Chapter 4

Proliferation of Health Care Data: Navigating Interoperability and Data Sharing Opportunities and Challenges

Alaap Shah
Karen Mandelbaum
Elizabeth (Beth) Scarola

Epstein Becker & Green, PC

4.1 Introduction

Innovations in modern day medicine depend greatly upon our ability to obtain, meaningfully interpret, and analyze a sufficient number of data points: Data is king! Arguably, when human life, health, and welfare are involved, such as in the health care settings, there are only two types of decision paradigms: decisions that *are* data driven and ones that *should be*.

The global response to the COVID-19 pandemic is a prime example of why robust data collection and sharing can promote health, prevent loss of life, and revolutionize global health care delivery. Fortunately, over the past two decades, many health care and life science companies had prepared themselves by steadily investing

in infrastructure and technologies. By the time COVID-19 became a pandemic, these companies were uniquely situated to utilize digital data to fight it. Digital data became the new oil powering the engine of progress. Many organizations have harnessed data in numerous ways to improve quality of care, drive down costs, and improve population health.[1] Patients have gained more access to their own health care data through patient portals, personal health records, and other health information exchange technologies, empowering them to be active participants in their own health care journeys. For years, health care data was underutilized. Its current day proliferation creates new opportunities.

Yet, while the proliferation of data presents immense opportunities, numerous risks and challenges hamper the ability to capture, share, and analyze data in ways that may unlock the insights contained therein. These opportunities and challenges will be discussed throughout this chapter.

4.1.1 Exponential Data Growth in Health Care

Providers, payers, life science companies, digital health companies, wearable tech companies, telehealth companies, diagnostic companies, laboratories, and a cornucopia of other entities generate an ever-growing pool of data. In 2014, estimates indicated that the volume of health care data would grow from approximately 153 exabytes produced in 2013 to an estimated 2,314 exabytes produced in 2020.[2] Other experts estimate that in the year 2025 there will be 500 times more health care data than in the year

[1] *See generally,* The Rise of the Data-Driven Physician, Stanford Medicine 2020 Health Trends Report, http://med.stanford.edu/content/dam/sm/school/documents/Health-Trends-Report/Stanford%20Medicine%20Health%20Trends%20Report%202020.pdf.

[2] The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, EMC Digital Universe with Research and Analysis by IDC (April 2014), https://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm.

2012.[3] That scale is hard to fathom, and harder to verify, as health-related data spans information captured in clinical and non-clinical settings. However, some more understandable estimates have emerged. For example, every patient in the world adds approximately 80 megabytes of electronic health record (EHR) and imaging data each year.[4] That number alone illustrates the rapid escalation of data volume in health care. Yet, this estimate fails to capture the vast amount of data generated by sources such as wearable technologies, digital health and wellness apps, telehealth encounters, medical devices and sensors, insurance claims, laboratory testing, genomic and genetic tests, social media, and numerous other health care Internet of Things (IoT) devices.

Increasingly unfathomable amounts of health-related data are generated over time; but, to what end? Harnessing the power of this exponential data growth, in the health setting, requires fostering a culture that continues to ask and answer one question: *What don't we know, that, if we knew, would improve the quality and efficiency of health care, and benefit overall patient experience?* Asking and answering this question can help identify what gaps exist, determine what data are needed to fill to those gaps, and drive efforts to capture and harness the data to obtain insights that will drive advances in health care. Once an organization has determined its data needs, it must navigate the thorny legal, regulatory, and technological landscape to obtain, use, and share the captured data in ways to achieve desired goals. This chapter provides practical guidance on how to traverse this evolving landscape.

---

[3] Galetsi, Panagiota, Korina Katsaliaki, & Sameer Kumar, *Big Data Analytics in Health Sector: Theoretical Framework, Techniques and Prospects*, 50 *International Journal of Information Management* 206-216 (2020), https://fardapaper.ir/mohavaha/uploads/2019/12/Fardapaper-Big-data-analytics-in-health-sector-Theoretical-framework-techniques-and-prospects.pdf.

[4] Marco D. Huesch & Timothy J. Mosher, *Using It or Losing It? The Case for Data Scientists Inside Health Care*, NeJM Catalyst (2017), https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0493.

4.1.2 Drivers of Data Growth and Innovation in Health Care

The passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009 drove mass digitization of heath data.[5] Under HITECH, Congress created the Centers for Medicare and Medicaid Services (CMS) "Meaningful Use Program" (now called the Promoting Interoperability Program) to incentivize providers to adopt EHR systems. Over the next two decades, the health care industry achieved nearly ubiquitous adoption of EHRs and largely converted paper-based processes to digital recordkeeping and data exchange with payers.[6] The CMS Meaningful Use Program drove data proliferation further by creating opportunities for providers to utilize EHR data to showcase quality. Through these efforts, CMS sought to shift payment paradigms from traditional fee-for-service to value-based reimbursement models.[7]

As data storage generally became inexpensive and scalable through abundant and secure cloud storage, organizations could retain and repurpose data in ways never before imaginable. As health care organizations amassed data, demand for data access grew to promote research and innovation. Many companies began to leverage these amassed data assets internally to innovate and deploy

[5] Pub. L. No. 111-5, Title XIII, 123 Stat. 226 (2009).

[6] The Centers for Disease Control and Prevention estimates over 85% of office-based physicians have adopted the use of electronic health records. *See Electronic Medical Records/Electronic Health Records (EMRs/EHRs)*, CDC, https://www.cdc.gov/nchs/fastats/electronic-medical-records.htm (last modified March 3, 2020).

[7] Under the CMS Medicare and Medicaid Promoting Interoperability Programs, CMS requires eligible providers to electronically report eCQMs, which use data from EHRs and health information technology systems to demonstrate attaining certain health care quality measures. *See, generally*, *Electronic Clinical Quality Measures Basics*, CMS, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ClinicalQualityMeasures (last modified Jan. 14, 2020).

more precise, cost-efficient, and impactful interventions.[8] Over time, the external demand grew for data sharing between provider and payers on the one hand, and pharmaceutical companies and technology companies on the other hand.

Yet, over time, the industry and federal government recognized that most organizations existed as "data siloes" and that health information technology systems could not interoperate with one another; thus, data could not readily be shared amongst stakeholders. To address this challenge, the public and private sector sought to establish interoperability policies and standards to foster data sharing through application program interfaces and health information exchanges and networks. Those efforts created immense opportunities for the health care industry.[9] Health care data is becoming easier to collect, store, analyze, *and share*, which is facilitating further data propagation, lowering health care costs, advancing health care quality, and improving population health.

Health data is now collected beyond the walls of the clinic or hospital. In 2013, Gartner predicted that the health care IoT (convenient, efficient, and automated devices and software applications that connect to information technologies through computing networks and transmit data) would include approximately 26 billion devices by 2020.[10] Experts expect this market to continue to grow rapidly, with estimates that the market will grow from

[8] *See* Alaap Shah, *Artificial Intelligence and the Internet of Things in Health Care in* AHLA HEALTH LAW WATCH 2019 (AMER. HEALTH LAW ASSOC., 2019).

[9] Nagasubramanian, Gayathri, et al., *Securing e-health records using keyless signature infrastructure blockchain technology in the cloud*, 32 Neural Computing and Applications 639–647 (Feb. 2020), https://link.springer.com/article/10.1007%2Fs00521-018-3915-1.

[10] *See* Nick Jones, *The Internet of Things Will Demand New Application Architectures, Skills and Tools*, Gartner Research (Apr. 1, 2014), https://www.gartner.com/en/documents/2697819/the-internet-of-things-will-demand-new-application-archi.

$41 billion in 2017 to $158 billion by 2022.[11] More IoT will inevitably drive more data proliferation. In many ways, this decentralization of health care has facilitated continuity of care on remote bases, such as through telehealth and other digital means.

The goal of interoperability is to promote data access across the entire continuum of care, with the patient as the central focus. First, interoperability increases patients' access to their own data. Second, enhanced access enables patients to make better informed health care decisions. However, *caveat emptor*. Interoperability further drives the proliferation and commercialization of health data. As third-party app developers collect data, some might seek to leverage such patient data for various secondary commercial purposes.

Unsurprisingly, health care data is valuable. Big tech companies, and even small tech startups, realize the lucrative potential. In the past few years, health care providers, payers, and technology companies have formed large scale partnerships to facilitate data exchange. These alliances share the common purpose of reforming health care through data-driven decision-making, using big data analytics and artificial intelligence (AI), both of which require data sets of sufficient volume, variety, and veracity to develop, train, and operate successfully.[12] These more recent developments will likely drive data proliferation faster and further than before.

4.2 Overview of Key Legal Issues

U.S. privacy and data protection laws are a complex patchwork comprised of myriad federal and state laws, and regulations spanning several agencies. Additionally, there are various federal

[11] *See Medtech and the Internet of Medical Things: How connected medical devices are transforming health care*, Deloitte (July 2018), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf.

[12] Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, *The Wall Street Journal*. (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.

and state legislative proposals on the table, intended to address the pace of technological innovation impacting the industry. Due to the piecemeal nature of these laws, several gaps in privacy and data protection exist which create significant risks to individuals whose data may be shared and used without sufficient guardrails in place.

4.2.1 HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[13] was enacted during a time in which the health care industry maintained health records on paper. HIPAA serves as the predominant federal law governing use, disclosure, and protection requirements for protected health information (PHI).[14] HIPAA applies to "Covered Entities" and their "Business Associates" and sets a federal floor for data protection.[15] Though HIPAA reaches a large number of entities in the health care sector, an increasing number of technology companies are entering the health care space in ways that will not subject them to HIPAA regulation.

HIPAA was amended by HITECH in 2009 (with regulations following in 2013) to promote patient access to electronic medical records. HITECH requires that an individual's choice to share information with third parties "must be clear, conspicuous, and specific."[16] However, some argue that HIPAA and HITECH's protections do not go far enough.

---

[13] Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[14] *See* 45 C.F.R. § 160.103 for the definition of protected health information. Note that HIPAA also establishes de-identification standards which could be germane to allow entities to created de-identified data sets to train AI and IoT technologies. *See* 45 C.F.R. §§ 164.514(a)-(c); *see also 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 of Health and Human Servs. Office for Civil Rights (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[15] *See* 45 C.F.R. § 160.103 for definitions of Covered Entity and Business Associate.

[16] 45 C.F.R. § 13405(e)(1).

An increasing amount of data now flows through technologies and organizations not regulated by HIPAA. These technologies and organizations may be regulated by state laws (e.g., the California Consumer Privacy Act, discussed below) or the Federal Trade Commission Act; but, to date, there is no comprehensive federal law governing the security and privacy of consumer health information flowing beyond HIPAA's reach. This creates significant confusion about what privacy protections apply as data flows throughout the health ecosystem.

4.2.1.1 Breach Risk (Continues to Rise)

While HIPAA purportedly establishes the data protection standards[17] by which Covered Entities and Business Associates should operate, cyber threats and data breach risks continue to rise. Recently, the Federal Bureau of Investigation (FBI), U.S. Department of Health and Human Services (HHS), and the Federal Cybersecurity and Infrastructure Security Agency (CISA) released a report calling attention to rampant ransomware[18] attacks targeting the health care sector.[19] Health data breaches increase year over year

[17] It should be noted that HIPAA has been criticized as being antiquated in today's technologically advanced world as well as lacking clear prescription on privacy and security controls required for compliance. On January 5, 2021, HITECH was amended to require that "recognized cybersecurity practices" be considered by the Secretary of HHS in determining any HIPAA fines, audit results, or mitigation remedies. Pub. L. No. 116-321 (Jan. 5, 2021).

[18] Ransomware is a serious form of cyber extortion that employs malware to prevent users from accessing their systems or data, either by locking the system or encrypting critical files until a ransom is paid. The hacker holds the key to unlock the system and usually demands payment in cryptocurrency.

[19] Cybersecurity & Infrastructure Security Agency, Ransomware Activity Targeting the Health care and Public Health Sector, Alert (AA20-302A) (Oct. 28, 2020), https://www.us-cert.gov/ncas/alerts/aa20-302a (last revised Nov. 2, 2020).

at staggering rates,[20] and the cost of such breaches is the highest among all sectors.[21]

Recent HIPAA modifications were promulgated with the understanding that the digitization of health data is on the rise. Data breach risks inherently multiply with technologic advancements and adoption due to the expanded attack surface created by increasing nodes on a network (e.g., wearables, apps, and other smart devices).[22] Similarly, in terms of decentralization among entity functions, breach statistics indicate that in 2020 alone, 11 of the 20 largest data breaches occurred at the Business Associate level, which highlights the need for more robust diligence, contracting, and ongoing management of vendors that capture, process and/or host personal information. Further, breach risks multiply exponentially as data proliferates and moves between HIPAA-regulated to largely unregulated entities.

4.2.1.2 Recent and Future HIPAA Modifications

The HHS Office of Civil Rights (OCR) recognized HIPAA's limits when it issued a Request for Information[23] in December 2018 seeking feedback regarding areas where HIPAA could be modified to, *inter alia*, improve care coordination and individual engagement. On January 21, 2021, HHS issued the notice of proposed rulemaking

[20] *See* Steve Adler, *2019 Healthcare Data Breach Report*, HIPAA Journal (Feb. 13, 2020), https://www.hipaajournal.com/2019-healthcare-data-breach-report/ (noting a 37.4% increase in breaches over 2018 and more total breaches in 2019 than that combined number from years 2009-2014); *see also* Steve Adler, 2020 Healthcare Data Breach Report, HIPAA Journal (Jan. 19, 2021), https://www.hipaajournal.com/2020-health care-data-breach-report-us/ (noting a 25% increase in breaches over 2019 with 92% of breach records resulting from hacking/IT incidents).

[21] *See* IBM Security, *Cost of Data Breach Report* (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (noting that health care average breach cost to be $7.13 million which is a 10.5% increase over 2019).

[22] *See* Alaap Shah, *Death by a Thousand Cuts: Cybersecurity Risk in the Health Care Internet of* Things, *in* AHLA Weekly (May 18, 2018).

[23] 83 Fed. Reg. 64302 (Dec. 14, 2018).

(NPRM) titled "Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement."[24] According to HHS Deputy Secretary, Eric Hargan, the proposed rule aims to "reduce burden on providers and support new ways for them to innovate and coordinate care on behalf of patients, while ensuring that [HHS] uphold[s] HIPAA's promise of privacy and security."[25]

The objective of the NPRM is to strengthen and clarify the individual right of access to PHI through shortened response timelines, fee notices, and documentation requirements, along with restricting certain identity verification procedures. This emphasis on patient empowerment is a continuation of HHS's emphasis on patients over paperwork. OCR's current enforcement posture related to the patient right of access highlights this objective.[26] The NPRM also bolsters care coordination by clarifying the scope of activities encompassed within "health care operations." Notably, these proposed amendments would codify the patient's right to authorize third party access to their PHI. This would likely encourage greater data sharing beyond Covered Entities and Business Associates. Finally, in line with its efforts during the COVID-19 pandemic, the NPRM also bolsters data sharing in the context of emergencies and other health crises.

During 2020, and likely well into 2021, the COVID-19 pandemic tested the limits of HIPAA relative to the federal government's public health emergency response efforts. Specifically, OCR took a number of steps to relax HIPAA rules to support greater sharing of

[24] 86 Fed. Reg. 6446 (Jan. 21, 2021).

[25] HHS Proposes Modifications to HIPAA Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens, HHS (Dec. 10, 2020), https://www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html.

[26] Since OCR made the HIPAA Right of Access Initiative an enforcement priority in 2019, OCR has settled 14 investigations between September 9, 2019 and January 12, 2021, which resulted in over $900,000 in settlement payments.

PHI to combat the pandemic as well as support continuity of care. These efforts included clarifying (1) how HIPAA-subject entities could share PHI for public health purposes, (2) how providers could leverage consumer apps to provide telehealth, and (3) how OCR would exercise enforcement discretion related to privacy and security rule violations. On a grand scale, the pandemic has fostered greater data sharing and proliferation while also reinvigorating the debate about HIPAA's role in an era when individuals increasingly interact virtually with the health care sector via telehealth, wearables, and IoT.

4.2.2 The 21st Century Cures Act

On December 13, 2016, President Obama signed the 21st Century Cures Act (Cures Act) into law.[27] The Cures Act enjoyed the most bipartisan support of any law in many decades. Provisions of the Act included funding to accelerate new and innovative treatments, drug and device development, and health care delivery. A common theme running through many provisions was the promotion of data sharing. The Cures Act was the push the health care industry needed to improve and encourage data sharing by recognizing the critical role it plays in improving the health of individuals and communities.[28] To understand the Cures Act, it is necessary to understand the backstory.

The turning of the century ushered in the age of savvy consumers and big data, and health care was not immune. The internet, and online access to information about health, opened a new world of knowledge and educational resources for patients and caregivers. The health care industry was slow to adopt technology, however.

---

[27] Act to Accelerate the Discovery, Development, and Delivery of 21st Century Cures, and for Other Purposes, Pub. L. No. 114–255, also known as the 21st Century Cures Act.

[28] Mary A. Majumder et al., *Sharing data under the 21st Century Cures Act*, 19 Genetics in Medicine 1289–93 (Dec. 2017), https://www.nature.com/articles/gim201759.pdf?origin=ppub.

Through a 2009 Executive Order,[29] the federal government officially recognized that openness and transparency would strengthen and promote efficiency and effectiveness in government (the Open Government Data initiative). To meet this obligation, HHS leveraged its health care data reserves and established healthdata.gov, a website dedicated to making high value health data more accessible to entrepreneurs, researchers, and policy makers in the hopes of better health outcomes for all.[30] Agencies across HHS (including CMS, the Centers for Disease Control (CDC), and Food and Drug Administration (FDA)), and state agencies contributed thousands of datasets on a wide range of topics, including environmental health, medical devices, Medicare & Medicaid, social services, community health, mental health, substance abuse, and federally funded research. This "openness" was designed to create accountability, encourage public-private partnerships, build trust, and add to the proliferation of health data. HHS nicknamed this initiative "Liberating the Data."

The cost of health care during this time was increasing faster than ever, which pushed consumers to become savvier. Even consumers who thought they had "good" health care coverage began to feel the pinch of paying higher premiums and out-of-pocket expenses. Despite having more access to health information, the people who had the information weren't necessarily the ones who needed it; or, if they were the ones who needed it, they did not necessarily have it at the time it was needed. It became clear that obtaining the information necessary in the right form or format so that it could be used efficiently or effectively would drive improvements to the quality of health care, and may lower its cost. Though most agreed

[29] *See* Memorandum for the Heads of Executive Departments and Agencies, OMB M-10-06, Open Government Directive (Dec. 8, 2009), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

[30] *See generally 2016 HHS Open Government Plan*, Immediate Office of the Secretary, https://www.hhs.gov/open/2016-plan/index.html (last reviewed Sept. 30, 2016).

with this principal, barriers prevented stakeholders, including patients, providers, and insurers from achieving this aim.

It became apparent that interoperability was not going to be an organic outgrowth from the adoptions of technology or the marketplace. It would take a mandate before health care stakeholders would give up their reluctance to share the health information that belonged to the patients they were responsible to treat and insure. The Cures Act took a no-nonsense and transformative approach to breaking down these barriers, achieve interoperability[31] and eliminate information blocking.

The Cures Act and the Interoperability Rules promulgated thereunder by the Office of the National Coordinator for Health Information Technology (ONC)[32] and CMS,[33] mandate that certified health information technology (IT) technologies must be interoperable and push subject entities to implement standards-based application programming interfaces (Open APIs). The Act also prohibits: (1) interference with access, use, and exchange of electronic health information; (2) restrictions on communications about the usability, interoperability, and user experience with an EHR; and (3) the practice that has become known as "Information Blocking" by certain actors.[34]

---

[31] The term "interoperability, with respect to health information technology, means such health information technology that (A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; (B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (C) does not constitute information blocking as defined in section 3022(a)." *See* 21st Century Cures Act § 4003(10).

[32] 45 C.F.R. Part 171.

[33] 45 C.F.R. Part 156.

[34] The term "information blocking" generally means a practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. *See Information Blocking*, Health IT (Jan. 5, 2021), https://www.healthit.gov/topic/information-blocking.

The ONC Interoperability and Information Blocking rules apply to health care providers, developers of certified health IT and health information exchanges and networks (each an "Actor" and collectively "Actors"). For the first time, health care providers (e.g., hospitals, health centers, physicians, therapists, and others) will be directly regulated by the ONC. And, while health plans are not per se considered Actors under the ONC Interoperability Rules, they may find themselves as such under the definition of health information exchange or network.[35]

Commentary to the proposed rules demonstrated that stakeholders wanted to avoid the burden of additional regulation. Many questions were posed to the agencies seeking clarification as to how the rules may not apply to certain Actors, or how an Actor could avoid having to comply. Once again, the industry appears to be taking a siloed approach to compliance rather than seeing the opportunities that a more fluid information sharing environment may unleash.

However, it remains to be seen whether the enforcement mechanisms of these rules will be sufficient to overcome these obstacles. The Information Blocking Rule carries stiff penalties.

4.2.2.1 OIG Rule Summary—Enforcement Authority

The Cures Act authorizes the HHS Office of Inspector General (OIG) to enforce the CMS and ONC information blocking rules.[36] Accordingly, OIG is authorized to: (1) investigate claims of information

[35] A "health information network" or "health information exchange" means an individual or entity that determines, controls or has the discretion to administer any requirement, policy or agreement that permits, enables or requires the use of any technology or services for access, exchange or use of EHI: 1) among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and 2) that is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 C.F.R. § 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 C.F.R. parts 160 and 164 (§ 171.102).

[36] 45 C.F.R. Parts 171 and 156.

blocking[37] (broadly speaking, any practice that is "not reasonable and necessary" that may interfere with the use, access to, or exchange of EHI);[38] and (2) impose civil monetary penalties (CMPs) of up to $1 million per violation by Actors (health IT developers, health information networks, and health information exchanges).[39]

In April 2020, OIG published a Proposed Rule[40] clarifying how the agency would use its enforcement authority to address violations of the CMS and ONC information blocking rules.[41] The Proposed Rule defines a "violation" as each practice that constitutes information blocking, and incorporates the ONC Final Rule's definitions of "practice" and "information blocking."[42] OIG also provided hypothetical and non-exhaustive examples to illustrate conduct that would constitute a single violation[43] or multiple

[37] "Information Blocking" is defined as "a practice that—(A) except as required by law or specified by the Secretary pursuant to rulemaking . . ., is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and (B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or (ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." 42 U.S.C. § 300jj-52(a)(1).

[38] 21st Century Cures Act, Pub. L. No. 114-255 (Dec. 13, 2016), https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.

[39] 45 C.F.R. § 171.102; *id.*

[40] *See* 85 Fed. Reg. 22979, *Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Monetary Penalty Rules*, Proposed Rule by the HHS (Apr. 24, 2020), https://www.federalregister.gov/documents/2020/04/24/2020-08451/grants-contracts-and-other-agreements-fraud-and-abuse-information-blocking-office-of-inspector.

[41] 45 C.F.R. Parts 171 and 156.

[42] 45 C.F.R. § 171.102.

[43] The following examples in the Proposed Rule would constitute a single violation:

> "A health care provider notifies its health IT developer of its intent to switch to another electronic health record (EHR) system and requests a complete electronic export of its patients' electronic health information

violations.[44] As is typical, the OIG emphasized that the final determination of the constitution of a violation would depend on the facts and circumstances of each allegation of information blocking. Importantly, the OIG emphasized in the Proposed Rule that it would not bring enforcement actions for "innocent mistakes."[45]

(EHI) via the capability certified to in 45 CFR § 170.315(b)(10). The developer refuses to export any EHI without charging a fee. The refusal to export EHI without charging this fee would constitute a single violation."

"A health IT developer (D1) connects to a health IT developer of certified health IT (D2) using a certified API. D2 decides to disable D1's ability to exchange information using the certified API. D1 requests EHI through the API for one patient of a health care provider for treatment. As a result of D2 disabling D1's access to the API, D1 receives an automated denial of the request. This would be considered a single violation."

[44] The following examples in the Proposed Rule would constitute multiple violations:

"A health IT developer's software license agreement with one customer prohibits the customer from disclosing to its IT contractors certain technical interoperability information (i.e., interoperability elements), without which the customer and the IT contractors cannot access and convert EHI for use in other applications. The health IT developer also chooses to perform maintenance on the health IT that it licenses to the customer at the most inopportune times because the customer has indicated its intention to switch its health IT to that of the developer's competitor. For this specific circumstance, one violation would be the contractual prohibition on disclosure of certain technical interoperability information and the second violation would be performing maintenance on the health IT in a discriminatory fashion. Each violation would be subject to a separate penalty."

"A health IT developer requires vetting of third-party applications before the applications can access the health IT developer's product. The health IT developer denies applications based on the functionality of the application. There are multiple violations based on each instance the health IT developer vets a third-party application because each practice is separate and based on the specific functionality of each application. Each of the violations in this specific scenario would be subject to a penalty."

[45] 85 Fed. Reg. 22979, at 22984.

OIG's anticipated approach to enforcement stresses conduct that: (1) was performed with actual knowledge; (2) resulted in, is causing, or has the potential to cause patient harm; (3) significantly impacted a provider's ability to care for his/her patients; (4) was of significant duration; or (5) caused the federal health care programs or other government or private entities financial loss.

Actors should take heed that, where OIG does not pursue enforcement, they may become subject to the oversight of another agency. OIG noted that it would refer information blocking claims to OCR if consultation regarding HIPAA regulations would resolve[46] an information blocking claim; and, that it would closely coordinate[47] with ONC.

Health care providers that do not meet the definition of Actor are not subject to the $1 million per violation CMPs. Instead, the Cures Act authorizes OIG to determine when a health care provider commits information blocking and obligates OIG to refer the provider to the applicable agency for the appropriate disincentive.[48] This means that health care providers participating in the Medicare Quality Payment Program or Medicare and Medicaid Promoting Interoperability Program may see lower performance scores and payment adjustments under those programs if they engage in practices determined to be information blocking. Further, other authorities could serve as a basis for the sanction of health care providers. For example, some conduct that constitutes information blocking by Actors could potentially be punishable as a violation of a patient's right of access under HIPAA and HITECH.

As anticipated, numerous comments were submitted in response to the Proposed Rule. Almost all comments noted the impact of COVID-19 on entities and individuals and requested additional time

---

[46] *Id.* at 22981.

[47] *Id.* at 22984.

[48] 42 U.S.C. § 300jj-52(b)(2)(B).

before OIG imposes sanctions. As previously mentioned, numerous commenters sought clarification to limit their exposure to CMPs.

Specifically, hospital commenters requested a limitation to the imposition of CMPs to an overall "practice" of information blocking as opposed to individual transactions. They also sought clarity on the circumstances under which providers may be treated as health information networks or health information exchanges, which would categorize them as subject to OIG enforcement.

EHR vendors and app developers offered suggestions as to mitigating factors that OIG could consider in determining CMP amounts, including self-disclosure and effective compliance plans. One EHR vendor commenter specifically requested clarification as to how OIG would address unintentional information blocking that is hard to uncover and suggested lack of knowledge as a mitigating factor.

Payer commenters recommended that OIG consider a stepwise approach to CMP determinations, allowing Actors the opportunity to correct innocent mistakes that lack the requisite intent for a violation via an official warning and issuance of a corrective action plan.

Most commenters also promoted the promulgation of safe harbors, and many stressed the importance of OIG's coordination with other agencies and issuance of clear subregulatory guidance to enable individuals and entities to comply with federal and state laws.

The comment period for the Proposed Rule ended on June 23, 2020.

Although OIG is currently authorized to impose CMPs under the Cures Act, the timing of enforcement remains unclear until the agency issues its Final Rule on how it will enforce the information blocking provisions. The Agency stated in the Proposed Rule, however, that it will not begin enforcement until 60 days after the

Proposed Rule is finalized to provide "individuals and entities with time to come into compliance with the ONC Final Rule."[49]

We recommend at this time that affected parties familiarize themselves with OIG's proposed enforcement priorities and consider how to establish compliance policies to comport with the new ONC and CMS final rules. In the interim, the Federal Trade Commission (FTC) has enforcement authority for misuses of consumer data by any organization.

4.2.3 Privacy Gaps—Unregulated Consumer Health Data

4.2.3.1 Federal Trade Commission Role

The FTC is the primary federal agency overseeing privacy policy and enforcement. Its authority to do so began in the 1970s, when it was authorized to enforce one of the first federal privacy laws—the Fair Credit Reporting Act.[50] Since then, advancements in technology have brought new privacy challenges, but the FTC states that its overall approach has been consistent.[51] The FTC aims to "protect consumers' personal information; and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace."[52] When companies convey to consumers that they will safeguard personal information, the FTC can, and does, take enforcement action to ensure that such promises are kept.

---

[49] 85 Fed. Reg. 22979, at 22985.

[50] The Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970).

[51] *See FTC Privacy & Data Security Update: 2019*, FTC (Jan-Dec. 2019), at 2, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[52] *Id*.

Since its inception, the FTC has brought hundreds of actions against companies for violations of consumers' privacy rights.[53] In many of these cases, the FTC has charged defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce.[54] The FTC may challenge such "unfair or deceptive act[s] or practice[s]," "unfair methods of competition," or violations of other laws in the FTC Act by instituting an administrative adjudication.[55]

Stated plainly, Section 5 of the FTCA authorizes the FTC to issue cease-and-desist orders to enjoin unfair or deceptive acts or practices, or to settle charges in a consent order.[56] If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations.[57] Section 13(b) of the FTC Act also authorizes the FTC to seek preliminary or permanent injunctive relief in federal district court.[58]

FTC has brought more than 70 privacy and data security cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data since 2002.[59] To resolve these allegations, the FTC has required defendants to implement comprehensive privacy and security programs,[60]

---

[53] *See generally,* Federal Trade Commission Cases & Proceedings, https://www.ftc.gov/enforcement/cases-proceedings (last accessed Feb. 10, 2021).

[54] 15 U.S.C. § 45(a)(1).

[55] *See generally,* Section 5(b) of the FTC Act, 15 U.S.C. 41, *et seq.*

[56] 15 U.S.C. § 45(b).

[57] *See* 86 Fed. Reg. 2539, Adjustments to Civil Penalty Amounts, A Rule by the FTC (Jan. 13, 2021), https://www.federalregister.gov/documents/2021/01/13/2021-00483/adjustments-to-civil-penalty-amounts.

[58] 15 U.S.C. § 53(b).

[59] *See FTC Privacy & Data Security Update: 2019*, FTC (Jan-Dec. 2019), at 2, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[60] *See* Federal Trade Commission Civil Action against Equifax, Inc. Case Number 1:19-cv-03297-TWT (July 31, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

undergo assessments by independent experts,[61] and pay monetary fines.

Recently, the FTC has demonstrated increasing interest in enforcing claims against companies that misrepresent uses and protections for consumer health data. In January 2021, the FTC settled allegations that a company shared consumer health information of its users with third-party data analytics providers after promising that such information would be kept private.[62] As part of that settlement, the FTC required deletion of data the company improperly shared with third parties; obtaining users' affirmative express consent before sharing their health information with third parties; reporting to the FTC future unauthorized disclosures; obtaining an outside assessment of its privacy practices; and providing a notice to its customers.[63] In the FTC's press release announcing the settlement, Andrew Smith, Director of the FTC's Bureau of Consumer Protection, stated, "[the FTC is] looking closely at whether developers of health apps are keeping their promises and handling sensitive health information responsibly. This enforcement action may serve as a strong signal of similar enforcement action moving forward.

Companies utilizing and storing health information should also heed FTC's Breach Notification Rule[64] which requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information. The Health Breach Notification Rule requires certain businesses not covered by

[61] *See FTC Brings First Case Against Developers of "Stalking" Apps*, FTC (Oct. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps.

[62] *See* In the Matter of Flo Health, Inc. (January 31, 2021) File Number 1923133, https://www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc.

[63] *Id*.

[64] 16 C.F.R. Part 318.

HIPAA to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information.[65]

The FTC has testified before Congress numerous times on privacy and data security issues.[66] To better equip the agency to meet its statutory mission, the FTC has called upon Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The role the FTC will play in a future privacy law remains unknown.

4.2.3.2 State Law Developments

In the absence of a comprehensive federal law that regulates the protection of personal information, there has been a surge in states enacting data privacy and security laws.[67] Many of the state-level regulations have overlapping or incompatible provisions. For example, all 50 U.S. states have adopted data breach notification laws. Yet, most state laws have different definitions for personal data and breach; divergent breach triggers and notification timelines; and unique reporting requirements.[68] The same holds true with state

[65] *See generally*, *Complying with the FTC's Health Breach Notification Rule*, FTC (Apr. 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[66] *See* Chairman Joseph J. Simons, *Prepared Statements of the Federal Trade Commission: Protecting Consumers and Fostering Competition in the 21st Century*, (Sept. 25, 2019), https://www.ftc.gov/public-statements/2019/09/prepared-statement-federal-trade-commission-protecting-consumers-fostering; Andrew Smith, *Prepared Statement of the Federal Trade Commission Before the Subcommittee on Economic and Consumer Policy of the Oversight and Reform Committee, United States House of Representatives*, (March 26, 2019), https://www.ftc.gov/public-statements/2019/03/prepared-statement-federal-trade-commission-subcommittee-economic-consumer; *see also, Prepared Remarks of Chairman Joseph J. Simons Before the Senate Appropriations Subcommittee on Financial Services and General Government*, (May 7, 2019), https://www.ftc.gov/public-statements/2019/05/prepared-remarks-chairman-joseph-j-simons-senate-appropriations.

[67] We note that certain entities and data handling scenarios may also implicate international data protections laws, such as the E.U. General Data Protection Regulation, but this chapter does not discuss any particular international laws.

[68] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research

data privacy laws. Multiple states enacted legislation to protect consumers; but many state laws have different access, consent, and notice requirements, while others have granted individuals the right to "be forgotten" or to have their data erased.[69] Some state legislatures are considering whether to grant a private right of action for consumers to bring a lawsuit against a business that violates an individual's privacy interests.

The state data privacy law that has gotten the most attention is the California Consumer Protection Act of 2018 (CCPA).[70] The CCPA includes five specific data privacy rights that California residents enjoy. The law also obligates companies doing business in California to protect those rights and grants the California Attorney General broad authority to implement related regulations designed to protect those rights. Specifically, the CCPA enumerates that California consumers have the right to: (1) know what consumer personal information is collected; (2) know whether the personal information is sold or disclosed, and to whom such information is sold or disclosed; (3) say no to the sale of personal information; (4) access personal information; and (5) equal service and price, even if privacy rights are invoked.

The CCPA does not apply to government agencies, nonprofit businesses, or businesses that have annual revenue of less than $25 million, or those that receive, buy, or sell personal information of fewer than 500,000 individuals, or derive less than half their annual revenue from the sale of personal information. The CCPA also does not apply to: (1) medical information governed by the California Confidentiality of Medical information Act; (2) PHI collected by

Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[69] *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, International Associate of Privacy Professional Tracker, https://iapp.org/resources/article/state-comparison-table/ (last updated Feb. 4, 2021).

[70] *See* CAL. CIV. CODE § 1798.100 (2018).

entities covered by the HIPAA privacy rule; and (3) entities covered by other federal and California sector specific data protection laws (including the Gramm-Leach-Bliley Act,[71] the Driver's Privacy Protection Act,[72] and the California Financial Information Act[73]).

Even before CCPA regulations had a chance to take effect, privacy advocates initiated a push for stronger protections. On November 3, 2020, California voters approved Proposition 24,[74] also known as the California Privacy Rights Act (CPRA),[75] effective January 1, 2023, and applicable to companies serving more than 100,000 California residents. The CPRA codifies the nation's strongest privacy protections.

Under the CPRA, companies must: (1) destroy data when personal information is no longer needed and (2) ensure that any third parties with whom they share personal consumer information comply with the CPRA. Additionally, CPRA permits California consumers to opt-out of having their data shared and consumers may force companies to correct inaccurate information. Furthermore, the CPRA creates a very broad private right of action for consumers to bring lawsuits against companies for a breach of personal information. This private right of action includes the right to sue for damages, *without a showing of harm*, with potential triple damages for the breach of personal information of minors under the age of 16.

---

[71] Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[72] 18 U.S.C. § 2721 (1994).

[73] Ca. Fin. Code § 4050 (2004).

[74] California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020) was on the ballot on November 3, 2020 and was approved by California voters. *See* Cameron F. Kerry & Caitlin Chin, *By passing Proposition 24, California voters up the ante on federal privacy law*, Brookings (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/.

[75] The CPRA amends the CCPA and will become effective on January 1, 2023. The CPRA's full text is available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf (last accessed Feb. 11, 2021).

Most striking, the CPRA mandates the creation of a state consumer privacy agency, which takes responsibility for enforcing privacy law violations away from the state's attorney general.

While California focused on consumer rights and privacy protections, New York's data protection laws focused on companies that fail to take the appropriate precautions to protect personal and sensitive data against hacks and cybercrimes. On July 25, 2019, New York's Governor, Andrew Cuomo, signed the Stop Hacks and Improve Electronic Data Security Act (NY SHIELD Act).[76] The NY SHIELD Act expanded state data breach law and imposed affirmative obligations on certain companies to improve cybersecurity. The NY SHIELD Act also requires certain companies to implement a cybersecurity program and develop an incident response program designed to detect and prevent unauthorized access and to respond to intrusions.

In contrast, Illinois focuses on biometric identifiers. The Biometric Information Privacy Act (BIPA)[77] requires that, prior to collecting biometric information (including fingerprints, retina scans, and facial geometry scans), a business must obtain written consent from individuals and provide appropriate disclosure of the policies for use and retention of the biometric identifiers. Although Illinois was the first state to pass a law that specifically regulates the collection of biometric data, other states are also considering the issue.

As the proliferation of data continues to grow in parallel with the multiplication of the patchwork of state privacy and security laws, it may become more complicated and difficult for companies to navigate the web of regulation and litigation risks.

---

[76] *See* N.Y. GEN. BUS. § 899-bb (2019), https://legislation.nysenate.gov/pdf/bills/2019/S5575B.

[77] *See* 740 ILL. COMP. STAT. 14/1 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

4.3.3.3 Federal Legislation

Federal legislation could streamline the convoluted patchwork by creating a federal standard to which all entities that handle personal information in the United States must consistently adhere, and upon which all Americans could rely.

In recent years, consensus for such legislation has gained momentum. Republicans and Democrats have each issued their unique proposals. In late 2020, the U.S. Senate Committee on Commerce, Science, and Transportation held a hearing entitled, "Revisiting the Need for Federal Data Privacy Legislation" to discuss frontrunners.[78]

Most proposals that were discussed: (1) recognize an individuals' right to control his/her personal information; (2) require a defined class to respect this right; and (3) establish enforcement processes.[79] However, the proposals differ in terms of: (1) whether states' existing privacy laws would be preempted by such a federal law; (2) what rights consumers might have to individually sue for privacy harms; and (3) which federal agency would enforce such a law.[80] Lawmakers have settled on opposite sides of the aisle on these issues.

By way of illustration, in 2019, Democratic senators introduced the Consumer Online Privacy Rights Act (COPRA).[81] The next year, Republican senators introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE

[78] *See Revisiting the Need for Federal Data Privacy Legislation*, U.S. Committee on Commerce, Science, & Transportation (Sept. 23, 2020), https://www.commerce.senate.gov/2020/9/revisiting-the-need-for-federal-data-privacy-legislation.

[79] *See Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, Congressional Research Services (Apr. 3, 2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10441.

[80] *Id*.

[81] The Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (1st Sess., 2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968.

DATA) Act.[82] As proposed, COPRA's federal privacy legislation would create a federal "floor," and would allow states to enact stricter privacy standards if they elect to do so. This would allow states, like California, to operate under their existing state laws, and would require companies to continue to navigate the patchwork of various state laws that go above and beyond the federal "floor." In contrast, the proposed SAFE DATA Act would broadly preempt state privacy laws. Additionally, unlike the SAFE DATA Act, which contains no provision for a private right of action, COPRA provides a private right of action for individuals to assert violations, with damages from $100 to $1,000 per violation per day.

These examples are merely just a reference point as federal legislative priorities and proposals frequently change year over year. Nevertheless, one constant theme emerges. In the vacuum of a federal privacy law or consistent state laws, many private entities have taken to establish their own frameworks.

4.2.3.4 Efforts to Fill Gaps in Existing Privacy Regulation

As we move forward, it is clear that personal information continues to rapidly proliferate and permeate largely unregulated spaces, creating the risk of data misuse and substantial consumer harm. Recent surveys also indicate that the majority of Americans (four out of five) are concerned about how their data is collected and used.[83] These trends, coupled with an aging privacy regime in the United States, have triggered dialogue in both the public and private sectors.

---

[82] The Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, S. 4626 116th Cong. (2d Sess. 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4626/text.

[83] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

The private sector, driven by many entities not otherwise subject to HIPAA, has recently sought to fill existing gaps in privacy regulation by collectively establishing, and committing to, privacy standards. The majority of these gap-filling efforts focus on governing ethical collection, processing, and protection of consumer health information. These standards take various forms ranging from best practices to codes of conduct to self-regulatory privacy frameworks.

These standards have several commonalities and certain notable differences in terms of enforceability. By way of example, a few notable standards addressing consumer health information include the CARIN Code of Conduct,[84] American Medical Association Privacy Principles,[85] Consumer Technology Association (CTA) Guiding Principles for the Privacy of Personal Health and Wellness Information,[86] and the eHealth Initiative Consumer Privacy Framework.[87] In terms of commonalities, each of these standards are currently (1) voluntary in nature and (2) address key privacy dimensions including, but not limited to, transparency, consent, use and disclosure, access rights, protection, and accountability. By way of contrast, these standards vary in terms of the level of notice required, limitations on secondary use of data, and categories of data subject to more stringent requirements.

[84] *See* CARIN, *Trust Framework and Code of Conduct,* https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/ (last visited February 12, 2020).

[85] *See AMA Privacy Principles*, American Medical Association (2020), https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf.

[86] *See Guiding Principles for the Privacy of Personal Health and Wellness Information*, Consumer Technology Association (2019), https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf.

[87] *See Proposed Consumer Privacy Framework for Health Data*, eHealth Initiative Center for Democracy & Technology (Aug. 26, 2020), https://www.ehidc.org/sites/default/files/resources/files/COMBINED%20FRAMEWORK831.pdf.

Another key area of difference relates to enforceability. For example, the CARIN Code of Conduct has no official enforcement mechanism. By contrast, the eHealth Initiative Consumer Privacy Framework contemplates a certification program including possible enforcement mechanisms such as independent monitoring, complaint processes, dispute resolution through self-regulatory programs, loss of certification, as well as referral to state or federal consumer protection authorities. As this variability demonstrates, while these standards fill certain gaps, many do not sufficiently ensure consumer protection.

4.3 The Current Environment: Opportunities and Risks

In the absence of a comprehensive federal privacy law, significant risk remains to individuals whose information is already flowing well beyond regulated spaces and entities. Until the federal government crystallizes its efforts, it is likely that the FTC and states will continue to be more active on privacy issues as data moves from regulated spaces to currently unregulated spaces. This will add to the already complex patchwork of laws and regulations that organizations must navigate.

Meanwhile, the push for interoperability will continue, with federal agencies coordinated in their approach. Organizations should evaluate their compliance obligations under the new Interoperability Rules, and brace for changes in regulatory obligations. As there are steep penalties for violating the information blocking rules, it is critical that organizations adopt a defensible position, as well as embrace the opportunities that interoperability presents: the potential for innovation, improvements in quality of care, and enhancements in overall health.

The CMS Interoperability and Patient Right of Access Rules empower patients to actively participate in making healthy medical and lifestyle choices, and support reimbursement models that encourage providers to focus on patient outcomes and greater price

transparency. They will redefine how hospitals, critical access hospitals, and psychiatric hospitals that participate in CMS programs make patient information available and create opportunities to engage with patients in a whole new way. Hospitals will have to publish an Open API that supports individual patient and population-level export. This will allow application developers to create technologies that patients can download to request access to their PHI and share their PHI with third parties.

Further, health plans offering Medicare Advantage, Part D, Managed Medicaid and Children's Health Insurance Program (CHIP) plans, and Qualified Health Plans on the federally facilitated exchanges will have a place in the health information sharing circle like never before. Health plans will be required to make historic claims and encounter data available when an enrollee or former enrollee requests access to their electronic health information, or requests that it be exchanged or shared with a third party. Health plans will be required to publish Open APIs that support a patient's right to access their electronic health information, a Provider Directory API, and Payer-to-Payer exchange.

Collectively, opportunities abound to empower patients with improved access to their electronic health information. Interoperability will improve care coordination and encourage patient engagement and ultimately give patients the tools to make better and more cost-effective health care decisions.

4.4 What Health Lawyers Need to Know

Increasingly, consumers authorize computers, biosensors, mobile devices, wearables, and other technology to gather, store, and share vast amounts of health care data. As discussed in this chapter, the Cures Act fosters the portability of this data through the Interoperability Rules. The Cures Act also promotes the use of this data to drive innovation in clinical decision making, patient treatment, and clinical research.

As an example, the Cures Act authorizes FDA to evaluate the potential use of real world data and evidence to help support the approval of new indications for an approved drug, or satisfy post approval study requirements. As FDA states, "[t]his data holds potential to allow us to better design and conduct clinical trials and studies in the health care setting to answer questions previously thought infeasible."[88]

However, juxtapose the benefits that lie in the interoperability of this sensitive data against present day cybersecurity risks. One example is the federal government's "All of Us" program, one of the world's largest and most diverse data sets for precision medicine research. In 2016, the National Institutes of Health (NIH) launched the $130 million Precision Medicine Initiative cohort program, "All of Us," to build a dataset of more than one million participants' genetic, lifestyle, and health information for further study and use by NIH researchers, providers, and patients.

"All of Us" participants submit a plethora of data, including: answers to questionnaires and surveys; electronic health records; physical measurements and biospecimens; and even passive mobile and digital health data. Early in its launch, NIH proclaimed that it would, "[e]nsur[e] that participant data are securely maintained [as this] is paramount to retaining the participants' trust and participation in All of Us."[89]

However, in 2019, OIG concluded in an audit of two All of Us awardees that adequate controls were not in place to protect

[88] *See* FDA Guidance, *Real-World Evidence*, U.S. Food & Drug Administration (Nov. 30, 2020), https://www.fda.gov/science-research/science-and-research-special-topics/real-world-evidence.

[89] *See* Office of Inspector General, *The National Institutes of Health Could Improve Its Monitoring To Ensure That an Awardee of the All of Us Research Program Had Adequate Cybersecurity Controls To Protect Participants' Sensitive Data*, U.S. Department of Health & Human Services (June 10, 2019), https://oig.hhs.gov/oas/reports/region18/181709304.asp.

the participants' sensitive data.[90] Specifically, OIG identified 13 vulnerabilities (two classified as "high") that could have exposed All of Us participants' personally identifiable information and allowed unauthorized users to alter the participants' data. In its report, OIG stated that because of the nature of the vulnerabilities identified, an attacker with limited technical knowledge could exploit and compromise the systems.[91]

This example highlights what is most important for lawyers to know: that with its best intentions, the government was unable to sufficiently protect the sensitive health data it amassed. This cybersecurity challenge is not unique to the public sector as countless private sector entities struggle with adequate data protection and related breach issues. As consumers will likely continue to share their personal health data only to the extent that they can rely on strong privacy and security protections, it is increasingly important for both the public and private sectors continue to implement, evaluate, and strengthen privacy and security controls over time.

4.5 Practice Tips and Tools

The public and private sectors view increased data collection and sharing through interoperability as the road to innovation and improvements in the health care and life sciences industries. Some go as far as to argue that health care data should be viewed as a public utility to be used to propel the industry into a new age of data-driven progress. Yet, the rapid proliferation and sharing of data without adequate guardrails poses significant risks. As such, continuing on this path will require a keen focus on establishing and maintaining trust about good data stewardship among individuals,

[90] *See* Office of Inspector General, *The National Institutes of Health Could Improve Its Monitory to Ensure that an Awardee of the All of Us Research Program Had Adequate Cybersecurity Controls to Protect Participants' Sensitive Data*, U.S. Department of Health & Human Services (June 2019), https://oig.hhs.gov/oas/reports/region18/181709304.pdf.

[91] *See id*.

the private sector, and the public sector, as it flows throughout the industry.

There are several dimensions to the complexities associated with data collection, use, protection, and sharing in the health care ecosystem. First, it is critical to engage legal and compliance personnel early and often. Legal counsel can help identify what laws, regulations, and other standards apply to a particular organization and particular data handling scenarios. Legal counsel can also help identify salient risks associated with certain data handling activities. Compliance counsel can assist in determining how best to structure operational policies and programs to put an organization in a defensible posture relative to applicable laws.

Second, no matter what data handling scenario may arise, it is critical that privacy and good data stewardship remain prioritized throughout developing compliance programs and decision making around specific data handling issues. At the simplest level, it is critical for organizations to "say what you do, and then, do what you say." More granularly, key data governance policies and programmatic activities should address fair information best practices related to: (1) transparency; (2) limiting collection of data to specific purposes; (3) limiting use of data to such purposes; (4) ensuring adequate data protection, (5) individual rights; and (6) ensuring a person within the organization remains accountable for these compliance activities. Each organization and use case may require different policy and procedural controls; but, documenting, monitoring, and openly communicating about an organization's data stewardship commitments are critical to establishing trust and a defensible posture with respect to individuals, customers, partners, and governmental authorities.

Third, as data proliferates and interoperability increases, it is critical to develop a defensible posture relative to the individuals an organization serves, as well as to the regulators that are keenly focused on promoting transparency and data sharing. In the

immediate term, organizations ought to evaluate their positioning in the health care ecosystem to determine the impact of the new ONC and CMS interoperability rules on their enterprise. Specifically, legal counsel should be engaged to analyze which interoperability laws and regulations may apply to an organization. Once identified, a compliance program may be developed including enterprise-wide commitments, policies and procedures, compliant contracting strategies,[92] and cost-accounting mechanisms, among other activities.

Fourth, organizations will need to consider how best to technologically meet the new interoperability and data sharing requirements. Some organizations may seek to leverage existing technologies in new ways to share data. Others may seek to develop their own technologies in house. Still others may want to consider whether to obtain the necessary technology through partnering with third parties or otherwise licensing technology. In any case, these build, buy, or partner decisions should be addressed in the short term so that an organization is positioned to carry out its interoperability obligations when OIG enforcement becomes effective.

Fifth, organizations should also be reminded that the interoperability rules have reinvigorated enforcement of HIPAA relative to the individual right of access. This means organizations should revisit existing patient engagement and response policies and procedures related to carry out obligations under that rule in the context of the new push for interoperability. In particular, HIPAA-subject organizations should determine whether, and how best, to educate individuals about possible risks of sharing data with third parties that are not otherwise regulated by HIPAA. Organizations

[92] By way of illustration, entities should also consider the impact of upstream agreements and downstream agreements on rights to collect, use or disclosure data through the chain of custody. Agreements that warrant considering may include, *inter alia*: Master Services Agreements, Data Use Agreements, Business Associate Agreements, Data Sharing Agreements, and/or Confidentiality/Non-disclosure Agreements.

may also want to consider establishing policies and procedures to conduct third-party application vetting in ways that comport with the interoperability rules.

Finally, it is imperative that, no matter what data is collected, how it is used, or with whom it is shared, organizations can only maintain trust by placing an increased focus on data protection and cybersecurity. The benefits of data collection and use can quickly erode in the wake of a data breach resulting in significant financial and reputational damage. As such, organizations should make security central to their data strategy. However, this is not a one-and-done exercise; but, rather, a journey that involves a continuous improvement cycle that requires implementing, evaluating, and augmenting controls over time to strengthen cybersecurity posture and reduce risks as the threat landscape evolves.

Navigating the complex and ever-evolving landscape of laws, regulations, and risks associated with data proliferation and sharing can be daunting. Partnering with legal counsel, compliance personnel, and IT personnel is a key first step to developing a successful compliance strategy. Further, a plethora of resources exist to provide good guidance to inform aspects of compliance. These best practice guides are often issued by federal or state government authorities,[93] trade associations or professional societies,[94] as well as various experts in data, technology, privacy, cybersecurity, and

[93] *See*, *e.g.*, *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards & Technology (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; *Guide to Privacy and Security of Electronic Health Information*, ONC (Apr. 2015), http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

[94] *See*, *e.g.*, *Risky Business? Sharing Data with Entities Not Covered by HIPAA*, eHealth Initiative & Manatt (March 18, 2019), https://www.ehidc.org/sites/default/files/resources/files/Sharing%20Data%20with%20Non-HIPAA%20Entities%20March%202019.pdf; *see also IAPP White Papers*, International Associate of Privacy Professional, https://iapp.org/resources/topics/white-papers/ (last accessed Feb. 13, 2021).

interoperability.[95] A good place to start to familiarize yourself with these obligations would be ONC's website dedicated to interoperability.[96] Coalescing the right team members and leveraging the right guidance resources is critical to successfully seizing the opportunities presented by data proliferation and sharing, while also minimizing risks associated with the same.

[95] *See*, *e.g.*, *The Ten Most Critical Web Application Security Risks*, Open Web Application Security Project (2017), https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf.

[96] *See generally*, *Interoperability*, Health IT (May 9, 2019), https://www.healthit.gov/topic/interoperability.