2021

One Small Step for Interoperability, One Giant Leap for Patients' Rights

Emma Lombard

One Small Step for Interoperability, One Giant Leap for Patients' Rights

Emma Lombard*

I. Introduction

In the digital age, the rise of technology means many things to many people. For lawyers, it means that legal research can be done entirely online, without ever entering a library or picking up a Reporter.[1] For doctors, it means that they can make house calls, without ever leaving their office.[2] The list goes on. Most importantly, for many people, it means that they can communicate with just about anyone, anywhere in the world, instantaneously. Along with the plethora of benefits that advances in technology bring, there is the accompanying risk of misuse. Because "the amount of data created and collected is exponentially rising," the average data breach now affects more people than ever before.[3] While data breaches have occurred for as long as individuals and companies have maintained records and stored private information, they have increased significantly in number and magnitude as more companies and individuals rely on computers for communication, record-keeping, and administrative uses.[4] A data breach is best defined as "an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so."[5] Breaches in the administration of healthcare have become increasingly prevalent—the origins of which are complex to trace.

---

*J.D. Candidate, 2021, Seton Hall University School of Law; B.A., 2017, University of California Santa Barbara.

[1] Rachel Buchanan, *The Role of Technology in the Future of Legal Professions*, OXFORD UNIVERSITY RESEARCH COLLECTION: LAW AND TECHNOLOGY (Feb. 27, 2017), https://www.law.ox.ac.uk/research-and-subject-groups/research-collection-law-and-technology/blog/2017/02/role-technology.

[2] Mei Wa Kwong, *Telehealth and Public Programs - Evolution of Telehealth Policy in Medicare and Medicaid*, 15 J. HEALTH & BIOMED. L. 7, 8 (2019).

[3] Danielle Abril, *Data Breaches Declined Last Year. But Here's Why You Should Be More Worried Than Ever*, FORTUNE (Jan. 29, 2019), https://fortune.com/2019/01/29/data-breaches-decline-2018-consumer-data-risk-rises/.

[4] Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN: DATA INSIDER (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches.

[5] *Id.* (including among the most common types of breached data: "payment card information (PCI), personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property.").

Healthcare data breaches, in particular, are on the rise.[6] Over the past seven years, the annual number of health data breaches has risen by seventy percent—with seventy-five percent of those breached, lost, or stolen records resulting from "hacking or IT incident."[7] This "nebulous category created by the government" does not distinguish between malicious data theft (such as phishing attempts and ransomware) and accidental loss (such as sending to an unintended recipient).[8] Unlike other data breaches, healthcare data breaches involve what is known as "protected health information" (PHI).[9] PHI is any personally "identifiable health information that is used, maintained, stored, or transmitted by . . . [a] healthcare provider, health plan or insurer, or a healthcare clearinghouse – or a business associate" of one of those entities.[10] It includes past, current, and future health information related to the administration of care or payment for care, regardless of the form in which it is kept.[11] Importantly, this includes both physical and electronic records, as well as spoken information.[12] "Essentially all health information is considered PHI when it includes individual identifiers," such as patient names, Social Security numbers, driver's license numbers, birth dates, telephone numbers, or e-mail addresses.[13]

In recent years, more healthcare providers have begun implementing Electronic Health Records (EHR) into their practices—and in doing so, patients have received many benefits.[14] By making health records available to patients in a digital format, patients can more easily access the

---

[6] Helen R. Pfister and Randi Seigel, MASSIVE DATA BREACH UNDERSCORES IMPORTANCE OF BUSINESS ASSOCIATE SECURITY, 5–7 Pratt's Privacy and Cybersecurity Law Report 05 (2019).
[7] *Id.*
[8] Michela Tindera, *Government Data Says Millions of Health Records Are Breached Every Year*, FORBES: MONEY & POLITICS (Sept. 25, 2018, 11:30 AM), https://www.forbes.com/sites/michelatindera/2018/09/25/government-data-says-millions-of-health-records-are-breached-every-year/#51a8b93416e6.
[9] HIPAA Journal, https://www.hipaajournal.com/considered-phi-hipaa/ (last visited Oct. 10, 2019).
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.* While there are mechanisms by which the access of electronic records can be recorded, it is worth noting that other such breaches are much more difficult to track.
[14] Sara Heath, *How Patient Health Data Access Drives Patient Engagement*, PATIENT ENGAGEMENT HIT (June 3, 2016), https://patientengagementhit.com/features/how-patient-health-data-access-drives-patient-engagement.

information, the information can be updated more quickly, and patients can be in charge of taking the necessary steps to safeguard their own health.[15] Not only can they track their visits, but they can view test results and cross-reference the information uploaded by their doctors. Studies have similarly shown that when patients are engaged in other ways, such as being able to schedule and confirm appointments electronically or through text message, they are more responsive and less likely to no-show to an appointment.[16] In response to these kinds of integration efforts by providers, there has been a push to develop other methods of health information technology.[17] Online portals and other new technologies have proven increasingly effective at getting patients more involved in their care, leading to better outcomes.[18] While patients typically wait to hear from doctors until they are able to call them to deliver test results or until they have an appointment to see the doctor next, this method of making data available online allows patients to access their health information in real-time—rather than being at the mercy of a doctor's hectic schedule.

Despite the obvious ways in which technology has advanced and become integrated into the administration of healthcare, the legal safeguards for cybersecurity matters have not progressed as rapidly. The first federal law created to address mounting concerns was the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[19] HIPAA is commonly known as the Privacy Rule, which requires, among other things, that those in possession of patient data take measures to

[15] HEALTHIT.GOV https://www.healthit.gov/faq/what-are-advantages-electronic-health-records (last updated May 16, 2019).
[16] Sara Heath, *How Text Message Communication Improves Patient Outreach*, (Oct. 15, 2018), https://patientengagementhit.com/news/how-text-message-communication-improves-patient-outreach (this is particularly as it pertains to text-message reminders for patients and more modern forms of technology rather than calling patients).
[17] Sara Heath, *How Patient-Centered Care Is Shaping Provider Health IT Strategy*, (Sept. 9, 2019), https://patientengagementhit.com/news/how-patient-centered-care-is-shaping-provider-health-it-strategy.
[18] Sara Heath, *6 Patient Engagement Technologies that Improve Clinic Operations*, (Aug. 22, 2019), https://patientengagementhit.com/news/6-patient-engagement-technologies-that-improve-clinic-operations.
[19] Johnathan D. Bick, *Cybersecurity: A Combination of Legal, Business and Technical Measures*, NEW JERSEY L. J. (Oct. 28, 2019).

protect it from accidental exposure or malicious theft.[20] If a patient's information is compromised or exposed during a data breach, that individual has certain rights and remedies.[21] While there is no private right of action under HIPAA, which would allow an individual patient to sue an entity, a patient may report the violation to the Secretary of Health and Human Services, who can then bring an enforcement action.[22] HIPAA does not preempt state laws that give rise to a private cause of action, and many courts hold that failure to comply with HIPAA serves as evidence that a physician failed to act reasonably, thus deviating from the standard of care.[23] In addition, a covered entity that is aware of a breach has a duty to inform patients that the security of their health information has been compromised.[24]

Following this trend toward electronically stored information and in furtherance of the goal to improve patient access and engagement, the Center for Medicare and Medicaid Services (CMS) proposed and recently passed an interoperability rule.[25] Interoperability has many technical definitions but put most simply, it "is the ability of two or more systems to exchange information and to interpret and use that information."[26] The purpose of the rule is "to move the health care ecosystem in the direction of interoperability," and to signal CMS' commitment to improving access to, and the quality of, healthcare information.[27] The Final Rule seeks to prioritize the availability of the information necessary for patients to make informed health care decisions. Ideally, the rule does so without increasing the burden on health care providers and payers.[28] In

[20] *Id.*
[21] *Id.*
[22] 42 U.S.C.S. § 300gg-22 (LexisNexis, Lexis Advance through Public Law 116–65, approved October 9, 2019).
[23] *Id.*
[24] 42 U.S.C.S. § 17932 (LexisNexis, Lexis Advance through Public Law 116–65, approved October 9, 2019).
[25] 84 Fed. Reg. 7610, (March 4, 2019) (https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02200.pdf).
[26] HIMSS, https://www.himss.org/library/interoperability-standards/what-is-interoperability (last visited Oct. 12, 2019).
[27] *Id.* This includes both medical records from providers and claim information from insurers.
[28] *Id.*

application, the interoperability rule purports to give patients access to their health information by requiring providers and insurers to compile that information into one EHR, made available through an application programming interface (API).[29] An API is a system by which "third party software applications connect to make the data available to patients."[30] The "open API"[31] would include both medical information (such as test results and diagnoses) as well as healthcare plan information (such as a provider directory and claims data).[32] While all of this information is certainly available to patients through various platforms, the task of collecting this data "can be burdensome and frustrating to the consumer."[33]

Although the final rule's framework under CMS' rule for increasing patient access to EHRs serves a worthwhile and meaningful purpose, its implementation is more complicated, if not entirely undermined by stringent state privacy laws. This Comment proposes that in order for this interoperability rule to succeed at increasing patient access to health data without putting patients at an increased risk of data breaches, Congress should amend the definition of "covered entities" to include the third-party applications that will collect and maintain the patient health data. Additionally, in the absence of the implementation of a Federal Privacy statute, Congress should create a private right of action under HIPAA to ensure that patients who do suffer adverse effects from a data breach are not without recourse. Section II of this Comment addresses past efforts to promote interoperability and the ways in which such efforts have progressed toward, but ultimately fell short of, the ultimate goal of interoperability. Section III of this Comment discusses the current efforts and strategy on which the rule relies. Section IV addresses the benefits of interoperability,

[29] 84 Fed. Reg. 7610, 7612, 7627.
[30] 84 Fed. Reg. 7610, 7612.
[31] 84 Fed. Reg. 7617.
[32] 84 Fed. Reg. 7619.
[33] *Id.*

while Section V discusses the barriers (both potential and actual) impeding the rule's implementation. Section VI adds other considerations which may complicate compliance with the rule, and Section VII concludes with proposed solutions to the problems that will arise. This Comment will not address the cybersecurity issues posed by implementation but will instead focus on the practical problems posed by attempts at compliance with both state laws and the CMS rule given that no federal privacy law exists. Rather than advocating for a federal privacy law, the proposed solutions focus on ways to amend HIPAA.

II. Past Efforts to Promote Interoperability

This rule is not the first effort by CMS and Congress to achieve interoperability, but it is the most recent effort to achieve it on a widespread scale. While it is certainly a revolutionary measure, this newfound emphasis is also a long time coming. CMS and Congress have worked toward a rule such as this by passing acts that play a key role in incentivizing providers to integrate technology into their practices.

In 2009, Congress implemented the Health Information Technology for Economic and Clinical Health Act (HITECH),[34] which provided an opportunity to move interoperability forward by "authorizing CMS to make incentive payments to eligible professionals, eligible hospitals and critical access hospitals, and Medicare Advantage (MA) organizations to promote the adoption and meaningful use of certified electronic health record technology (CEHRT)."[35] It also codified the Office of the National Coordinator for Health Information Technology (ONC).[36] This codification is significant because it bestowed regulatory authority upon the newly created agency and allowed it to enforce these measures in a way that had not previously occurred. This was a

[34] 42 U.S.C.S. § 17932 (LexisNexis, Lexis Advance through Public Law 116–65, approved October 9, 2019).
[35] 84 Fed. Reg. 7610, 7612.
[36] 42 U.S.C.S. § 17932 (LexisNexis, Lexis Advance through Public Law 116–65, approved October 9, 2019).

crucial move toward the integration of interoperability because it allowed CMS to incentivize providers to join in the efforts while offering its own guidance and standards. It involved three stages of implementation, allowing providers to integrate technology at a gradual pace. Stage 1 created a foundation for the EHR Incentive Programs by enacting requirements for capturing clinical data electronically, which included the requirement to provide patients with electronic copies of health information.[37] Stage 2 focused on advancing clinical processes and "ensuring that the meaningful use of EHRs supported the aims and priorities of the National Quality Strategy."[38] Stage 2 criteria encouraged the use of CEHRT for continuous quality improvement at the point of care and the exchange of information in the most structured format possible."[39] "Stage 3 focuses on using CEHRT to improve health outcomes."[40]

The federal government has spent over $35 billion under these EHR Incentive Programs, and while seventy-eight percent of physicians[41] and ninety-eight percent of hospitals[42] now use a certified EHR system, there has been very limited progress toward the implementation of an API, or a method to share system-wide data.[43] Because these incentivization programs were only partially successful, more changes were necessary. In 2010, ONC established a set of initial standards for the temporary certification program.[44] In 2011, the ONC changed those standards to create a Permanent Certification Program, showing the continued commitment of the government

[37] 84 Fed. Reg. 7610, 7612.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] ONC, HEALTH IT DASHBOARD, *Office-Based Physician Health IT Adoption: State Rates of Physician EHR Adoption, Health Information Exchange & Interoperability, and Patient Engagement*, https://dashboard.healthit.gov/apps/physician-health-it-adoption.php (last visited November 2, 2019).
[42] ONC, HEALTH IT DASHBOARD, *Non-Federal Acute Care Hospital Health IT Adoption and Use: State Rates of Non-Federal Acute Care Hospital EHR Adoption, Health Information Exchange and Interoperability, and Patient Engagement*, https://dashboard.healthit.gov/apps/hospital-health-it-adoption.php (last visited November 2, 2019).
[43] 84 Fed. Reg. 7610, 7612.
[44] *Id.*

to prioritize interoperability in a meaningful and practical way.[45] Given the amount of money that the federal government has spent promoting interoperability and giving providers an opportunity to pursue it themselves, it makes sense that the rule codifies and mandates these practices.

Congress enacted another important piece of legislature, the Medicare Access and CHIP Reauthorization Act (MACRA),[46] in April of 2015.[47] The stated aim of MACRA was to "achieve widespread exchange of health information through interoperable CEHRT nationwide."[48] The Act defines interoperability as "the ability of two or more health information systems or components to exchange clinical and other information and to use the information that has been exchanged using common standards as to provide access to longitudinal information to facilitate coordinated care and improved patient outcomes."[49] Congress declared, in MACRA, that it was a national objective to achieve widespread exchange of health information through interoperable certified EHR technology nationwide by December 31, 2018.[50] Based on the response to MACRA, ONC identified two metrics for measuring interoperability.[51] The first measure is the proportion of health care providers who electronically engage in "sending, receiving, finding, and integrating information received from outside sources" as opposed to those which are not.[52] The second measure is "the proportion of health care providers who report using the information they electronically receive from outside providers and sources for clinical decision-making."[53] ONC

---

[45] 45 CFR part 170.
[46] 114 P.L. 10, 129 Stat. 87, 2015 Enacted H.R. 2, 114 Enacted H.R. 2, 114 P.L. 10, 129 Stat. 87, 2015 Enacted H.R. 2, 114 Enacted H.R. 2. (CHIP refers to Children's Insurance Plan).
[47] *Id.*
[48] 84 Fed. Reg. 7610, 7613.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] ONC, HEALTHIT.GOV https://www.healthit.gov/sites/default/files/fulfilling_section_106b1c_of_the_medicare_access_and_chip_reauthorization_act_of_2015_06.30.16.pdf (last visited Oct. 25, 2019) (The former which the ONC considers "the core domains of interoperable exchange of health information.")
[53] *Id.*

stated in 2018 update to Congress that it would continue to measure and evaluate performance according to these measures, keeping a keen eye on policy changes being implemented under the 21st Century Cures Act.[54]

III. Current Efforts

In recent years, there has been a great deal of legislation that has further shaped the health privacy landscape for payors, providers, and patients. In April 2018, EHR Incentive Programs and the MIPS Advancing Care Information Performance category became "Promoting Interoperability Programs" as "just one part of the CMS strategic shift in focus to advancing health IT and interoperability."[55] 21st Century Cures Act[56] Section 4003 defines interoperability with respect to health IT as "technology that enables the secure exchange of electronic health information from, other health IT without special effort on the part of the user."[57] It also provides for "complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law and does not constitute information blocking as defined in section 3022(a)."[58] Information blocking refers to any practice that a provider knows or should know "is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."[59] The two practices can be in tension, but this bill promotes and funds the acceleration of research into methods for prevention and cures for serious illnesses—for

[54] HHS & ONC, *2018 Report to Congress*, https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf (last visited Nov. 1, 2019).
[55] 84 Fed. Reg. 7610, 7613.
[56] *21st Century Cures Act*, Pub. L. No. 114-255,130 Stat. 1033 (codified at 42 U.S.C. §§300jj(11) –(14) (Supp. V 2018)).
[57] 42 U.S.C.S. § 300jj (9) (LexisNexis, Lexis Advance through Public Law 116–56, approved August 23, 2019).
[58] 42 U.S.C.S. § 300jj (9) (LexisNexis, Lexis Advance through Public Law 116–56, approved August 23, 2019).
[59] 42 U.S.C.S. § 300jj-52(a)(1) (LexisNexis, Lexis Advance through Public Law 116–56, approved August 23, 2019).

which it is aptly named.[60] While the bill is largely about funding research, it contains provisions about information blocking and interoperability.[61]

Since its implementation, the ONC has introduced another proposed rule that outlines seven main exceptions—situations in which activities that would otherwise constitute information blocking are exempt from that characterization.[62] The full effect of these exceptions has not yet been realized, as they are part of a rule that will go into effect in 2020—the same time as the interoperability rule.[63] It is somewhat difficult to recognize the trend toward creating more leniency in the enforcement of the act. In May 2019, the Health Innovation Alliance called on ONC to "go back to the drawing board" and rework the proposal.[64] The group said the seven exceptions "contain too many loopholes which would result in extensive litigation before there can be meaningful enforcement of the 21st Century Cures Act prohibition on information blocking."[65] CMS has not, as of yet, provided more guidance on the proposal.

The interoperability rule arguably works *with* the 21st Century Cures Act through requirements that prevent information blocking.[66] Information blocking works both to protect patient data and to limit the liability of providers in charge of uploading that data.[67] But the

---

[60] HIMSS, *21st Century Cures Act—A Summary*, (Feb. 20, 2017), https://www.himss.org/news/21st-century-cures-act-summary.
[61] *Id.*
[62] James A. Cannatti III et al., THE NATIONAL LAW REVIEW, (Feb. 14, 2019), https://www.natlawreview.com/article/onc-proposes-to-define-conduct-not-information-blocking-under-cures-act. Those seven exceptions are: (1) preventing physical harm to patients and others; (2) promoting privacy of EHI; (3) promoting security of EHI; (4) recovering costs reasonably incurred to provide access, exchange, or use of EHI; (5) responding to infeasible requests to provide access, exchange, or use of EHI; (6) licensing interoperability elements; and (7) maintaining and improving performance of health information technology.
[63] *Id.*
[64] *Providers Call For HIPAA Clarity On Proposed Info Blocking Exceptions*, INSIDE HEALTH REFORM (June 12, 2019).
[65] *Id.*
[66] Lynsey Mitchel, *Overview of Proposed Rule from the Centers for Medicare & Medicaid Services Regarding Interoperability and Patient Access to Data*, NAT'L L. REV. (Apr. 19, 2019), https://www.natlawreview.com/article/overview-proposed-rule-centers-medicare-medicaid-services-regarding-interoperability.
[67] *Id.*

interoperability rule extends the requirement to make data available by focusing heavily on APIs, and simultaneously focusing on data privacy.[68] CMS believes that because the APIs have standardized technology, are technically transparent, and are implemented in a pro-competitive manner, they will allow for meaningful and convenient access to electronic health records.[69] If the API technologies are standardized, it will be easier for payors (insurers) to update the information and for patients to not only access the information but also to understand it.[70]

To promote transparency, "CMS is proposing to require that API-documentation be publicly accessible – meaning any individual using commonly available technology to browse the internet could access the information without any preconditions or additional steps beyond downloading and using a third-party application."[71] The idea behind pro-competitive implication is that pro-competitive practices "promote the efficient access to, exchange of, and use of electronic health information to support a competitive marketplace that enhances consumer value and choice of direct-to-consumer technology, health coverage and care."[72]

Seemingly, CMS believes that by creating a need and a market for APIs, more APIs will be developed. Within this competition to create them quickly and effectively, there will emerge better, lower-cost APIs. This strategy may also address the current problem providers face because there is little compatibility between and among different formats of healthcare data. This problem is due in large part to the fact that the EHR companies "have little incentive to make it easy to

[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Lynsey Mitchel, *Overview of Proposed Rule from the Centers for Medicare & Medicaid Services Regarding Interoperability and Patient Access to Data,* NAT'L L. REV. (Apr. 19, 2019), https://www.natlawreview.com/article/overview-proposed-rule-centers-medicare-medicaid-services-regarding-interoperability.

share data with providers who use their competitors' software."[73] CMS distinguishes two types of interoperability that it intends to promote with the rule: technical interoperability and semantic interoperability.[74] Technical interoperability refers to the capability of systems to "connect and exchange" data without alteration, and semantic interoperability refers to the capability of systems to "interpret and use" the data that has been exchanged.[75] The goal is to achieve both of these objectives simultaneously.[76]

Under the rule, the open API must include: "adjudicated claims (including cost); encounters with capitated providers; provider remittances; enrollee cost-sharing; clinical data, including laboratory results."[77] The API should also include other information patients need to easily access care, such as a provider directory so that patients can easily select a doctor within their network.[78] There are practical limits to updating this information and while insurance providers face penalties for inaccuracies in the directories,[79] providers themselves are under no penalty for being unresponsive to inquiries from patients. It is unclear if the implantation of this data into APIs would remedy this problem, it should certainly be a goal. This data must be updated "no later than one (1) business day after a claim is adjudicated or the encounter data is received by the plan" because the immediacy/timeliness of the updates is a crucial part of allowing providers to make determinations and to keep patients updated, as the rule intends to.[80] Because one day is

[73] Heather Bell, *CMS Announced 3 New Interoperability Initiatives. Here's What You Need to Know*, AMERICAN HEALTH LINE (Mar. 7, 2018).
[74] 84 Fed. Reg. 7615.
[75] 84 Fed. Reg. 7615.
[76] 84 Fed. Reg. 7619.
[77] Lynsey Mitchel, *Overview of Proposed Rule from the Centers for Medicare & Medicaid Services Regarding Interoperability and Patient Access to Data,* NATIONAL LAW REVIEW (Apr. 19, 2019), https://www.natlawreview.com/article/overview-proposed-rule-centers-medicare-medicaid-services-regarding-interoperability.
[78] *Id.*
[79] *Id.*
[80] *Id.*

not a long period of time, the practical limits of the requirements become relevant to the effectiveness of the overall stated purpose.[81] This information can be used, in theory, to better aggregate a patient's data and to prioritize research that will assist in detecting diseases earlier and more accurately.

IV. Other Benefits

When patients have access to all of the data in their medical records, they can take that data "with them from doctor to doctor, or to their other health care providers" more easily because they would already have access to it in a format that belongs to them.[82] This would not only mean that patients can choose a doctor that is available to them and meets their needs, but this would also "give that provider secure access to their data, leading to greater competition and reducing costs."[83] Immediate access to data lessens the burden on patients because if they wish to take their medical records to a new doctor, they do not have to wait for their provider to compile the records, print them, and then pick them up. They also will not have to pay the cost of printing or compiling the records.

The move toward interoperability will also assist in the healthcare industry's shift to "value-based payments."[84] "Value-based payment" models focus on rewarding hospitals, physicians, and other providers "for delivering high-quality health care" by tying payment to value.[85] As the name aptly suggests, payments are based on value: the monetary amount providers

---

[81] Jessica Kim Cohen, *AMA, CHIME Call for Interim Info-Blocking Rule*, MODERN HEALTHCARE (Sept. 23, 2019, 1:01 PM), https://www.modernhealthcare.com/technology/ama-chime-call-interim-info-blocking-rule (calling for supplemental rulemaking "to address a slew of industry concerns").
[82] Heather Bell, *CMS Announced 3 New Interoperability Initiatives. Here's What You Need to Know*, AMERICAN HEALTH LINE (Mar. 7, 2018).
[83] *Id.*
[84] *Id.*
[85] Sylvia M. Burwell, *Setting Value-Based Payment Goals – HHS Efforts to Improve U.S. Health Care*, NEW ENGLAND JOURNAL OF MEDICINE 372;10, PAGE 897 (Mar. 5, 2015) (available at https://pdfs.semanticscholar.org/0b48/6979fc7c7a9908db78ac99f9a070f62a455e.pdf).

receive is directly tied to the quality of the healthcare they provide to patients.[86] The "value" is measured by certain benchmarks, and in some "bundled care" arrangements, providers are encouraged to work as a team with a network of other providers to deliver the care efficiently together.[87] If, for instance, a patient needs to attend physical therapy prior to or after undergoing a surgical operation, a value-based payment model is one in which the surgeon and physical therapist work together to coordinate the patient's care and to ensure the patient makes a full recovery, within a specified time frame, in order to receive a higher level of payment. Essentially, the providers receive a bonus payment for ensuring the patient receives care quickly, but without sacrificing the quality of the care they receive. The incentive works to lower healthcare costs overall by preventing unnecessary visits to multiple providers and to ensure better patient care through coordination between and among providers.[88] As more insurers are beginning to incorporate value-based payment models and other alternative payment models, there is a need to better facilitate the exchange of patient data to meet the benchmarks outlined in the payment structures.[89] Interoperability would assist this goal by allowing all providers involved in the administration of care to access and update patient information, and would similarly allow the insurer or payer to monitor the patient's progress on an active basis.[90]

---

[86] *Id.*

[87] *Id.* The benchmarks are often metrics related to how quickly the patient recovers, how full of a recovery they make, and so on. The benchmarks ensure that doctors do not compromise the quality of care they provide in order to achieve the bonus payment.

[88] *Id.*

[89] Chelsea Cirruzzo, *CMS Releases New Model Request for Applications Amid Push Towards APMs*, INSIDE HEALTH REFORM (Oct. 30, 2019).

[90] Sylvia M. Burwell, *Setting Value-Based Payment Goals – HHS Efforts to Improve U.S. Health Care*, The New England Journal of Medicine, N. Engl. J. Med 372;10. March 5, 2015. (available at https://pdfs.semanticscholar.org/0b48/6979fc7c7a9908db78ac99f9a070f62a455e.pdf).

Most importantly, the API platform can be utilized to prioritize certain findings within a patient's medical records.[91] If providers work with software developers to prioritize data based on certain symptoms, the patient's age, or their medical history, this could ease the burden on providers to look back at the patient's entire medical history before making a diagnosis and recommendation.[92] For example, "a vendor can develop software that prioritizes a patient's most recent hospital visit over a negative colonoscopy."[93] This would revolutionize the way that doctors provide care and utilize their medical judgment when diagnosing patients. By employing an API capable of analyzing the data and self-selecting important information, doctors could, in theory, view a list of different diagnoses proposed by the software and then decide the best course of treatment. While in many cases this may automatically present a solution, doctors could also use the information gleaned by the API to employ additional tests to confirm the diagnosis.

The API would work by combining a patient's symptoms and her test results or vital signs to categorize possible medical diagnoses. By automating this crucial function, providers can more accurately treat patients and screen for more potential diseases by having all of the information in one place. Instead of relying on a patient's inevitably faulty memory, providers would be able to search a patient's complete medical record for other symptoms or potential complications and ascertain with better precision the proper diagnosis and course of treatment for the patient. Because the data would be automatically prioritized for the provider, this could lessen provider response time. It could also allow for providers to "create high-risk alerts for certain patients,"

[91] Chelsea Cirruzzo, *Providers Praise Medicare Claims Pilot, Call on Vendors to Stratify Data*, INSIDE HEALTH REFORM (Aug. 20, 2019, 5:56 PM).
[92] *Id.*
[93] *Id.*

and run the data through the software to eliminate care options and select the best one for the patient, perhaps by also including the patient's history into the care analysis.[94]

The COVID-19 pandemic has brought pre-existing conditions to the forefront of our minds and the news cycle. This emphasis on increasing awareness about which demographics are most at-risk to contract the coronavirus is a real-life example of how this tool could work to help identify diseases sooner and to proactively treat patients. As the CDC gathers more information from patients who have contracted coronavirus, it can better identify which patients are at a heightened risk. This seems elementary, given what we know now, but when the first cases of the virus were spreading, the lack of information greatly contributed to its transmission. This example highlights how important it is—now more than ever—to use the power of data to help people stay healthy or to recover from illnesses.

V. Perceived and Actual Barriers to Implementation

There are difficulties associated with fully implementing interoperability and there is uncertainty among providers about their ability to comply with both the interoperability rule and HIPAA. This can be dealt with simply by understanding what HIPAA is and what it is not. HIPAA was passed to help protect and safeguard the security and confidentiality of a person's health information.[95] One part of HIPAA, the Privacy Rule, aims to keep a patient's medical information private and prevent unnecessary disclosures of his or her PHI.[96] That certainly does not mean that a doctor can never talk to anyone about a patient's health information—doctors can still disclose a patient's PHI without his or her express written consent in many situations, especially if it is

[94] *Id.*
[95] Vincent Iannelli, *HIPAA Guide for Parents and Patients*, https://www.verywellhealth.com/hipaa-guide-for-parents-and-patients-2632300 (last visited Jan. 3, 2020).
[96] *Id.*

related to treatment, payment, or health care operations.[97] For example, if a patient has a heart attack, his doctor has to inform his insurance company in order to receive payment, but his credit card company does not have to be told about it.[98] If that same patient fell behind in paying his medical bills, that fact *can* be reported to credit agencies (but they cannot identify which bills or for which procedures the patient has yet to pay).[99] Under HIPAA, PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses).[100] This includes "diagnoses, treatment information, medical test results, and prescription information," as well as "national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information."[101] This means that entities *not* covered by HIPAA are *not* required to safeguard PHI and are not subject to penalties for mishandling it.[102] If all personal identifiers are stripped from health data, it ceases to be protected health information and the HIPAA Privacy Rule's restrictions on uses and disclosures no longer apply.[103] In the context of interoperability, however, all information uploaded and updated would be covered by HIPAA because it is all being handled by HIPAA-covered entities.

---

[97] *Id.*
[98] *Id.*
[99] Trisha Torrey, *11 Myths About HIPAA and Medical Records Privacy for Patients*, https://www.verywellhealth.com/hipaa-patients-and-medical-records-privacy-myths-2615514 (last updated Mar. 30, 2019).
[100] HIPAA J., *What Is Considered Protected Health Information Under HIPAA Law?*, (Apr. 2, 2018), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[101] *Id.*
[102] For an interesting discussion on the use of third-party data controllers such as "app developers", see *Cassidy Seeks to Tighten Privacy For Health Data In Third-Party Apps*, INSIDE HEALTH REFORM (June 19, 2019).
[103] *Id.*

To finance healthcare, administer benefits, and check benefit eligibility, a health insurer may, and always does, access medical records.[104] Improper use or access of data, outside of this limited scope, would be considered a breach.[105] It is a myth that a healthcare provider is required by law to provide *all* medical records to a patient when they exercise their right to request a copy of their records.[106] This exception serves as an additional protection for patients—if a doctor believes a patient's records will prove harmful (or if a doctor suspects a patient might inflict self-harm after viewing the records) then a doctor may deny the patient access.[107] Providers are not required to correct errors found in patient records—however, patients may request changes to their records.[108] Patient access to medical records is therefore essential—without access, patients will be unable to identify mistakes or request corrections. According to a 2016 study by Johns Hopkins, an estimated 250,000 patients die each year as a result of "diagnostic errors and medical mistakes."[109] Ross Kopel, a Health IT academic, estimates that nearly seventy percent of patient medical records contain mistakes.[110] Many of these errors are "irrelevant to health outcomes," such as listing that a patient twisted her ankle "on a Thursday, when it was in fact, Friday."[111]

Even when these mistakes are not acutely fatal, it is possible that many mistakes or instances when doctors accidentally overlook critical data for the patient's care do prevent patients from being diagnosed at an early stage. Particularly with cancer diagnoses, the importance of early

---

[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.* (this would likely be in the case of psychotherapy notes or other mental health information—this is not especially common, but it is important to note that patients do not have an absolute right to their records).
[108] Torrey, *supra* note 99.
[109] Johns Hopkins Medicine, *Study Suggests Medical Errors Now Third Leading Cause of Death in U.S.*, (May 3, 2016), https://www.hopkinsmedicine.org/news/media/releases/study_suggests_medical_errors_now_third_leading_cause_of_death_in_the_us.

[110] Christina Farr, *This patient's medical record said she'd given birth twice – in fact, she'd never been pregnant*, https://www.cnbc.com/2018/12/09/medical-record-errors-common-hard-to-fix.html (last updated Dec. 9, 2018).
[111] *Id.*

detection and prevention is the single most important factor to a patient's chances of survival. Interoperability would serve to curb this problem by allowing patients to actively monitor their EHR and to prevent inaccuracies from impacting the care they receive. While a patient may not remember what she told her physician during a yearly physical four years prior, she will ostensibly remember quite well what she told her doctor earlier in the day, the week, or the month.

By enabling patients to take an active role in monitoring their own records, not only will it ensure better accuracy, but it will also create an additional mechanism by which fraudulent claims can be identified, thereby combating rising healthcare costs in the aggregate.[112] In cases where providers may be inclined to alter medical records to reflect (and then bill for) services not actually rendered, the ability of patients to monitor their health records and claims data will function as a deterrent. The lack of patient involvement in medical record maintenance can pose serious problems during the administration of their health benefits. Even if a patient has coverage for a service, their health insurer may deny a portion of a claim or an entire claim simply because the information provided by the doctor (or the lack thereof) negates the needs for the insurer to pay for it. This is only one of many examples of how mistakes in medical records can pose problems for patients. Because patients trust their providers to upload the information correctly, they have little ability to check that the information is correct. For example, a patient may have his or her information mistakenly placed in another person's file, such as a sibling's file, or another family member. A provider could mistakenly update a patient's information twice, to reflect a procedure they only had once and should have been covered for the first time, but their insurance may refuse

[112] See generally, Jacqueline LaPointe, *How Providers Can Detect, Prevent Healthcare Fraud and Abuse*, (July 14, 2017) https://revcycleintelligence.com/features/how-providers-can-detect-prevent-healthcare-fraud-and-abuse (discussing CMS implementing "a proactive approach to fraud protection, eliminating its previous pay-and-chase method.").

the second. By allowing patients to actively check this information as it is uploaded, rather than after a problem arises with it, there will be fewer issues with which to deal.

In addition to easing access for patients, the Final Rule purports to champion ease of access for providers. In anticipating a problem that will arise through the initial implementation of the API, CMS has offered guidance on how to connect the many pieces of claim data and healthcare records that an individual patient will have (in the absence of the ability to implement a Universal Patient Identifier (UPI)).[113] The use of a UPI would be similar to a license plate number or a driver's license number, where each person has a unique combination of letters and numbers.[114] The main concern with UPIs is that they are easy to identify, once standardized, and lack the requisite security.[115] If every hospital, doctor's office, and healthcare insurance company suddenly organizes patient files simply by a string of letters and numbers, it may be easier to compromise.[116] Instead, CMS proposes the use of "patient-matching," a process whereby demographic and other unique information is used to match the data to the patient.[117]

Another potential barrier to complete implementation of interoperability relates to the Substance Abuse and Mental Health Services Administration (SAMSHA).[118] As a federal agency established by Congress in 1992 within the U.S. Department of Health and Human Services that "leads the public health efforts to advance the behavioral health of the nation,"[119] SAMSHA recently released a final rule, known as 42 CFR Part 2, which modernized the confidentiality

[113] 84 Fed. Reg. 7612.
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION, https://www.samhsa.gov. (last visited Jan. 3, 2020).
[119] *Id.*

requirements for substance use disorder (SUD) patient records.[120] "Previously, Part 2 applied to disclosures that 'would identify a patient as an alcohol or drug abuser."[121] Now, Part 2 applies to SUDs, which are defined as "a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired, control, social impairment, risky use, and pharmacological tolerance and withdrawal."[122] This definition does not include tobacco or caffeine use. In commentary, SAMHSA provides examples such as "alcohol, cannabis, hallucinogens, inhalants, opioids, sedatives, hypnotics, anxiolytics, and stimulants."[123] Under Part 2, a Part 2 Program must obtain written patient consent to disclose information related to SUD treatment.[124] The consent must contain: "the patient's name; the part 2 program permitted to make the disclosure; the amount and kind of SUD-related information to be disclosed; and the name of the individual or entity that is to receive that information."[125] While "tracking disclosures may prove to be burdensome to Part 2 Programs,"[126] this heightened level of privacy for patient information aligns with the sensitive nature of SUD treatment and should be afforded to all patients seeking SUD treatment that wants their information to remain private. The administrative burden is light in comparison to the burden the patient could suffer if their private information was shared without their consent. It is also worth noting that SAMHSA Part 2 is not synonymous with HIPAA.[127] Part 2 provides much more stringent federal protections than are required under other health privacy laws.[128] "This suggests

[120] Jennifer R. Breuer & Gregory E. Fosheim, *Top 10 Takeaways from SAMHSA's Recent Update of Substance Use Disorder Confidentiality Regulations,* 3-5 PRATT'S PRIVACY AND CYBERSECURITY LAW REPORT 08 (2017).
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] Breuer & Fosheim, *supra* note 120.
[127] *Id.*
[128] *Id.* (stating that while "Part 2 may look, talk[,] and smell like HIPAA, . . . it is not HIPAA").

that providers risk non-compliance by relying solely on their HIPAA policies to safeguard Part 2 Program patients' privacy."[129] In relation to interoperability, Part 2 seemingly requires informed written consent to include this information in a patient's EHR, which would be possible to achieve.[130] What is less clear, however, is if the patient must give written consent for *each* person who may access the information.[131] Even if a provider does not look at the particular record which indicates a patient's past SUD treatment, the fact that they have access to the information by virtue of access to the API would seem to indicate that the patient should be able to dictate whether or not they consent to such access. Although software programming may solve this by requiring patient consent on an on-going basis, it is clear that this requirement is in direct conflict with the affirmative requirement of the interoperability rule to disclose and make available *all* patient information. Without a clearer understanding of the specific capabilities and features of the API, the importance of patient privacy should trump the affirmative requirement to include the information in the EHR.

There are also a variety of state-specific laws aimed at maintaining the confidentiality of and protecting certain types of patient information that requires a heightened level of security. These laws regulate, among other things, the use and storage of genetic information, pregnancy and other women's' health information, and information pertaining to HIV/AIDS diagnoses.

Genetic information[132] and a patient's ability to control the use and storage of his or her genetic information is "at the heart of controlling and protecting an individual's rights."[133]

---

[129] Breuer & Fosheim, *supra* note 120.
[130] *Id.*
[131] *Id.*
[132] Leslie E. Wolf et al., *The Web of Legal Protections for Participants in Genomic Research*, 29 HEALTH MATRIX 1 (2019) (discussing the use of genetic information in the form of DNA uploaded to ancestry databases to identify people suspected of committing violent crimes).
[133] Jeffery Lawrence Weeden, *Genetic Liberty, Genetic Property: Protecting Genetic Information*, 4 AVE MARIA L. REV. 611 (2006).

"Genetic Liberty" is defined as the personal control of all aspects of a person's genetic make-up, including genetic material and information.[134] There are a variety of laws between and among the United States which dictate how genetic tissue may be collected, stored, and used for research and disease prevention.[135] Most state legislatures have enacted legislation with the purpose and effect of safeguarding genetic information at a heightened level than other types of health information.[136] This approach, known as genetic exceptionalism, "calls for special legal protections for genetic information as a result of its predictive, personal and familial nature and other unique characteristics."[137] Some commentators argue in favor of treating genetic information the same as other health information because "genetic information is simply another form of health information and is, therefore, difficult to distinguish from other health information, all of which deserves equal protection under the law."[138] With respect to privacy, Washington is the only state that explicitly complies with this approach by treating genetic information the same as other health information.[139] It does so simply by including genetic information in the definition of health care information under the state health privacy law.[140] This means that every piece of information in a patient's medical record is confidential and requires express written consent for disclosure. While

---

[134] *See* ROBERT C. KING & WILLIAM D. STANSFIELD, A DICTIONARY OF GENETICS 140 (5th ed. 1997) ("Genetic Information" in the field of genetics is "the information contained in a sequence of nucleotide bases in a nucleic acid molecule."); Nora O'Callaghan, *Human Origins and Human Rights in the Genome Age*, 3 AVE MARIA L. REV. 123, 123 (2005) (positing that a person is substantially more than just his genetic materials and information).

[135] NATIONAL CANCER INSTITUTE CANCER DIAGNOSIS PROGRAM, *50-State Survey of Laws Regulating the Collection, Storage, and Use of Human Tissue Specimens and Associated Data for Research*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwif5a-pqejmAhUZAp0JHYDYBdEQFjABegQIBhAI&url=https%3A%2F%2Fdrexel.edu%2F~%2Fmedia%2FFiles%2Fresearch%2Fadministration%2Fqaqi%2Fresources%2F50StateSurveyresearch%2520Law.ashx&usg=AOvVaw34VUf5WlnuedtsnbygzFRG (last visited Jan. 3, 2020).

[136] NATIONAL CONFERENCE OF STATE LEGISLATURES, *State Genetic Privacy Laws*, http://pierce.wesleyancollege.edu/faculty/hboettger-tong/docs/hbt%20public%20folder/FYS/State%20Genetic%20Summary%20Table%20on%20Privacy%20Laws.htm (last visited Jan. 1, 2020).

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

a total of twenty-six states require written consent to disclose genetic information, only seven states require written consent to retain that same information.[141] Perhaps even more alarming, of the twenty-six states that do require consent to disclose genetic information, only five define genetic information as personal property—belonging to the person from whom it is extracted.[142] The inclusion of genetic information in a patient's EHR poses a problem similar to that presented with SUD treatment information—in those states which require specific consent, it is unclear whether the API will contain the necessary functions to comply with state-specific privacy laws. It is unclear whether there will be a method by which the API monitors the location from which the information is accessed. Ideally, it will include a mechanism by which the sensitive information is secured and only viewable by providers to whom patients have expressly granted access.

Information regarding HIV/AIDS diagnoses and treatment are typically subject to heightened scrutiny and pose similar problems to those discussed in connection with genetic information. Virtually all states have enacted some HIV-specific statutes, many of which concern information collection and protection either directly or indirectly.[143] "Twenty-three states classify HIV/AIDS as a separate category of disease, sixteen classify it as a communicable disease, and twelve as a sexually transmitted disease."[144] All states require reporting of AIDS cases to the state or local health department, and forty-one states also require reporting of HIV infection.[145] Much like the limited-scope disclosure allowed by HIPAA, forty-eight states allow for disclosure of

---

[141] *Id.*
[142] NATIONAL CONFERENCE OF STATE LEGISLATURES, *State Genetic Privacy Laws*, http://pierce.wesleyancollege.edu/faculty/hboettger-tong/docs/hbt%20public%20folder/FYS/State%20Genetic%20Summary%20Table%20on%20Privacy%20Laws.htm (listing those five states as Alaska, Colorado, Florida, Georgia, and Louisiana.) (last visited Jan. 1, 2020).
[143] ELECTRONIC PRIVACY INFORMATION CENTER, *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization*, https://epic.org/privacy/medical/cdc_survey.html (last visited Oct. 10, 2019).
[144] *Id.*
[145] *Id.*

HIV-related information in certain proscribed circumstances.[146] The most commonly cited permissible disclosures relevant to interoperability are to: a health care provider involved in the patient's care (43); blood banks or organ donors (22); epidemiologists and researchers (22); HMOs, health care institutions, or mental health facilities (14); and insurance companies (8).[147] Some disclosure provisions require that patient-identifying information be removed from the data, which would not be consistent with the goal of interoperability, but would be consistent with patient privacy goals.[148] "Thirty-eight states report statutory requirements for specific consent for HIV testing including consent to the release of information."[149]

Conversely, just because a state lacks an HIV-specific consent statute does not necessarily mean that informed consent is not required in a particular state.[150] Informed consent may be required by other statutes, common law, regulations or policies.[151] Consistent with, but reaching farther than, the stated objectives of HIPAA, "[f]orty-five states have either criminal or civil penalties for unauthorized disclosure of HIV related information.[152] Thirty-three states have criminal penalties, thirty-three have civil penalties and twenty-one provide for both civil and criminal penalties."[153] For providers tasked with updating the health information of their patients in order to comply with the interoperability rule, and tasked with safeguarding the privacy of their patients' most sensitive information, there is no clear path forward. Compliance with both rules is seemingly impossible—and providers are forced to face potential civil and/or criminal penalties for including a patient's information in his or her EHR. This seems antithetical to the stated

[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 143.
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*

objectives behind interoperability. The point of creating the open API is to ease the burden on providers, not to force them to choose which laws to break and which to obey.

VI. The Role of the Internet

The California Consumer Privacy Act (CCPA) was passed with the intention of "holding businesses accountable for data protection through strict guidelines and threatening consequences, the new California privacy act is setting the foundation for US data privacy in 2020."[154] For patients who reside in California and wish to access their health information via the open API structure, the CCPA would seemingly limit how they and their providers access and upload that data. The CCPA "outlines new standards for data collection, new consequences for businesses that fail to protect user data, and new rights that California consumers can exercise over their data."[155] According to the CCPA, "businesses" that collect "consumer" data are subject to the heightened regulations.[156] Under the CCPA, a "consumer" is defined simply as a California "resident" and a "business" is defined as a "for-profit entity that collects 'consumer' data" and has either: an annual gross revenue over $25 million; or annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households, or devices for commercial purposes; or derives fifty percent or more of its annual revenue from selling consumer personal information.[157] By that definition, every healthcare insurer that provides health insurance to 50,000 or more California residents is a "business" subject to the heightened regulations. While it is unlikely that a single doctor would satisfy the definition of business, it is possible that a hospital group or network of providers could ostensibly meet the two-pronged "business" test. The

[154] KJ Dearie, *CCPA: California Consumer Privacy Act*, TERMLY (June 18, 2019), https://termly.io/resources/articles/california-consumer-privacy-act/.
[155] *Id.*
[156] *Id.*
[157] *Id.*

CCPA applies to all businesses—regardless of the headquarters of the business, itself.[158] This is perhaps the most important aspect—because all insurers that collect data must comply with the regulations outlined in the CCPA.

Personal information under the CCPA means "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and includes other categories such as biometric information, IP addresses, and inferences drawn about a consumer related to their preferences, predispositions, and psychological trends.[159] Importantly, the CCPA includes an exemption for protected health information collected by a covered entity or business associate that is otherwise subject to HIPAA, but because this is not an "entity-wide exemption" it does not entirely eliminate an insurance provider's obligations under the Act.[160] Insurance companies must still do their due diligence to identify the categories of consumers for whom they collect information and "determining whether they fall under an exemption to the law."[161] Though insurance companies will not be "selling" patient data in order to make it accessible in accordance with the interoperability rule, it is important that they update contracts with their service providers to ensure compliance with the CCPA.[162]

The purpose underlying the CCPA is, as the name suggests, to give more rights to individuals in furtherance of consumer privacy objectives. It gives individuals a list of enumerated rights, all of which concern the access, transfer, editing, and deletion requests of their data.[163] It establishes greater consequences for businesses that fail to adequately protect data and shifts

[158] *Id.*
[159] Kirk J. Nahra & Ali A. Jessani, *Reading the Fine Print: What Insurance Companies Need to Know About the CCPA*, THE RECORDER (January 24, 2020).
[160] *Id.*
[161] *Id.*
[162] *Id.*
[163] Dearie, *supra* note 154.

accountability for data protection onto businesses that collect and handle user information—both of which match up well with the rule's goals to empower patients and incentivize providers to generate more patient-friendly solutions.[164] On its face, the CCPA is seemingly perfectly aligned with the goals outlined in the interoperability rule. Upon closer inspection, however, it is tough to reconcile some of the other rights the CCPA grants with the Final Rule. For example, the CCPA gives consumers the ability to opt-out of certain data-processing practices.[165] Again, insurers and providers who fall into the category of "businesses" under the CCPA are faced with almost an impossible choice—comply with either the interoperability rule or the CCPA. According to the CCPA text, Californians are now entitled to "know what information is being collected about them; to know if their personal information is sold or disclosed, and to whom; to say 'no' to the sale of personal information; to access their personal information; and to equal service and price, even if they exercise their privacy rights."[166] Because the interoperability rule does not squarely address the way in which the CCPA interacts with the stated requirements, it is tough to know how to proceed.

For health care providers and insurers, the CCPA means they must comply with more state-specific laws than simply those of state in which they reside. If their patients, enrollees, beneficiaries, etc. travel to or live in a state with different privacy laws than the provider's home state, it is unclear how the interoperability rule changes the requirements. Under statutes like the CCPA, however, it would appear they need to comply with those requirements as well as their home state requirements. This *is* possible, albeit difficult. With proper guidance from CMS, it should be possible to simultaneously comply with multiple rules. Because all of these rules are

[164] *Id.*
[165] *Id.*
[166] *Id.*

aimed at increasing patient privacy rights and granting access within the existing framework, compliance is possible. It may take time, but CMS is optimistic that the right API can and will be developed and that it will enable interoperability, so that providers may remain focused on giving the best healthcare possible to their patients. This further highlights the aforementioned key role that the API plays, despite the fact that it has not yet been established.

VII. Potential Solutions

It is important to note that just because patients may be granted "access" to their data—the affirmative requirement for providers to disclose such information is not accompanied by heightened security or privacy measures. Patients (aside from those residents in California who have a private right of action under the CCPA) still do not have any actionable legal right or remedy for the misuse or impermissible disclosure of their health information. This transitional period while developers are creating the open API brings a heightened chance of healthcare data breach. Lacking any private right of action under HIPAA, patients are in no position to protect themselves from over-zealous providers and insurers who are still acclimating to this new structure. While the benefits of interoperability certainly outweigh the initial burdens associated with implementation, it is important to keep in mind that this rule was passed for, and its implementation and continued use should be tailored to, individual patients whose health and privacy depend on it. In addition, it is important to note that COVID-19 already has and will continue to increase pressure on our healthcare system. In response to the drastic changes that COVID-19 has caused, CMS is considering delaying the implementation of the interoperability rule and will offer enforcement leniency for various deadlines within the bill.[167]

[167] Amy Lotven, *Insurers Ask CCIIO For Short-Term Plan Moratorium, Rule Delays*, INSIDE HEALTH REFORM (April 22, 2020, 1:52 PM); see also Michelle M. Stein, *CMS Relaxes Quality Reporting For 2019, 2020 Amid COVID-19 Pandemic*, INSIDE HEALTH REFORM (March 23, 2020, 1:08 PM) ("'CMS recognizes that quality measure data collection and reporting for services furnished during this time period may not be reflective of their true level of

Because the main goal of interoperability is to make patient data available, more protections are needed to ensure that patient data is not subject to breach or misuse without recourse. As written and enacted, the rule does little to actually equip patients with anything other than their data. It does not have a private right of action, such as the one included in the CCPA. This means that patients whose PHI or other data is subject to a breach have no new legal protections. Advocates for greater patient privacy protection have noted that because of the rule, "a lot more data, both covered and not covered by [HIPAA], will be available in the wild."[168] "A lot more" is putting it lightly. Currently, 67.7 million Americans are enrolled in Medicare,[169] and 70.7 million Americans are enrolled in Medicaid and CHIP.[170] As the Coronavirus pandemic continues to threaten the health, employment, and finances of millions of Americans, these enrollment numbers and sure to rise.[171]

The need for increased privacy protections, however, does not stem from an increase in enrollment. This need stems from the existing privacy landscape and the rule itself. By enlisting the help of vendors to develop the APIs on which patients will eventually access their data, CMS has failed to account for the privacy risks this poses for patients at an individual level. This is precisely because the rule "lacks the necessary guardrails to protect consumers from actors such

---

performance on measures such as cost, readmissions and patient experience during this time of emergency and seeks to hold organizations harmless for not submitting data during this period,' CMS says.")

[168] Chelsea Cirruzzo, *Providers, Hospitals: ONC Rule Doesn't Do Enough To Protect Privacy*, INSIDE HEALTH REFORM (March 9, 2020, 8:31 PM).

[169] Meredith Freed, Anthony Damico, & Tricia Neuman, *A Dozen Facts About Medicare Advantage in 2020*, KAISER FAMILY FOUNDATION, (April 22, 2020) https://www.kff.org/medicare/issue-brief/a-dozen-facts-about-medicare-advantage-in-2020/.

[170] *January 2020 Medicaid & CHIP Enrollment Data Highlights*, MEDICAID.GOV (available at https://www.medicaid.gov/medicaid/program-information/medicaid-and-chip-enrollment-data/report-highlights/index.html).

[171] Bob Herman, *Medicaid will be a coronavirus lifeline*, AXIOS (April 1, 2020) https://www.axios.com/medicaid-aca-coronavirus-lifeline-f71c3adc-c153-4069-97f6-fa439060ef71.html.

as third-party apps that are not required to meet the same stringent privacy and security requirements as hospitals."[172]

In response to this obvious shortcoming, Congress must amend HIPAA to explicitly include these third-party apps as covered entities. The Trump administration and CMS have addressed privacy-related concerns by assuring stakeholders "they will take privacy into account,"[173] and that "it is taking steps to let payers and patients protect their information."[174] These steps include asking "third-party application developers to attest to certain privacy provisions" and educating "enrollees about sharing health information with third parties."[175] According to HHS, however, "third-party apps that are developed outside of a HIPAA-covered entity are not subject to HIPAA rules even if a breach occurs."[176] Simply asking vendors to comply without any potential criminal or civil liability for failing to do so is not enough/completely juvenile. Likewise, educating patients is not enough without equipping them with a source of legal recourse in the even that their information is misused.

Given the purpose of the rule and the enforcement power that CMS holds, it is inapposite to place the onus on a patient to know whether or not or for which purpose they should give their most sensitive health information to a third-party app. I do not mean to undercut the ability or knowledge of patients—I merely mean that patients should not be forced to choose between better access to their health data and the protections afforded by the law. They should be able to have both knowledge and legal protection, and it is up to Congress to make that happen. If the success of this rule and the future of interoperability rely on the APIs and third-party apps, there

---

[172] Cirruzzo, *ONC Rule Doesn't Do Enough*, supra note 168.
[173] Chelsea Cirruzzo, *ONC Finalizes Long-Awaited Interoperability Rule, Addresses Privacy*, INSIDE HEALTH REFORM, March 9, 2020 8:28 PM.
[174] Michelle M. Stein, *CMS Changes Hospitals CoPs, Will Require Digital Provider Directories*, INSIDE HEALTH REFORM, March 9, 2020 8:18 PM.
[175] *Id.*
[176] Cirruzzo, *ONC Finalizes*, supra note 173.

is no reason why those entities should not be accountable the way that hospitals, providers, insurers, and their business associates are. By this I mean, if they play such a crucial role in enabling patient access to data, there should be liability for mishandling that information or compromising its confidentiality.

In addition, Congress should amend HIPAA to clearly include a private right of action. This would enable patients who suffer injuries as a result of a data breach by a covered entity to be made whole. A private right of action would further incentivize the entities that handle EHR to take extra measures to safeguard patient information. By placing the burden of compliance of payers, providers, and the third-party apps without additionally granting individual rights, patients do not have adequate privacy protection. Though the idea of adding a private right of action under HIPAA has garnered a plethora of reactions ranging from full support to condemnation, newer, more comprehensive privacy statutes like the CCPA and the GDPR in Europe do include private causes of action. The CCPA has not been enacted long enough to definitively determine whether the creation of a private right of action has caused a noticeable increase in cases or significantly burdened the courts, as opponents of creating a private cause of action suggest. Though oft-cited, there are practical limitations in place that will limit—if not entirely dispel—the proverbial "flooding of the courts" that critics often warn against.

The most obvious safeguard against this concern has plagued privacy advocates and those attempting to bring privacy-based claims for many years: standing requirements. In order to bring a claim for anything, including a proposed private right of action under HIPAA, a plaintiff must meet Article III Standing requirements. To have standing to sue, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that

is likely to be redressed by a favorable judicial decision."[177] Standing requirements have long served as a barrier to bringing superficial claims, and in the privacy context in particular, they have prevented plaintiffs from bringing claims where they suffered no injury in fact. The need for a private right of action is most obvious particularly where CMS and the Trump administration state that they are encouraging app developers to create and implement privacy policies. While privacy policies are a good start, they do not equip patients with sufficient standing for redress suffered as a result of a health data breach.[178] This is due especially to the fact that data breaches are unlike other forms of tangible injury—once the data has been breached, it cannot simply be put back in a patient's file. Those patients whose information is misused and who suffer as a result of that breach deserve the ability to pursue that harm the same way that a person who suffers a tortious injury is able to.

Other critics have pointed to congressional intent (or rather, the lack thereof) as a reason not to implement or infer a private right of action.[179] While it is true that the statute as written does not include any means by which private enforcement may occur, it is also true that when Congress enacted HIPAA in 1996 it had no way of knowing what the health data privacy landscape would look like almost a quarter of a century later. When Congress amended HIPAA in 2006 to allow HHS enforcement, it similarly could not predict with any certainty what the data privacy landscape would evolve into. The push toward interoperability has occurred much more recently, and with this major change comes the need for other changes, namely, more protection and more enforcement. As new data privacy risks emerge, and as legislation changes, Congress now has

[177] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
[178] While Section 5 of the FTC prohibits unfair and deceptive practices, there is no private cause of action under the FTC either.
[179] See Acara v. Banks, 470 F.3d 569, 571-72 (5th Cir. 2006) ("HIPAA limits enforcement of the statute to the Secretary of Health and Human Services. Because HIPAA specifically delegates enforcement, there is a strong indication that Congress intended to preclude private enforcement.") (internal citations omitted).

both the understanding and the opportunity to fill in the gaping holes that this changing landscape exposes.

VIII. Conclusion

It is possible that the perfect API can be developed to allow compliance with a plethora of laws and objectives. Given the advancement of technology and the incentivization that the rule provides, the healthcare industry will inevitably generate solutions to these problems as they arise. Although it will be costly to initially implement, the API will eventually lower the costs of healthcare by decreasing barriers to accessing the data and by enabling researchers to find cures for diseases by better aggregating health data.

In terms of the lasting impact of the rule on patients, if the data can be prioritized or stratified in a way that better predicts a patient's health outcomes, then it would lead to better, more informed diagnoses and hopefully lead to a healthier population. By involving patients on a more consistent basis, they will ask better questions, be more involved in their care, and lessen the chance that providers will miss a crucial piece of their care (because patients will be able to remind them, or to ask questions, or to know when things have been incorrectly updated to their charts). This approach helps foster a better system of checks and balances between the patient, provider, and insurer. When patients, providers, and payers all have access to the same information and can be directly involved in (and informed of) what is happening, there are more opportunities to correct discrepancies and to catch the crucial information that is needed to make the best decision—both for the patients' physical health and financial benefit. Mere access to this data is not enough to achieve the goals of interoperability—patients must be able to hold providers, payers, and vendors accountable for any harm that mishandling of this sensitive information causes.