does not "deny[] to the Congress the necessary resources . . . to perform its function[s]").

166. 5 U.S.C. § 552(a) (2018). Additionally, agencies are required to follow additional procedures outside of the rulemaking process, including submitting public regulatory plans once a year on a unified agenda of regulatory and deregulatory actions regarding future rulemaking activities to update the public on pending and completed regulatory actions. *See* Exec. Order No. 13,771 § 3(c), 82 Fed. Reg. 9339, 9340 (Jan. 30, 2017).

167. *See* 5 U.S.C. § 553(b)–(d) (2018).

168. Rules are agency statements of "general or particular applicability" to all entities regulated by the agency and are designed to implement, interpret, or prescribe law or policy. *Id.* § 551(4).

169. I will only be addressing the informal rulemaking procedure under APA § 553 rather than rulemaking that requires a formal hearing under APA §§ 556, 557. *See id*. § 553(c) ("When rules are required by statute to be made on the record after opportunity for an agency hearing, [APA §§ 556, 557] apply . . . ."). HIPAA does not require a formal hearing procedure in its statute. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 707, 110 Stat. 1936, 1951 (codified as amended in 29 U.S.C. § 1911c (2018)) ("The Secretary . . . may promulgate such regulations as may be necessary or appropriate to carry out the provisions of this part."). Also, HIPAA does not have the unmistakable indicia of formality required to trigger a formal hearing. *See* U.S. v. Fla. E. Coast Ry., 410 U.S. 224, 238 (1973) (finding that statutes delegating administrative agency authority need to explicitly state a need for a formality to require a formal hearing).

170. An agency's motivations for rulemaking include Congress passing new legislation that directs an agency; external factors, such as technology, scientific data, or accident in the field; required reviews, lawsuits, petitions, and prompt letters from the Office of Information and Regulatory Affairs ("OIRA"); and recommendations from other agencies, committees, or groups.

171. § 553(b), (c) (detailing the requirements for public notice and opportunity to participate, colloquially known as notice-and-comment).

172. *Id.* Interested parties can provide comments through written data, views or positions, arguments, and oral presentation in certain circumstances. *Id.* § 553(c).

comment period is thirty to sixty days, though this can be longer if the agency determines an extension is necessary.[173]

Based on these public comments, the agency must determine whether its proposed solution will help accomplish its goals or solve identified problems.[174] It also must consider alternative solutions that may be more effective or cost less. Before the final rule is issued, the President of the United States, as head of the executive branch, has an opportunity to review the rule.[175]

Once the final rule is approved, the agency must publish it in the Federal Register. [176] Final rules are then sent to Congress and the Government Accountability Office ("GAO"), an independent agency that provides auditing, evaluation, and investigative services for Congress, before they can take effect.[177]

Administrative rulemaking through the APA process is legally binding on the regulated entities that the agency governs. Because agencies are typically led by experts in the field that they are regulating, and because agencies must provide the public an opportunity to provide feedback during the rulemaking process, administrative rulemaking may be viewed as one of the most democratic ways to regulate certain industries.[178] Congressional rulemaking, on the other hand, relies on representative legislators to vote on behalf of their constituents. Members of the public generally do not have opportunity to comment on the record during congressional rulemaking proceedings. [179] However, the APA requirements are a "costly, time-consuming set of procedures."[180] These procedures include notice and comment in the Federal Register as well as executive oversight, which often result in a lengthy rulemaking process. [181] This lack of speed and flexibility can stymie timely

173. *Id.* § 553(d)(3).

174. Exec. Order No. 13,563 § 1(b), 76 Fed. Reg. 3821, 3821 (Jan. 21, 2011).

175. *Id.* (reaffirming Exec. Order 12,866, 3 C.F.R. 638 (1994)).

176. 5 U.S.C. § 552(a)(1)(D) (2018).

177. *See* Contract with America Advancement Act of 1996, Pub. L. No. 104-121, § 251, 110 Stat. 847, 868 (codified at 5 U.S.C. § 801 (2018)) (providing that agencies must submit rules to Congress for review).

178. Although the APA requires agencies to provide the public an opportunity to comment on the issue that will go on the official record (i.e. notice and comment), the APA does not actually require that agencies follow any public comment in crafting its rule. *See* 5 U.S.C. § 553(c) (2018).

179. Congressional hearings and committee meetings are typically announced publicly with the date, time, and subject matter to be discussed with the intention of being open to the public to attend. *See generally* Standing Rules of the Senate, S. Doc. No. 110-9 (2013), Rule XXVI at 31 (describing Congressional committee procedure for investigations and hearings). However, the Congressional rules do not provide the public an opportunity to comment on the proceeding on the record, unless individuals were already invited or subpoenaed to speak as a witness. *See id.*

180. Nicholas R. Parillo, *Federal Agency Guidance and Power To Bind: An Empirical Study of Agencies and Industries*, 36 YALE J. REG. 165, 168 (2019) [hereinafter Parillo, *Power To Bind*].

181. Though no comprehensive collection of guidance exists, some have estimated that for a given agency the page count for guidances can be greater than actual regulations by factors of anywhere

solutions to pressing issues. As such, many administrative agencies forgo the APA rulemaking process and instead turn to guidance to provide real-time interpretation on issues.

B. *Practical Legal Binding Effect of Administrative Agency Guidance*

Guidance is a general term used in administrative law to describe documents created by government agencies intended to explain, interpret, or advise interested parties about rules, laws, and procedures, clarifying and influencing how government agencies administer regulations and programs.[182] However, unlike regulations enacted through the APA that officially bind the agency, guidance does not technically carry the full weight of law.[183] Still, issuing guidance is a much easier process than APA rulemaking, and agencies often turn to guidance as a tool to answer questions about the meaning of a regulation and how to comply with it.[184]

Guidances are "ubiquitous and essential feature[s]" of government agencies and do not require the same stringent and time-consuming process as administrative regulations do under the APA.[185] The APA defines guidances as agency statements that qualify as "interpretive rules" or "general statements of policy," though neither phrase is defined within the APA.[186] As such, guidances are supposed to provide an agency's "current thinking about individual

between twenty and two hundred. Peter L. Strauss, *Publication Rules in the Rulemaking Spectrum: Assuring Proper Respect for an Essential Element*, 53 ADMIN. L. REV. 803, 805 (2001); Peter L. Strauss, *The Rulemaking Continuum*, 41 DUKE L.J. 1463, 1468–69 (1992) (comparing how much space guidance materials for particular agencies occupied on library shelves to the space occupied by the rules themselves).

182. *See* Syncor Int'l Corp. v. Shalala, 127 F.3d 90, 94 (D.C. Cir. 1997) ("An interpretive rule . . . typically reflects an agency's construction of a statute that has been entrusted to the agency to administer."); Pac. Gas & Elec. Co. v. Fed. Power Comm'n, 506 F.2d 33, 38 (D.C. Cir. 1974) ("[Guidance] only announces what the agency seeks to establish as policy."); U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S MANUAL ON THE ADMINISTRATIVE PROCEDURE ACT 30 n.3 (1947) (explaining the difference between substantive and interpretive rules).

183. However, while not legally binding, administrative agency guidance is entitled *Skidmore* deference. United States v. Mead Corp., 533 U.S. 218, 228 (2001). Under *Skidmore* deference, courts are not entirely deferential to agencies, instead giving deference based on the agency's care in crafting guidance, consistency with previous guidance, formality of such guidance, relative expertise, and persuasiveness of the agency's position. *See id.*; Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944) ("The weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control.").

184. *Guidance*, REG. GROUP, https://www.regulationwriters.com/regulatory_glossary/ [https://perma.cc/7UQ6-PVYX].

185. Parillo, *Power To Bind*, *supra* note 1780, at 180.

186. 5 U.S.C. § 553(b)(A) (2018). Instead, many cite to U.S. DEP'T OF JUSTICE, *supra* note 182, which defines interpretive rules as "rules or statements issued by an agency to advise the public of the agency's construction of the statutes and rules which it administers" and general statements of policy as "statements issued by an agency to advise the public prospectively of the manner in which the agency proposes to exercise a discretionary power." *Id.* at 30 n.3.

adjudicatory or enforcement proceedings" and leave room for case-by-case discretion.[187] In actuality, many regulated parties face "practical pressure to follow what a guidance document 'suggests,'" absent individual exemptions from the agency, which many agencies are "inflexible" in providing.[188] In fact, the GAO has determined that certain guidance documents can qualify as rules under the Congressional Review Act ("CRA")[189] and the APA.[190] The fear is that guidance documents provide strong incentives for regulated parties to comply as if they were binding regulatory rule.

For regulated parties, the incentive to follow guidance is influenced by four factors compiled by Nicholas R. Parillo ("Parillo factors"): (1) pre-approval requirements, (2) investment in relationships to agencies, (3) prevalence of compliance personnel, and (4) high costs for one-off enforcement.[191] The first factor, pre-approval requirements, contemplates the effect of a regulated party having to obtain affirmative assent from a government agency in the form of permits, licenses, or accreditation.[192] For example, the Food and Drug

187. Parillo, *Power To Bind*, *supra* note 180, at 168–69.

188. *Id.* at 174.

189. The CRA empowers Congress and the GAO to review and potentially overrule new federal regulations by government agencies. Contract with America Advancement Act of 1996, Pub. L. No. 104-121, § 251, 110 Stat. 847, 868 (codified at 5 U.S.C. §§ 801–808 (2018)).

190. In 2017, the GAO determined that two guidance documents regarding lending practices were legislative rules. *See* Letter from Susan A. Poling, Gen. Counsel, U.S. Gov't Accountability Office, to Senator Pat Toomey (Oct. 19, 2017), https://www.gao.gov/assets/690/687879.pdf [https://perma.cc/227B-MV23] (determining that the CRA applied to interagency guidance on leveraged lending); Letter from Thomas H. Armstrong, Gen. Counsel, U.S. Gov't Accountability Office, to Senator Pat Toomey (Dec. 5, 2017), https://www.gao.gov/assets/690/688763.pdf [https://perma.cc/2WW8-8WJM] (determining that the CRA applied to a bulletin on indirect auto lending and compliance with the Equal Credit Opportunity Act).

191. Parillo, *Power To Bind*, *supra* note 180, at 177. The methodology in developing these factors relies upon a series of interviews regarding guidance with a number of individuals involved within eight distinct regulatory areas, including agency officials, industry attorneys, corporate executives, and representatives for nongovernmental organizations. *Id.* at 173–74. Parillo's empirical study included interviews with representatives from the following administrative agencies: the FDA, Environmental Protection Agency, Occupational Safety and Health Administration, Department of Energy, U.S. Department of Agriculture, Federal Aviation Administration, banking regulatory agencies, and HHS. *Id.* Parillo's analysis of HHS guidance is limited to Medicare reimbursement under the Center for Medicare and Medicaid Services program. *Id.* at 190. Since this Comment focuses on HHS and its role in promulgating HIPAA regulations, Parillo's analysis regarding HHS Medicare guidance is not quite on point; thus, I chose not to discuss it in this Comment. Parillo's use of highly diverse individuals from a myriad of regulatory agencies in the development of the Parillo factors hones its effectiveness in trans-substantive application. Trans-substantivity refers to the doctrine that certain rules or application do not vary between substantive contexts and thus can be applied effectively in any of those contexts. *See* David Marcus, *Trans-Substantivity and the Processes of American Law*, 2013 BYU L. REV. 1191, 1191 (2013). While the empirical study is not wholly comprehensive, it includes a subset of agency examples that are representative of much of the administrative agency state at large, encompassing agencies that regulate healthcare, the environment, workplace, science and technology, and banking and finance.

192. *See* Robert A. Anthony, *Interpretive Rules*, *Policy Statements*, *Guidances*, *Manuals*, *and the Like—Should Federal Agencies Use Them To Bind the Public?*, 41 DUKE L.J. 1311, 1340 (1992) (explaining that

Administration ("FDA") mandates that drugs and medical devices be approved as safe and effective before a company can market them. Companies will generally follow this guidance without exception since the FDA's approval decisions are discretionary and "represent[] the FDA's latest thinking on the matter."[193] Noncompliance with the FDA's pre-approval guidance would be a "folly" and potentially waste significant investment in protocol and marketing.[194]

The second factor provides incentive to comply if there is a need to maintain a good relationship with the agency. This can occur in situations where an agency continuously monitors a regulated party and that party needs to interact with the agency under a complex regulatory scheme. These conditions behoove a regulated party to win the trust of the agency to receive favorable treatment in case of future noncompliant conduct.[195] With the FDA, many companies seek to establish good relations since they must repeatedly seek approvals under the FDA's complex reporting requirements.[196] Having a good relationship can smooth over noncompliance, especially when a company is subject to a series of pre-approval requirements. Following guidance can allow the regulated party to show that it is "not seeking to push the edge of the law" but is deferential to the agency's suggested conduct.[197]

The third factor refers to the rise of compliance personnel within regulated entities and their effect on improving compliance with agency guidance. These "compliance officers" have backgrounds, socialization, and career incentives that provide them with strong incentives to maintain good relations with agencies by following guidance.[198] In the FDA context, many compliance officers are the interface between companies and the agency and seek to understand the agency's expectations, disseminate the information within the companies, and ensure their compliance.[199] Thus, the existence of compliance officers creates a culture of compliance within regulated companies.

pre-approval requirements have significant influence on applicants because failure to comply can result in significant penalties).

193. Parillo, *Power To Bind*, *supra* note 180, at 186.

194. *Id.* (quoting Interview with Source 24, Official, Fed. Trade Ass'n). Parillo's research methodology involved interviewing individuals within different regulated agencies to discern common attitudes towards agency guidance.

195. Stronger relationships can lead to agencies interpreting noncompliant conduct as less deserving of penalties, e.g. accidental actions as opposed to deliberate ones. *See generally* Winston Harrington, *Enforcement Leverage When Penalties Are Restricted*, 37 J. PUB. ECON. 29 (1988) (detailing a dynamic repeated-game model that explains the actions and inactions of regulated entities and enforcement agencies).

196. Parillo, *Power To Bind*, *supra* note 180, at 192.

197. *Id.*

198. *Id.* at 200–01.

199. DANIEL CARPENTER, REPUTATION AND POWER: ORGANIZATIONAL IMAGE AND PHARMACEUTICAL REGULATION AT THE FDA 644–46 (2010).

Finally, a regulated entity has incentives to follow agency guidance in order to reduce the risk of sanctions in a one-off enforcement proceeding against the particular entity. Because guidance outlines what an agency considers to be lawful or announces what conduct an agency will or will not allow, a regulated party could significantly reduce enforcement risk by following such guidance to the letter. However, in reality, regulated entities base their compliance strategy on a risk calculation that looks at the probability of the agency detecting noncompliance, finding a violation, and imposing sanctions.[200] If the potential cost for noncompliance is low, an entity might not push as hard to follow agency guidance to the letter and may choose not to request clarification from the agency on particular issues.

C. *Binding Effect of OCR Guidance Generally*

Many covered entities treat OCR guidance on HIPAA compliance as binding for three reasons: (1) knowledge of HIPAA's public, complaint-driven enforcement system; (2) fear of violating HIPAA due to costly penalties; and (3) a desire to promote public confidence in protection of patient PHI. As such, many hospital systems employ several compliance personnel and pay for consulting services[201] to ensure HIPAA compliance. Additionally, OCR's guidances are binding in practical effect for institutional reasons, as supported by the Parillo factors that demonstrate why regulated entities are incentivized to follow guidance.[202]

First, covered entities treat OCR guidance as binding due to the complaint-driven enforcement system and the public nature of OCR investigations and findings of noncompliance.[203] OCR enforces HIPAA rules by investigating complaints filed directly with OCR; conducting reviews to

200. Parillo, *Power To Bind*, *supra* note 180 at 208 (explaining factors involved when FDA-regulated companies calculate compliance risks).

201. A quick Google search reveals a bevy of HIPAA compliance consulting firms. *See*, *e.g.*, *HIPAA Compliance Checklist*, HIPAA J., https://www.hipaajournal.com/hipaa-compliance-checklist/ [https://perma.cc/2XXR-7KYK]; *How to Become HIPAA Compliant*, COMPLIANCY GROUP, https://compliancy-group.com/how-to-become-hipaa-compliant/ [https://perma.cc/2878-K558]; *Health Care Compliance and Regulatory Services*, STRATEGIC MGMT., https://compliance.com/services/ [https://perma.cc/AV2N-653C]; *HIPAA and HITECH Health Care Compliance Consulting*, RSM, https://rsmus.com/what-we-do/industries/health-care/hipaa-hitech-compliance-consulting.html# [https://perma.cc/K4G5-SG54]. Additionally, many companies develop electronic health record ("EHR") software to comply with HIPAA technical requirements. *See, e.g.*, *Allscripts Security Program*, ALLSCRIPTS, https://www.allscripts.com/legal/security-program/ [https://perma.cc/JD2S-VQQG]; *Cerner Security Program*, CERNER, https://www.cerner.com/security [https://perma.cc/65YS-7RG2]; *Government Regulations*, EPIC, https://www.epic.com/software#GovernmentRegulations [https://perma.cc/26JJ-VW5A].

202. *See supra* Section II.B (detailing how the Parillo factors influence an agency's likelihood to follow guidance).

203. For a list of cases currently under investigation by OCR, see Office for Civil Rights, *supra* note 47.

determine if covered entities are in compliance; and engaging in education and outreach to foster compliance with HIPAA requirements.[204] Complaints are often initiated by third parties through OCR's online, public portal.[205] If the complaint describes an action over which OCR has jurisdiction,[206] OCR will contact the involved parties, determine if an investigation is necessary, and possibly even refer the complaint to the DOJ when there is a violation of a criminal provision of HIPAA.[207] OCR also performs compliance reviews on its own initiative to investigate problems that may be particularly acute, national in scope, or newly emerging.[208]

If OCR determines that an investigation is necessary and later finds that the covered entity was not in compliance, OCR will resolve the case by obtaining voluntary compliance, corrective action, and/or a resolution agreement.[209] Additionally, OCR can provide technical assistance prior to or after an investigation to ensure compliance.[210]

For resolution agreements, covered entities enter into a settlement agreement with HHS where the covered entity or business associate agrees to meet certain obligations and make reports to HHS.[211] During this time, HHS monitors compliance with the obligations set out in the agreement.[212] If the covered entity does not take corrective action or otherwise resolve the violation

204. *See* 45 C.F.R. §§ 160.306–312, 164 (2019); *see also* Office for Civil Rights, *Enforcement Process*, U.S. DEP'T HEALTH & HUM. SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [https://perma.cc/J5C3-9VP6] (outlining the enforcement process).

205. Office for Civil Rights, *Complaint Portal*, U.S. DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf;jsessionid=BFFCDC8DFF0CABBAF5417CCD6411CE25 [https://perma.cc/D9PW-T4F7].

206. The alleged action must have taken place after the HIPAA rules took effect and the complaint itself must have been filed against a covered entity or business associate within 180 days and allege an activity that would violate HIPAA rules. Office for Civil Rights, *What OCR Considers During Intake and Review*, U.S. DEP'T HEALTH & HUM. SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-ocr-considers-during-intake-and-review/index.html [https://perma.cc/3UNE-757G]; *see* § 160.306 (describing the complaint procedure).

207. 42 C.F.R. § 1320d-6 (2019).

208. *See, e.g.*, Office for Civil Rights, *Recent Civil Rights Resolution Agreements & Compliance Reviews*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 2, 2020), https://www.hhs.gov/civil-rights/for-providers/compliance-enforcement/agreements/index.html [https://perma.cc/4XAK-EEA7] (listing previous compliance review initiatives for HIV/AIDS and language access in critical access hospitals).

209. 45 C.F.R. § 160.312 (2019).

210. OCR only offers or requires technical assistance after a complaint has been through the initial intake and review process. For breach compliance review, OCR only offers technical assistance post-investigation. *See* Office for Civil Rights, *Enforcement Data*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 22, 2019), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html [https://perma.cc/SGS8-NV9F].

211. Generally, this period is three years. Office for Civil Rights, *Resolution Agreements*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 3, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html [https://perma.cc/CS5G-AT8C].

212. *Id.*

satisfactorily, OCR may impose CMPs.[213] CMPs are imposed in tiers based on the culpability associated with each violation and failure to correct said violation.[214] As such, CMPs can quickly add up.

The high cost of CMPs hits at the heart of the second reason why entities treat OCR guidance as binding: fear of violating HIPAA and the high costs associated with such a violation. Additionally, CMPs implicate the fourth Parillo factor—high costs of one-off enforcement. In 2018, OCR obtained settlements and CMPs in ten cases for a total of $28 million, corresponding to an average of $2.8 million and median of $500,000 per fine.[215] That being said, these ten cases where monetary penalties were obtained represent merely a fraction of total cases that OCR processed[216] and investigated,[217] corresponding to 0.0305% of total cases and 0.62% of cases investigated.[218] OCR's investigational framework is highly dependent on the submission of public complaints, although some reviews are initiated by OCR. As such, the risk that OCR both detects noncompliance and initiates an investigation could potentially be very low. Even if OCR were to receive a complaint, there is a chance that it will not fine the covered entity and might even provide technical assistance to help the entity become compliant. This all factors into a covered entity's risk calculation and its incentive for complying with OCR guidance. The risk calculation of HIPAA-regulated entities is in line with the reasoning behind the fourth Parillo factor in that the regulated entity does not look solely at the high cost of one-off enforcement proceedings, but instead looks at a variety of factors in a risk-benefit analysis. Depending on the size of a covered entity, the complexity of its system, and potential risk, the cost of one-off enforcement can vary significantly.[219]

213. *See* 45 C.F.R. § 160.402(a) (2019) ("[T]he [HHS] Secretary will impose a civil money penalty . . . if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.").

214. *Id.* § 160.404(b)(2) (detailing that the civil money penalty ranges from $100 to $50,000 for each violation made without knowledge, $1000 to $50,000 for each violation due to reasonable cause but not willful neglect, $10,000 to $50,000 for each violation made with willful neglect and corrected within 30 days, and $50,000 or more for each violation made with willful neglect and not corrected within the 30-day grace period). Additionally, each tier has a cap of $1.5 million for identical violations during a calendar year. *Id.*

215. *See* Office of Civil Rights, *supra* note 211 (listing all publications regarding resolution agreements and settlements from 2008 through 2019).

216. In 2018, OCR received 25,089 complaints, initiated 438 compliance reviews, and provided technical assistance in 7243 cases for a total of 32,770 cases. Office for Civil Rights, *Compliance Enforcement*, *Enforcement Results by Year*, U.S. DEP'T HEALTH & HUM. SERVS. (Mar. 30, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html [https://perma.cc/D2S8-HU6C].

217. Of the 32,770 total cases in 2018, OCR investigated 1610. *Id.*

218. *Id.*

219. For example, larger hospital systems will likely have a stronger incentive to become HIPAA compliant based on the number of PHI uses and disclosures in addition to their interconnectivity with third-party medical and nonmedical organizations.

However, determining if the covered entity is HIPAA compliant is a complex process. As previously mentioned, the HIPAA Privacy and Security Rules provide a series of administrative, technical, and physical safeguards for covered entities and business associates to follow. However, HIPAA intentionally leaves many of these requirements vague. Additionally, OCR does not respond to individual requests for compliance auditing. Without affirmation from OCR, it is impossible to proactively determine whether a covered entity is HIPAA-compliant. Instead, covered entities may not learn of their noncompliance until OCR investigates and places the covered entity on the "Wall of Shame."[220]

Thankfully, the HIPAA regulatory structure does provide a self-contained way for covered entities to monitor compliance. HIPAA requires that covered entities and business associates designate a "security official" and "privacy official" responsible for the "development and implementation of the policies and procedures required" by HIPAA.[221] This responsibility generally includes adopting appropriate policies and procedures to comply with HIPAA, updating those policies and procedures, overseeing and monitoring those policies and procedures, sending out notices of privacy practices to individuals, collecting business associate agreements and updating as necessary, coordinating training for employees who handle PHI, and handling complaints of alleged noncompliance with HIPAA.[222] While the responsibilities for both the privacy and security official can be fulfilled by one person,[223] more complex and larger covered entities will require more compliance personnel and even rely on third-party services. Additionally, covered entities must designate a contact person or office responsible for receiving OCR noncompliance complaints and communicating with OCR during their investigations.[224]

The HIPAA requirements for having security and privacy officers as well as designated contact persons implicate the second and third Parillo factors—investment in relationships with OCR and prevalence of compliance personnel. Given that the penalty structure is based on culpability level, working closely with OCR might help to reduce the amount that OCR ultimately fines an entity. The covered entity may even avoid a fine altogether through voluntary compliance. Privacy and security officials can help implement necessary changes through required voluntary compliance or OCR's technical assistance. As such, covered entities and business associates have a strong incentive to

220. *See What Is The HIPAA Wall of Shame?*, *supra* note 47.
221. 45 C.F.R. §§ 164.308(a)(2), 164.530(a)(1)(i) (2019).
222. *See generally id.* §§ 164.308, 164.530 (listing required responsibilities for officials).
223. *See id.* §§ 164.308(a)(2), 164.530(a)(1)(i).
224. *Id.* § 164.530(a)(1)(ii).

develop and maintain strong relationships with OCR when faced with a complaint or review.[225]

Finally, covered entities also treat OCR guidance as binding due to public sentiment and concern regarding privacy, which in turn creates a stronger culture of HIPAA compliance.[226] HHS has even acknowledged this reluctance to share patient PHI in fear of violating HIPAA.[227]

Patient confidence that covered entities will ensure the privacy, security, and integrity of their individual health information can affect whether patients choose to go with a certain hospital system. Because HIPAA is necessarily linked to patient privacy, building a long-term patient relationship requires more than just HIPAA compliance; it necessitates a deep commitment by the covered entity to keep PHI safe and private. In 2017, 28% of all data breaches occurred amongst healthcare organizations.[228] Of those breaches, human error was a major contributor: 35% were the result of accidental mishandling of PHI.[229] As mentioned previously, any investigation OCR handles is posted on

225. For example, in July 2017, the Mayo Clinic—the premiere not-for profit academic medical center focused on integrated clinical practice, education, and research—went live with its $1.5 billion investment in a new HIPAA-compliant EHR system. Mike Miliard, *Mayo Clinic Completes Epic EHR Rollout with Final Go-Lives*, HEALTHCARE IT NEWS (Oct. 9, 2018, 11:51 AM), https://www.healthcareitnews.com/news/mayo-clinic-completes-epic-ehr-rollout-final-go-lives [https://perma.cc/H9GC-QYGJ]. Mayo employs over 65,000 people, including more than 4800 physicians and scientists and over 100 information technology compliance personnel. MAYO CLINIC, AN INSIDE LOOK AT MAYO CLINIC 3 (2019), https://mcforms.mayo.edu/mc7300-mc7399/mc7360.pdf?_ga=2.28162876.1838852818.1578354340-1276621027.1578354340 [https://perma.cc/CS3Z-ZD4M]; *Information Security Careers*, MAYO CLINIC, https://jobs.mayoclinic.org/career-profiles/nonSmedical-professionals/information-security/ [https://perma.cc/Y5KE-M8NN]. Mayo has a very complex and large health system, and the number of compliance personnel and the amount spent on its third-party EHR system is indicative of its desire to avoid noncompliance.

226. *See Does HIPAA Help or Hinder Patient Care and Public Safety?: Hearing Before the Subcomm. On Oversight and Investigations of the Comm. On Energy and Commerce*, 113th Cong. 116 (2013) (statement of Tim Murphy, U.S. House of Representatives) (stating that physicians and nurses choose to disclose less PHI for fear of penalties associated with violating HIPAA); Bryan K. Touchet, Stephanie R. Drummond & William R. Yates, *The Impact of Fear of HIPAA Violation on Patient Care*, 55 PSYCHIATRIC SERVS. 575, 575–76 (2004) (concluding that concerns about violating HIPAA leads to covered entities being "less willing to disclose [PHI]"); Ruth Penafiel, *Nurses' HIPAA Phobia Does Exist: How To Address Its Hindrance to EHR Success (Part 1)*, HEALTHCARE GUYS (July 29, 2015), https://www.healthcareguys.com/2015/07/29/nurses-hipaa-phobia-does-exist-how-to-address-its-hindrance-to-ehr-success-part-i/ [https://perma.cc/9JBR-RDT3] (describing HIPAA phobia—the fear of violating HIPAA—and how it hinders EHR adoption and sharing PHI).

227. *See* RFI Coordinated Care, *supra* note 157, at 64,303 ("[S]ome HIPAA-covered entities have expressed reluctance to share this information for fear of violating HIPAA."). Given that HHS did not identify what entities had voiced their concerns, these comments were likely made in a nonpublic manner.

228. *See* VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 4 (2018), https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf [https://perma.cc/43GB-MCU2] (reporting 536 healthcare breaches out of a total of 1906 breaches across all industries).

229. *See id.* at 5.

the proverbial "Wall of Shame,"[230] where anyone can view the covered entity or business associate involved, the number of individuals affected, and the type and location of breach.[231] The public nature of this information can factor into whether a patient chooses to go with a certain hospital system and how they perceive overall patient care quality.[232] Healthcare organizations share this same view—damage to patient trust is costly to the healthcare organization's reputation and bottom line.[233] Both patients and healthcare organizations recognize that without strong PHI privacy protections, patients feel less comfortable and are less likely to remain long-term patients. Due to this patient sentiment, avoiding HIPAA violations is a high priority to healthcare covered entities.

In analyzing the three main reasons for compliance with OCR guidance, most of the Parillo factors are implicated. The only factor that is not implicated is the first factor: pre-approval requirements from the regulating agency. Pre-approval requirements do not actually exist within the HIPAA regulatory framework since OCR does not perform any preemptive compliance reviews prior to investigation of a public complaint. The remaining three factors—investment in relationships to agencies, prevalence of compliance personnel, and high costs for one-off enforcement—weigh heavily in favor of OCR guidance being practically binding for larger and more complex covered entities.

HIPAA mandates that covered entities have security and privacy officials as the point people in case of an OCR investigation. For larger and more complex covered entities such as hospital systems (which are often responsible for individual healthcare provider, billing, and insurance teams), having dedicated compliance personnel is essential to ensuring compliance with HIPAA regulations. Given that CMPs imposed by OCR vary according to culpability level and response time, maintaining strong relationships with OCR is absolutely necessary to avoid the high costs of CMPs and being posted on OCR's "Wall of Shame."[234] All of the applicable Parillo factors support the conclusion that OCR guidance is binding in practical effect.

230. *See What Is The HIPAA Wall of Shame?*, *supra* note 47.

231. Office for Civil Rights, *supra* note 47 (detailing cases currently under investigation for all breaches reported within the last 24 months).

232. *See* Victoria Kisekka & Justin Scott Giboney, *The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes*, 20 J. MED. INTERNET RES. 107, 113–14 (2018) (finding that trust in health information and belief in effectiveness of information security safeguards increases patient perceptions of healthcare quality).

233. FORRESTER CONSULTING, TAKE A DATA-CENTRIC APPROACH TO DATA PROTECTION AND PRIVACY (January 2019) (on file with the North Carolina Law Review).

234. *See What Is The HIPAA Wall of Shame?*, *supra* note 47.

III. OCR'S GUIDANCE ON CARE COORDINATION

As mentioned previously,[235] OCR solicited public feedback to improve HIPAA provisions related to care coordination. OCR specifically mentioned its desire to ensure that HIPAA does not "limit or discourage coordinated care."[236] Although OCR received numerous comments from various healthcare organizations on how to improve HIPAA to clarify care coordination, HHS has yet to make any formal regulation changes. Instead of clarifying care coordination as a whole, OCR published guidance for one specific scenario: sharing PHI between health plans for care coordination purposes.[237] The scant OCR guidance does not clarify whether HIPAA explicitly permits sharing PHI in other scenarios, which leaves covered entities uncertain as to whether sharing PHI for care coordination purposes will constitute a HIPAA violation. Instead, covered entities will need to go through a timely process of obtaining the patient's express authorization or drafting business associate agreements, which is, of course, valuable time that could be spent treating patients.

A. *OCR's Guidance on Care Coordination*

In June 2019, OCR issued guidance regarding how PHI can be shared between health plans to support care coordination and continuity of care (the "guidance").[238] The guidance confirmed that HIPAA allows PHI to be used and disclosed for healthcare operations as related to a second health plan for care coordination purposes.[239] Such disclosures must meet the conditions for permitted healthcare operations disclosures: both entities have or had a relationship with the individual, the disclosure pertains to that relationship, and the healthcare operation is permitted by HIPAA.[240] Since care coordination is included in permitted healthcare operations, disclosures for care coordination purposes are probably permissible without patient authorization.[241] However, such disclosures are still subject to the minimum necessary principle.[242] As a reminder, this means that if covered entities perform activities that qualify under the healthcare operations category of TPO, those entities can use or disclose only the minimum amount of PHI to achieve their intended purpose

235. *See supra* notes 157–60 and accompanying text (describing the Request For Information process).

236. RFI Coordinated Care, *supra* note 157, at 64,302.

237. Office for Civil Rights, *HIPAA and Health Plans - Uses and Disclosures for Care Coordination and Continuity of Care*, U.S. DEP'T HEALTH & HUM. SERVS. (June 26, 2019), https://www.hhs.gov/hipaa/for-professionals/faq/3014/uses-and-disclosures-for-care-coordination-and-continuity-of-care/index.html [https://perma.cc/2LQN-8NCP].

238. *Id.*

239. *Id.*

240. *See* 45 C.F.R. §§ 164.502(a)(1)(i), 164.506(c)(4) (2019).

241. Office for Civil Rights, *supra* note 237.

242. *Id.*

and no more.[243] Any other PHI that could conceivably have a potential benefit for a patient could be necessarily excluded under the minimum necessary principle. Because care coordination requires a holistic understanding of the patient's entire health background, restricting the amount of shared PHI, as required by the minimum necessary principle, reduces the efficacy of care coordination efforts.

The guidance goes on to state that HIPAA permits a health plan that receives PHI from another covered entity to use and disclose that PHI in order to inform individuals about other available health plans it offers without first obtaining the individual's authorization in limited situations.[244] The guidance specifically mentions that typically, disclosure for this purpose would be considered marketing and would not be permitted without prior authorization from the individual.[245] The marketing exception does not implicate care coordination and yet is included in the same guidance, which further emphasizes just how scant the guidance is in clarifying care coordination under HIPAA.

B. *Effect on Care Coordination for HIPAA-Covered Entities*

In effect, the guidance is limited in scope to allow sharing PHI between health plans, so long as that sharing does not fall within one of two marketing exceptions.[246] While it might be fair to assume that the other exceptions to the marketing definition are also applicable to sharing between health plans, OCR did not specifically mention these exclusions in its guidance. Without explicit

243. 45 C.F.R. §§ 164.402(b), 164.514(d) (2019); *see also* Office for Civil Rights, *supra* note 74.

244. Office for Civil Rights, *supra* note 237.

245. *Id.* Marketing is defined as "communication about a product or service that encourages recipients of the communication to purchase or use the product or service." 45 C.F.R. § 164.501 (2019). The marketing rule provided in HIPAA Section 164.508 includes a few exceptions. Exclusions to the marketing rule include face-to-face communication by the covered entity and promotional gifts of nominal value by the covered entity. 45 C.F.R. § 164.508(a)(3)(i) (2019). Additionally, the definition of marketing in Section 164.501 carves out other exceptions. *See* Office for Civil Rights, *supra* note 237 (explaining how the definition of marketing in § 164.501 does not include communication about products or services). OCR's guidance includes both exceptions to the marketing rule but only one from the marketing definition applying to health plan availability. *Id.* The guidance FAQ states that communications regarding "replacements to, or enhancements of, existing health plans" are an exception to the definition of marketing, so long as the covered entity "is not receiving financial renumeration for the communications." *Id.* Thus, a covered entity may disclose PHI that has been received for another purpose so long as the above conditions—the PHI is used to communicate with patients about health plan replacements and the communicating covered entity is not receiving payment—are met. *Id.* OCR's guidance FAQ does not mention several additional exceptions that are mentioned in HIPAA's definition for marketing, including one that explicitly allows for sharing if it is for "care coordination . . . and related functions" that do not fall within the treatment definition. *Compare id.*, *with* § 164.501. For HIPAA's definition of treatment, see *supra* note 82 and accompanying text. Again, this exception is only provided if the covered entity is not receiving financial renumeration in exchange for the communication. § 164.501.

246. See *supra* note 245 for discussion of marketing exceptions.

allowance, it is unclear whether OCR considers these actions as exclusions to marketing and thus permitted without express authorization, or if these actions are not exclusions.

Additionally, the guidance only contemplates situations where either both health plans are covered entities or there is at least a business associate agreement and relationship between the entities sharing PHI.[247] While the purpose of this is to ensure that individuals will not miss opportunities for continued health coverage with a different health plan, there are still many gaps regarding whether authorization is required in other situations involving care coordination. Since both entities must be covered entities (or at least business associates) with a relationship to the individual, the guidance does not consider whether a covered entity can share PHI with a nonmedical third party for care coordination purposes. As mentioned previously,[248] sharing information about patients to determine eligibility for third-party social services can be imperative for providing continuity of care for medically indigent people. The requirement for a previous relationship with the individual and some sort of covered status, whether as a covered entity or business associate, can significantly slow down the delivery of required medical care and even deter some patients and their families from seeking care. Without further guidance from OCR or HHS for all forms of care coordination, providers can be liable for sharing PHI without authorization. More importantly, many patients will fall through the cracks without receiving timely medical care.

For illustrative purposes, I will use the previous example with our diabetic patient.[249] In order to help manage the patient's diabetes, her primary care physician, a covered entity, wants to coordinate with a community-based diabetes support group right in the patient's neighborhood.[250] The support group is not any sort of healthcare provider or other covered entity, nor is it a business associate since it has not worked with a covered entity before. Under the current HIPAA rules, her physician will not be able to share the patient's PHI with the support group for care coordination purposes without the patient's express authorization. Thus, the provider would need to contact the patient to have her sign an authorization document specifically detailing what PHI will be shared and who is receiving it. This can become quite cumbersome for both the provider and the patient, wasting time and demoralizing both

247. *See* Office for Civil Rights, *supra* note 237.

248. *See supra* Section I.B.

249. *See supra* text accompanying notes 108–15.

250. In this scenario, the support group helps to ensure that patients stick with their diabetes health plan of restricted diet, increased exercise, and frequent check-ins with the provider. Support groups for chronic diseases, including diabetes, have been shown to improve healthcare outcomes. *See* Jina Huh & Mark S. Ackerman, *Collaborative Help in Chronic Disease Management: Supporting Individualized Problems*, COMPUTER SUPPORTED COOPERATIVE WORK, Feb. 2012 at 853.

parties such that these connections are often not made even though they can be quite useful for continuous management of chronic conditions.

For an indigent patient in the same exact scenario, this could be even worse. Reduced or free community-based services may indeed cater to medically indigent patients but covered entities likely cannot share a patient's qualifications with those programs. In other words, the indigent patient may have theoretical access to a plethora of services to help manage their chronic disease but will never know of them because of HIPAA's restrictions on care coordination. Due to the expensive cost of medications and healthy food, the medically indigent patient cannot improve her diabetic condition and continues to languish with dangerous health outcomes.

The OCR guidance does not address situations like these at all since there is still an inherent requirement that sharing PHI for care coordination purposes can only be done by covered entities or business associates. While this would not be an issue if the third-party service already has a previous relationship with the patient and is a business associate of the covered entity (which must be memorialized in a business associate agreement), drafting such an agreement between every single party involved in care coordination is voluminous work that is typically done on an ad hoc basis.

IV. HIPAA NEEDS TO REDEFINE CARE COORDINATION IN PROPER SCOPE

Modification of the HIPAA Privacy Rule would best facilitate exchanges of information and support care coordination. The most feasible solution is through regulatory change as opposed to OCR guidance. OCR guidance is limited because it cannot establish standards for social service agencies and community-based programs that are separate from the existing entities covered by HIPAA. Under the existing framework, these third parties can only operate as business associates, which requires business associate agreements or express authorization from the individual—both of which hamper the care coordination model due to their administrative costs. As such, regulatory change, rather than after-the-fact remedies, can most effectively improve care coordination under HIPAA.

Nonetheless, there are some downsides to regulatory change through the APA—namely, that it is time consuming and subject to approval by both the Executive Branch and Congress. Additionally, the APA mandates a minimum 30-day comment period for public input on updates. Despite this, regulatory change remains the most viable path forward to improve care coordination under HIPAA given the ineffectiveness of OCR guidance and the confusion that would inevitably result.

The alternative to regulatory change would involve rewriting the HIPAA statutes themselves. Certainly, this pathway through Congress would provide

more democratic accountability as House and Senate members must balance their constituents' interests. Additionally, Congress, due to its wide-ranging expertise, might also be better at looking at the bigger picture and crafting law that fits within the broader scope of the American legal system.

However, the efficiency of administrative agencies outweighs potential benefits from the congressional legislative process. Congressional rulemaking is limited due to its broad scope in that any legislation will reflect value tradeoffs between each individual legislator's political party, constituency represented, and special interest groups, creating milder and less effective laws or even a complete standstill.[251] In a similar vein, the bicameral nature of Congress often results in milder laws in order to successfully pass at the House of Representatives, Senate, and Executive stages.[252]

Instead, HHS is better equipped to create a regulation that properly frames the care coordination issue. First and foremost, HHS consists of specialists in healthcare who can provide smarter, more practical rules for covered entities involved in care coordination. And while it is not an elected body, HHS is not wholly without oversight; it must engage with the public during the decisionmaking process and receive significant input before crafting any regulations.[253] Thus, regulatory change by HHS is the best option going forward to achieve effective, comprehensive medical care that utilizes care coordination.

A. *Express Provision To Allow Disclosure to Nonmedical Third-party Agencies for Care Coordination Purposes*

The most effective way to facilitate a comprehensive care coordination model is for HHS to create a HIPAA regulatory permission that explicitly permits covered entities and related business associates to use and disclose PHI

251. *See generally* THOMAS E. MANN & NORMAN J. ORNSTEIN, IT'S EVEN WORSE THAN IT LOOKS: HOW THE AMERICAN CONSTITUTIONAL SYSTEM COLLIDED WITH THE NEW POLITICS OF EXTREMISM (2012) (attributing Congressional ineffectiveness to a vehemently adversarial system and outliers on the political spectrum caused by factors such as political donors, party ideals and pressure, and angry constituents); Kathy Canfield-Davis et al., *Factors of Influence on Legislative Decision Making: A Descriptive Study- Updated August 2009*, 13 J. LEGAL ETHICAL & REG. ISSUES 55, 56 (2010) (identifying factors that shape legislative decisionmaking as perceived by lawmakers); Geoffrey C. Layman, Thomas M. Carsey & Juliana Menasce Horowitz, *Party Polarization in American Politics: Characteristics*, *Causes*, *and Consequences*, 9 ANN. REV. POL. SCI. 83, 83–97 (2006) (analyzing the causes for partisan polarization across major issues).

252. *See generally* William N. Eskridge Jr. & John Ferejohn, *The Article I*, *Section 7 Game*, 80 GEO. L.J. 523 (1992) (explaining through game theory how regardless of where a bill starts on the political spectrum, the version signed into law will inevitably be milder than originally envisioned due to the congressional bicameral process and administrative agencies effectuating legislation).

253. Administrative agencies, however, are not required to consider comments by regulated entities in their rulemaking; they merely need to provide notice of and an opportunity to comment on proposed rules. *See* 5 U.S.C. § 553 (2018).

to social service agencies and community-based support programs. Effective treatment, especially for low-resource individuals and the medically indigent, requires utilizing all facets of medical care clinical services in combination with social services. Many clinical interventions are much less effective or even ineffective unless pursued in coordination with social service agencies, which can assist in finding appropriate health and housing services, consistent sources of healthy food, support groups, or protective services—resources not typically offered or available by traditional covered entities and related business associates.

Many of these supporting agencies are considered noncovered entities under the current HIPAA Privacy Rule, meaning that individuals need to provide express authorization so that covered entities may share PHI with these third parties.[254] To ensure the security of PHI for these noncovered entities, HIPAA should be modified to create a semicovered entity that is subject to aspects of HIPAA requirements by virtue of either participating in or providing care coordination services that require sharing of PHI. Creating a separate category for care coordination entities would allow HHS and OCR to regulate these supporting agencies, create separate privacy standards tailored to their needs and purposes, and ease provider hesitance in sharing PHI with a noncovered entity.

A new "care coordination associate" entity would require several provisional changes to the definition, safeguards, and use and disclosure provisions of HIPAA.[255] First, the care coordination associate definition would need to encompass all potential entities for all purposes; thus, it needs to be appropriately broad and tied to the definition of care coordination, which also needs to be defined in the definition section.[256] Until now, care coordination has been defined numerous ways by a variety of sources.[257] One suggestion is to use the one provided by the Agency for Healthcare Research and Quality ("AHRQ"): "deliberately organizing patient care activities and sharing information among all the participants involved with a patient's care."[258]

Secondly, the care coordination associate will need to have the appropriate organizational safeguards to ensure compliance with HIPAA's standards for privacy protection.[259] Given the limited scope of services that care coordination associates provide, it seems unnecessary to have the same stringent safeguard

254. *See* 45 C.F.R. § 164.508 (2019).

255. There will likely be other areas of HIPAA that HHS will need to update to accommodate a care coordination associate entity, such as breach notification. However, this Comment will not address them.

256. 45 C.F.R. § 160.103 (2019).

257. *See supra* notes 90–94 and accompanying text.

258. *Care Coordination*, *supra* note 5.

259. *See* 45 C.F.R. §§ 160, 164.102–106, 164.302–318 (2019).

restrictions as a covered entity or business associate. But some safeguards should still be made by balancing the cost and feasibility of implementation against the calculated risk of breach or lack of privacy. Such a balancing test is not unprecedented. HIPAA already provides specifications based on a flexible approach where covered entities "may use any security measures . . . to reasonably and appropriately implement the standards and implementation specifications" of the Privacy Rule.[260] This approach looks at factors such as the size, complexity, and capabilities of the entity; the entity's technical infrastructure, hardware, and software security capabilities; cost of security measures; and probability and criticality of potential risks to privacy.[261] Given the flexibility of the approach, this provision probably does not need significant change for the care coordination associate. Nonetheless, this approach does not provide clear standards and it would be valuable for OCR to provide some guidance on what appropriate specifications would look like for a care coordination associate.[262]

Finally, there needs to be an explicit care coordination provision added to the general rules for uses and disclosures of PHI.[263] Because care coordination associates will not fall squarely in another covered entity or business associate category, they will need to have specific rules for their use and disclosure of PHI. These rules should have a wide berth for a care coordination associate to receive and use PHI for care coordination and population-based health activities. On the other hand, the rules regarding disclosure of PHI should be flexible to accommodate for the different roles that care coordination associates can have. If the care coordination associate is a support or social service agency, HIPAA's allowance for disclosure should be minimal. Since these services are typically at the fringes of the care coordination model (the final entity to which a patient is referred and services are rendered), they do not need to further refer patients to organizations outside of the existing model; rather, they will likely only need to disclose updated PHI within the care coordination model. For example, a food delivery service will not need to refer the patient to another organization, but will need to provide updates, such as frequency and content of service, to parties already in the patient's care coordination model. While many of the third parties described above do not need all PHI aggregated for a patient,[264] it would be foolish and short-sighted to conclude that these scenarios are exhaustive. There may be scenarios where a care coordination associate can

260. *Id.* § 164.306(b).

261. *Id.* § 164.306(b)(2)(i)–(iv).

262. Incidentally, this is one of the intended purposes for administrative guidance: stating what is or is not viable under the corresponding federal regulations.

263. *See* 45 C.F.R. § 164.502(a) (2019).

264. *See, e.g.*, *supra* text accompanying notes 129–134. For example, meal delivery services likely only need a patient's name, phone number, address, and dietary needs, while a patient's previous phone numbers or addresses are probably not necessary.

better tailor their service to handle a patient's chronic condition using patient preferences and family history; in these instances, the rules should allow for disclosure of PHI for such purposes.

Additionally, because care coordination associates are service providers assisting patients in care management rather than providers of more direct treatment, HIPAA should not allow disclosures for other activities such as sale of PHI or other marketing uses. However, as discussed above, HIPAA still needs to permit care coordination associates to disclose information to other parties involved in a given patient's care coordination, regardless of whether they are a covered entity, business associate, or fellow care coordination associate. Allowing disclosures to all entities involved in a patient's care coordination allows the care team to dynamically adjust to changes in a patient's condition.

Moreover, HIPAA should continue to allow care coordination associate disclosures related to population-based health activities. Population-based health uses health data from individuals within a community to study general trends and create treatment plans based on aggregate data, improving the overall community health outcome.[265] Allowing care coordination associates to share and disclose PHI for population-based health reasons would provide additional patient data points. HIPAA currently allows sharing PHI for population-based activities reasons through the healthcare operations prong of TPO exceptions,[266] but an explicit mention in the HIPAA rules or an OCR guidance would clarify this point.

The main argument against a care coordination associate solution is that the HIPAA regulations already permit care coordination. As mentioned previously, [267] care coordination appears to fall under the "treatment" or "healthcare operations" prongs of HIPAA's TPO permitted uses and disclosures. Covered entities and business associates can share PHI for TPO purposes without reaching out to the patient for permission or, if the target of the shared PHI is not already a business associate, by drafting and executing a business associate agreement before sharing PHI. This, however, is still subject to a significant limitation—the minimum necessary principle. Unless the disclosure is to a healthcare provider, the covered entity will need to limit the PHI shared to just what will immediately treat the healthcare issue and nothing more. The minimum necessary principle hinders a true care coordination model, which requires a complete picture of patients to treat them holistically. This can lead to worsened healthcare outcomes and disproportionally affects patients who are indigent or suffer from chronic conditions.

265. *See supra* text accompanying note 138.

266. *See supra* text accompanying note 136–40.

267. *See supra* Section I.C.

Additionally, the language for the TPO prongs are vague, mentioning care coordination but not truly defining it.[268] As such, HIPAA-regulated entities fear violating HIPAA due to the public complaint-driven enforcement system, the high costs of violation, and patient confidence in health privacy.[269] Covered entities are reluctant to disclose PHI unless they are completely sure that such an action is expressly permitted by HIPAA. The recent OCR guidance on care coordination did not successfully define which care coordination scenarios are allowed, except for the health-plan-to-health-plan exception. As the HIPAA regulations are currently written—with a strict minimum necessary principle and vague TPO language—HIPAA-regulated entities are not willing to broadly share PHI for care coordination purposes.

Another argument against the care coordination associate solution is the additional cost to achieve compliance for resource-constrained organizations. The care coordination associate designation would thrust additional responsibilities on cash-strapped organizations to ensure patient privacy for care coordination purposes; however, such responsibilities will likely be manageable. For organizations that are already covered entities or business associates, HIPAA requires a designated "security official" and "privacy official,"[270] in addition to a contact person for OCR investigations.[271] The theoretical responsibilities of a care coordination associate are not significantly different from the existing responsibilities of compliance officers. As such, these responsibilities are unlikely to be an undue burden on these organizations, especially considering how they can improve the efficacy of a care coordination model.

Third-party organizations involved in care coordination that are not already regulated under HIPAA will feel the greatest burden with the introduction of a care coordination associate designation. These newly covered third parties will need to handle new responsibilities for patient privacy and security measures. However, if the care coordination associate did not exist, these third-party organizations would need to become a business associate to receive, use, and disclose health data from a covered entity. This would force them to follow all the administrative, technical, and physical safeguards required of a business associate, and subject them to the minimum necessary principle. In the existing HIPAA regulations, third-party organizations involved in care coordination need to undergo a privacy and security overhaul to become HIPAA compliant. With the care coordination associate delegation, third-party organizations will have the burden of similar, but possibly reduced,

268. *See supra* note 136 and accompanying text.
269. *See supra* Section II.C.
270. *See supra* text accompanying notes 221–22.
271. *See supra* text accompanying note 224.

privacy and security requirements, but greater access to a patient's holistic health information which will allow for more effective care coordination.

B. *Expand Exceptions to the Minimum Necessary Principle*

A separate approach to accomplish holistic care coordination is to expand the exceptions for the minimum necessary principle.[272] Under the existing framework, the minimum necessary principle applies to care coordination-related exchanges and limits sharing PHI to absolutely necessary information for the treatment or support for the immediate issue. This, however, is shortsighted since covered entities adhering to the minimum necessary principle will only address the most recent clinical issue. The limited treatment model caused by the minimum necessary principle is insufficient in allowing for effective care coordination and populated-based health initiatives. It also fails to consider assistance that nonmedical third-party entities can provide.

Instead, HHS should expand minimum necessary exceptions to encompass care coordination and population-based activities. The current regulation has only one health-care-related exception: for treatment reasons between health providers. Explicit allowance for care coordination and population-based activity purposes would encourage freely sharing PHI to noncovered entities involved in care coordination. This also allows for a comprehensive, person-centered approach where entities involved in care have complete pictures of the healthcare services that an individual receives. For low-resource patients and patients with chronic health conditions, who are often seen in various provider settings, a holistic approach can be critical to their care. Furthermore, a holistic approach can better address health issues that affect the broader community. Expanding the minimum necessary principle in the care coordination context can ensure that HIPAA does not impede covered entities in sharing the necessary PHI to promulgate the best possible healthcare services.

Additionally, adding a care coordination exception is the best approach to fix the minimum necessary principle since changing its definition[273] would have broader implications beyond the care coordination and overall population health context. Maintaining the existing definition while adding a care coordination exception retains flexibility in the standard while also protecting from unwarranted disclosures in other scenarios.

Modifying the minimum necessary principle could work as a solution on its own, but HHS could also integrate this solution into the care coordination

272. *See* 45 C.F.R. § 164.502(b)(2) (2019) (listing scenarios where the minimum necessary principle does not apply); *see also supra* notes 73–78 and accompanying text.

273. § 164.502(b) ("[A] covered entity must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.").

associate approach discussed above. Because the care coordination associate approach permits full use and disclosure to any entity involved in a patient's care coordination, expanding minimum necessary exceptions may be extraneous. However, expanding minimum necessary exceptions would provide additional clarity and emphasize that HIPAA allows for free sharing, encouraging entities to rely on a comprehensive care coordination model.

Furthermore, because these noncovered entities would not be subject to HIPAA as a covered entity or business associate, HHS would need to establish some sort of security and privacy standards to ensure secure handling of PHI as a collateral consequence of only modifying the minimum necessary principle. This would require going beyond carving out exceptions to the minimum necessary principle and require HHS to consider these additional factors in crafting regulations. Previously noncovered entities would need to implement administrative, technical, and physical safeguards—a costly endeavor for a third-party organization. Thus, merely adding exceptions to the minimum necessary principle creates collateral changes that are much more expansive than originally envisioned.

Ultimately, the first approach would be a more sweeping change—and probably more effective. But if it is not possible to adopt, then modifying the minimum necessary principle is a quick and simple solution. However, in modifying the minimum necessary principle, there will need to be additional consideration paid to how the noncovered entity will receive and handle PHI in a secure manner.

CONCLUSION

Without a clear definition for care coordination under HIPAA, covered entities are limited to providing care coordination for TPO purposes only. In order to work with third-party nonmedical social services, covered entities must take on a costly work-around by implementing business associate agreements or obtaining express authorization from patients. Yet these third parties can play a critical role in the proper management of chronic diseases for the medically indigent, even if their support services are not traditionally thought of as treatment.

This convoluted path makes for poor care coordination. After all, comprehensive care coordination requires an open communication network where entities involved can freely communicate with each other regarding a patient's physical, psychological, social, and spiritual well-being so that they may be able to adjust and adapt a patient's care plan as necessary. Additionally, these third parties need more flexibility to share data on population-based health activities, which can ultimately improve a community's overall health outcomes.

While the recent OCR guidance has clarified some areas related to care coordination, specifically for health plans and marketing purposes, guidance alone is insufficient to remove the barriers perceived by covered entities. Instead, reform to HIPAA regulations is the only way to accomplish this and ensure that care coordination can be maximized. Without HIPAA reform, indigent patients with chronic conditions will continue to languish with a high risk for serious health complications in the future.

FRANK QIN**

** I would like to thank Professor Joan Krause, Professor Kathryn Marchesini, and my Topic Editor, Jessica O'Brien, for their guidance in developing this topic and providing invaluable practical perspectives. I would also like to thank my Primary Editor, Morgan Maccherone, and the Board and Staff Members of the *North Carolina Law Review* who helped to fashion my idea into a publishable Comment. Lastly, I am thankful for my experience working at the premiere EHR software company, Epic, where I was first introduced to the world of Health IT, and the wonderful people I met along the way.