New York University
A private university in the public service
School of Law
Clinical Law Center
Technology Law & Policy Clinic

April 23, 2021

Marissa Gordon-Nguyen, Senior Advisor for HIPAA Policy
Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Marissa Gordon-Nguyen,

We write to you on behalf of NYU's Technology Law and Policy Clinic in response to the Department of Health and Human Services' (HHS') Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinate Care and Individual Engagement (Proposed HIPAA Rule) which was published in the Federal Register on January 21, 2021 (RIN 0945-AA00; Docket No. HHS-OCR-2021-0006-0001).

This comment raises an important issue not included in the proposed rule and HHS' broader regulation of health privacy. As HHS itself acknowledged in its notice, the current Privacy Rule permits provider-to-provider disclosures of protected health information (PHI) without individual patients' knowledge or authorization, so long as the exchanges are for treatment, payment, and healthcare operations.[1] This aspect of the current Privacy Rule harms some of the most vulnerable patients in light of the development of Health Information Exchanges (HIEs), which have accelerated the sharing of PHI from provider to provider. We urge HHS to reform the HIPAA disclosure rule codified at 45 CFR § 164.506 or implement new regulation of HIEs to increase medical privacy protections. While important consideration has been given in the Proposed HIPAA Rule to patients' ability to access their own medical data, some consideration must also be given to patients' ability to limit third parties' access to their data.

Gaps in current medical privacy laws erode patient privacy and harm some of the most vulnerable. Specifically, when increasingly powerful HIEs (described *infra*) share patients' sensitive personal prescription information with healthcare providers without the patients' knowledge or consent, the resulting harm falls disproportionately on groups at risk of

[1] Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Fed. Reg. 6446 at 6462 (proposed Jan. 21, 2021) (to be codified at 45 C.F.R. § 160 and 164).

discrimination. These groups often experience greater health disparities than the general population yet are less likely to gain access to healthcare given multiple structural barriers.[2]

This comment recommends several strategies to fill those gaps. Three key recommendations include requiring all healthcare providers to obtain prior patient authorization before disclosing PHI to third parties, strengthening patients' ability to opt out of provider-to-provider PHI sharing, and adopting HIE-specific regulation to require healthcare providers to obtain patient consent prior to accessing or sharing patient information with HIEs.

I. Health Information Exchanges Are Lightly Regulated Under Current HIPAA Rules

A. Introduction to HIEs and to a Leading HIE, Surescripts

HIEs are systems that allow healthcare providers to access and share a patient's medical information electronically.[3] A leading example of an HIE is Surescripts, the largest e-prescribing network in the United States, so this comment will describe Surescripts' technology and its reach to exemplify the broader industry.

While Surescripts' original function was to mediate electronic prescriptions sent from healthcare providers to pharmacists, today, Surescripts offers a separate Medication History look-up service. This service enables users of e-prescription software connected to Surescripts' network to view the e-prescription history of a given patient that was previously sent through Surescripts' network. In short, by making use of the data it collects through its e-prescribing function, Surescripts is able to offer a separate prescription history look-up function—Medication History. Therefore, Surescripts also acts as an HIE.

Surescripts is not the only HIE. Various other HIEs were created by and are regulated under state-run initiatives. These state-regulated HIEs are often required by state laws to provide patients the choice to opt out of or opt in to a given HIE. Unlike Surescripts, these state-regulated HIEs exist only for the purpose of sharing medical data.[4]

In practice, state-regulated HIEs are much less widely used than Surescripts' Medication History. Because Surescripts has an effective monopoly status as the nation's leading e-prescription network,[5] Americans' prescription data is becoming increasingly centralized in

---

[2] *See* Joshua D. Safer et al. *Barriers to Healthcare for Transgender Individuals*, 23 Curr. Opin. Endocrinol Diabetes Obes. 168-71, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4802845/.

[3] For more information on HIEs, *see Health Information Exchange*, HealthIT.gov, https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/health-information-exchange

[4] As an example of HIEs created by state-run initiatives, see the Statewide Health Information Network for New York (SHIN-NY), which is a network of HIEs created by New York State. Participating HIEs in SHIN-NY are required by New York State law, NYCRR tit.10, § 300.5(a), to obtain patient authorization before their participation in HIEs. *See* What is the SHIN-NY, New York eHealth Collaborative, https://www.nyehealth.org/shin-ny/what-is-the-shin-ny/.

[5] Surescripts has virtually monopolized the e-prescribing market and is currently the subject of an antitrust lawsuit over its use of exclusivity agreements. *See FTC Charges Surescripts with Illegal Monopolization of E-Prescription*

Surescripts' database. Surescripts' Medication History service is able to provide its customers—healthcare providers—access to medication information for 95% of patients in the U.S.[6] Given the ubiquity and necessity of e-prescription software for most healthcare providers, most providers have access to the prescription history held by Surescripts. For healthcare providers and certain patients, there are clear benefits to Surescripts' Medication History service. For example, the service enables healthcare providers to detect potential medication abuse and reduce errors in patient charts.[7]

But there is a problem: Surescripts does little to protect the privacy of patients' medication histories. Unlike with state-regulated HIEs, with Surescripts Medication History patients have no choice to prevent their data traveling through Surescripts unless they avoid receiving medication prescriptions altogether. Surescripts' ubiquity and business model makes its status as an HIE especially troublesome.

Surescripts thus hinders patients' ability to control sharing of their prescription drug history with healthcare providers. This state of affairs is unfortunately legal, given the current HIPAA Privacy Rule and generally limited regulation of HIEs, as we explain in the next section.

B. Surescripts and Other HIEs Are Subject to HIPAA, but HIPAA Imposes Few Substantive Restrictions on Their Operations

Surescripts is subject to HIPAA because it is an e-prescribing gateway, which is regulated as a "business associate" under HIPAA.[8] As explained above, besides being an e-prescribing gateway, Surescripts is also an HIE because of its Medication History service.[9] Guidance from HHS explains that HIEs that perform functions on behalf of covered entities like healthcare providers are treated as "business associates" under HIPAA.[10] As a business associate, an HIE is required to have a business associate agreement in place with any covered entity using its service to safeguard PHI in accordance with HIPAA rules.[11] Thus, Surescripts and other HIEs are subject to HIPAA and its rules.

Markets, FTC, Apr. 24, 2019 https://www.ftc.gov/news-events/press-releases/2019/04/ftc-charges-surescripts-illegal-monopolization-e-prescription

[6] *See* Benefit Optimization, Surescripts, https://surescripts.com/enhance-prescribing/benefit-optimization/6d5017a2-bf23-6adb-9614-ff010051f5b3/

[7] *See* Medication History, Surescripts, https://surescripts.com/inform-care-decisions/medication-history

[8] *See* 45 C.F.R. § 160.103; *HIPAA, Too: Many ARRA Privacy Provisions Amend HIPAA, Not Create New Regulation*, AHIMA, https://library.ahima.org/doc?oid=98112#.YCNOQpNKgl-.

[9] *See What is HIE? HealthIT.gov*, https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie.

[10] *See The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment*, HHS.gov, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf.

[11] *Id.*

HIEs' being subject to HIPAA has a negligible impact in practice because the HIPAA rules impose essentially no substantive constraints on Surescripts and other HIEs. Under 45 C.F.R. § 164.506(c), providers are allowed to use and disclose patient information among providers for the purpose of "treatment, payment, and healthcare operations" (TPO) without requiring patient consent.[12] Given that TPO is a broad category,[13] there is little limitation to providers obtaining access to patients' complete prescription histories, regardless of the type of care the providers are administering. For example, a dentist can easily gain access to prescription history information revealing intimate information about a patient's reproductive health without the patient's knowledge or authorization.

Additionally, while the HIPAA Privacy Rule has a provision that requires covered entities to provide patients with notice of their privacy practices for PHI, the provision does little to protect or inform patients. The HIPAA Privacy Rule's existing provision on use and disclosure requires only that covered entities provide a general description of the disclosures the covered entity is permitted to make for TPO, with at least one illustrative example.[14] The generality of this requirement means providers are not required to mention Surescripts by name, and thus patients are unlikely to be alerted to Surescripts' existence.

Since Surescripts and the providers who use its Medication History look-up service can credibly claim that the data sharing or access is for TPO, data sharing and data access through Surescripts is not a violation of any existing HIPAA rule. Because of the way Surescripts' technology works, data sharing with Surescripts' Medication History is an inevitable consequence of sending an e-prescription, which is an important part of a patient's treatment plan. Data access through Surescripts to verify a patient's medication history can likewise be characterized as related to treatment or operations. Thus, the existing Privacy Rule permit Surescripts and other HIEs to share patients' sensitive prescription drug histories among providers without patients' knowledge or consent.

This state of affairs was not inevitable. In fact, earlier versions of the Privacy Rule required covered entities and their business associates to obtain patient consent before sharing PHI from provider to provider. The need for patient consent was debated in public comments submitted in response to a March 2002 NPRM. Opponents of the consent rule cited the administrative burden a consent requirement imposed.[15] Supporters of the consent rule urged HHS to retain the consent requirement as a default rule and suggested individualized solutions to specific situations in which the requirement presented genuine obstacles to healthcare delivery.[16] Ultimately, in its final rule, HHS elected to eliminate the consent requirement because HHS

---

[12] 45 C.F.R. § 164.506(c)(1) and (2).

[13] HHS' guidance on what is considered "treatment, payment, and healthcare operations" defines these categories broadly. *See* Uses and Disclosures for Treatment, Payment, and Health Care Operations, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html

[14] 45 CFR § 164.520(b)(i)(ii).

[15] 67 Fed. Reg. 53182, 53190 (2002).

[16] 1 Hooper, Lundy and Bookman, Medical Records Privacy Under HIPAA § 3.02 (2020)

believed that replacing consent with a strengthened notice provision would afford consumers adequate privacy protections.[17]

Subsequently, a 2004 lawsuit, *Citizens for Health v. Thompson*, challenged the elimination of the consent requirement on the basis that it violated the Administrative Procedure Act as well as property and privacy rights guaranteed by the Constitution.[18] A federal district court rejected all of these arguments and found that, even assuming that there is a constitutional right to privacy, HHS' new rule did not violate patient rights because the rule neither requires nor *prohibits* healthcare providers from seeking consent from patients prior to sharing PHI.[19] The court reasoned that if a rule is not compulsory, then it does not affirmatively interfere with any constitutional rights.[20] In 2005, the Third Circuit affirmed.[21]

While the lack of a patient authorization requirement in sharing of PHI related to TPO has always posed medical privacy concerns, today it poses a greater threat than ever because of HIE's facilitation of the frictionless transfer of information. In the earlier days of the HIPAA Privacy Rule, before the technical infrastructure for frictionless data sharing become widely adopted, there were practical constraints on the sharing of PHI. For example, patients often had to initiate data transfers themselves, even if not required by law, by calling one healthcare provider to request a transfer of their medical records to another provider. This additional step at least gave patients notice and an opportunity to object. With the development of HIEs like Surescripts, a healthcare provider can now easily access a patient's prescription history by conducting a quick search using their e-prescription software, without providing any additional notice to the patient.

II. How the Erosion of Medical Privacy Disproportionately Harms Some of the Most Vulnerable Communities

The lack of control over one's prescription history resulting from Surescripts' service is troubling because prescription history can be as revealing as clinical record information. For example, from prescription history, a healthcare provider can infer transgender status, mental health condition, history of medical abortion, HIV status, and other health information that subjects patients to a heightened risk of discrimination.

The current use and disclosure rule under HIPAA presumes that providers need not obtain patient authorization prior to sharing or accessing PHI because it presumes that threats to patients are external to the relationship between patients and healthcare providers. The current rule presumes that the sharing of full health records between providers—not just a narrower set of records specifically relevant to a particular healthcare option or procedure—is necessarily

---

[17] *Id.*

[18] *Citizens for Health v. Thompson*, No. 03-2267, 2004 U.S. Dist. LEXIS 5745 (E.D. Pa. Apr. 2, 2004).

[19] *Id.*

[20] *Id.*

[21] 428 F.3d 167 (2005).

beneficial to the patient. The rule's presumption that *all* medical records are *always* relevant to care is fundamentally inaccurate.

The presumption that providers should have unfettered access to patients' complete medical histories causes real injury because many marginalized groups have long experienced, and continue to experience, discrimination and other harm by certain healthcare providers. For example, one-third of transgender people reported being refused medical care or harassed by medical professionals because of their transgender status, and a quarter avoided going to the doctor altogether.[22] LGBTQ people face greater health risks than the general population but are more likely to distrust the medical establishment due to personal or their community's experiences of discrimination.[23] Consequently, presumptive access to all of a patient's records effectively raises the barrier to healthcare access for many who are part of marginalized groups.

The following example illustrates how this dynamic raises the barrier to healthcare access for marginalized groups. Transgender and gender non-conforming people experience discrimination in the United States. To navigate discriminatory environments, people often rely on various tools to help. For many transgender and gender non-conforming people, the decision of whether to seek treatment at a given clinic sometimes depends on the extent to which a patient knows they will receive institutional support if an adverse event with a provider occurs. The need for safety fuels demand for health clinics that specifically serve transgender and gender non-conforming populations, as evidenced by the existence of many community- and government-generated directories of transgender-affirming providers and services.[24] That so many transgender and gender non-conforming people seek out health clinics that specifically serve them is evidence that many transgender and gender non-conforming people receive subpar care from other providers.

The ability to withhold sensitive medication information is an important tool that empowers patients and protects them from discrimination. Preserving a patient's choice to not share sensitive medication information allows transgender and gender non-conforming people's navigation of healthcare in a discriminatory environment. Specifically, despite the existence of trans-friendly providers, some transgender and gender non-conforming people will inevitably access care from healthcare providers who might lack trans-competency or exhibit discriminatory bias. Community health clinics that specifically serve the LGBTQ population often have limited resources, are geographically limited to major metropolitan areas, and offer a scope of services frequently limited to general healthcare. If a patient needs to see a specialist, they will often have to visit a practice other than their primary provider's practice. In addition to exposing a patient to potential discrimination, working with a provider who lacks trans-

---

[22] *See Transgender People Face Huge Barriers to Healthcare,* Consumer Reports, Nov. 20, 2020, https://www.consumerreports.org/healthcare/transgender-people-face-huge-barriers-to-healthcare/.

[23] *See L.G.B.T.Q. People Face Increased Risks From Covid, but Many Don't Want the Vaccine*, N.Y Times (Mar. 15, 2021), https://www.nytimes.com/2021/03/05/well/lgbtq-covid-19-vaccine.html

[24] *See* Transgender Resources, NYC.gov, https://www1.nyc.gov/site/doh/health/health-topics/transgender-resources.page; LGBT Health Services, CDC, https://www.cdc.gov/lgbthealth/health-services.htm; Transgender Resources, Ithaca Transgender Group, http://www.ithacatransgendergroup.com/transgender-resources.

competency can exacerbate a transgender patient's experience of gender dysphoria.[25] Having control over whether and when to share all aspects of one's prescription history is an important tool that facilitates many transgender and gender non-conforming people's navigation of discriminatory environments.

While one might assume that withholding PHI will lead to a lower quality of care, that is not necessarily true for many transgender and gender non-conforming people, and for other patient groups at risk of discrimination and other harms inflicted by healthcare providers. The value of withholding some information and what impact that withholding might have on the quality of care received can vary greatly depending on a given patient's needs and the type of care the patient is seeking.

For example, when a transgender person seeks a COVID test at an unfamiliar walk-in clinic and knows that they will be working with a new healthcare provider, they might not wish to disclose their transgender status or spend time educating providers on the necessity of medications related to transgender health. A transgender patient who is considering whether to wait in line for a COVID test might, after weighing their personal risk factors (including the possibility of experiencing a discriminatory event or heightened gender dysphoria caused by a provider who lacks transgender competency) opt to forego their visit. Foregoing healthcare entirely might be more likely if a patient lives in a region known to be generally hostile towards transgender people, or if the patient does not have the chance to establish a trusted, ongoing relationship with a healthcare practice. This example highlights how a patient's lack of control over whether they might be "outed" by their prescription history can lead to the avoidance of care, and subsequently a worse health outcome than if they were able to withhold access to this information. This example also illustrates how medication information related to transgender status is unlikely to be relevant to every type of care sought by the patient, and unlikely to result in a better quality of care in every setting.

While patient control over prescription history sharing cannot eliminate discrimination entirely, the current lack of patient control can clearly deter patients from seeking care and lead to a lower quality of care. Anti-discrimination laws are necessary but insufficient to address all health barriers. This is why the lack of patient consent requirement for sharing PHI relating to TPO and the lack of regulation of HIEs like Surescripts raises the barrier to healthcare for people with sensitive prescription drug histories.

---

[25] Gender dysphoria is a feeling of distress that can occur in people whose gender identity differs from their sex assigned at birth. Many, though not all, transgender and gender non-conforming people experience gender dysphoria. In a healthcare setting, this distress can be heightened by a provider who fail to use the pronouns that accords with a person's gender identity. For more information on gender dysphoria, see *Gender Dysphoria*, Mayo Clinic, https://www.mayoclinic.org/diseases-conditions/gender-dysphoria/symptoms-causes/syc-20475255#:~:text=Gender%20dysphoria%20is%20the%20feeling,some%20point%20in%20their%20lives.

III. Why Regulation Is Necessary and the Limitations of Self-Regulation

One problem with relying on self-regulation by HIEs is that HIEs are not consumer-facing products with which patients have direct contact. Therefore, how seriously HIEs take patient privacy is not subject to ordinary market pressures. This is particularly true when an HIE has a virtual monopoly, as Surescripts does. In such cases, there is no incentive for HIEs to provide a level of privacy beyond the bare minimum of what the law requires.

The following description of opting out from Surescripts Medication History is based on the lead author's experience and it illustrates the inefficiency and ineffectiveness of the opt-out process provided by the company.

For the average patient, the first obstacle in opting out of Surescripts' Medication History service is the lack of awareness of Surescripts' existence. Since Surescripts is not a product directly used by patients but a back-end network that is invisibly integrated with over nine hundred different e-prescribing software systems used by medical providers across the United States,[26] patients are unlikely to discover that their e-prescription history is held by Surescripts. (As noted above, the one-time notices that patients typically receive when they first visit a particular provider typically disclose, in very general terms, only that patients' PHI may be disclosed for TPO. The notices typically do not name Surescripts.) Because patients are guaranteed no notice of Surescripts' existence, they are most likely to learn of Surescripts only by asking their healthcare provider. If patients are lucky, the provider will share the name of the software the provider uses to access the patient's prescription records; if patients are luckier still, an inquiry to the software vendor might divulge information identifying the e-prescription network—likely Surescripts—that their software is integrated with.[27]

Unless and until patients know that Surescripts and its Medication History service exist, they are unlikely to encounter Surescripts' privacy statement on its website, which allegedly offers patients a method of opting out their prescription information. Patients discover Surescripts' privacy statement—and Surescripts' existence—only by asking. This process of learning about the entity holding one's prescription data is riddled with obstacles and assumes that the patient has sufficient technical knowledge to pose the right questions to their provider.

---

[26] *See* Find E-prescribing and HER Software for Providers, Surescripts, https://surescripts.com/network-alliance/eprescribing-prescriber-software.

[27] The lead author's experience discovering the entities that held and shared his medical data was an even more complex process than the one described in this hypothetical because both the clinic accessing his prescription information and the clinic that sent out his prescription did not understand his question when he asked for the name of their e-prescribing software vendor. One provider repeatedly provided the name "eRx," thinking that was the name of the software vendor, when in fact eRx is a generic description of e-prescription software. The provider lacked basic understanding of the technology the provider's own clinic was using. It took the author several weeks of looping through provider representatives—all reassuring him that they had done nothing wrong—before a pharmacy representative provided a tip that Surescripts was the likely source of his prescription data. It is very unlikely that all patients will invest the same amount of effort to trace the entities sharing their prescription data.

The process also assumes that the provider has sufficient technical knowledge to understand and answer the question.

If and when a patient discovers Surescripts and obtains Surescripts' privacy statement, more trouble awaits. Surescripts' opt-out process, as promised by its privacy statement, is also riddled with obstacles and can be ineffective.[28]

Surescripts' privacy statement suggests that patients can request to opt out of its Medication History service by contacting Surescripts' Privacy Officer at a designated email address. It can take several weeks before the paralegal administering the Privacy Officer's email account responds to an email requesting an opt-out.[29] The patient requesting an opt-out might eventually receive an email from the paralegal with an opt-out form, which is required to be notarized (which generally requires a fee) and to be sent to Surescripts only by paper mail (which often involves commuting to a post office and spending more money). Because Surescripts does not contact the patient with updates, the patient must then follow up via multiple emails about whether the paperwork has been received and whether it has been processed. When Surescripts eventually confirms to the patient that they have been successfully opted out of the Medication History service, the patient might discover months later that this is not true and that there is no other self-help remedy to safeguard their prescription data. (This is, in fact, precisely what happened to the lead author.)

Whether intentional or not, Surescripts' opt-out process is extremely complicated and appears to be designed to deter patients from opting out—if, in fact, they can opt out at all. There is no compelling reason why an opt-out request should need to be sent to Surescripts by paper mail when the opt-out form is sent to the requestor by email by the same paralegal who receives and manually processes the mailed-in paper opt-out form. There is no compelling reason to require patients to get their paperwork notarized, which requires additional time and funds. Given the slow response time from Surescripts the lead author experienced—and Surescripts failure to actually opt him out after he completed every step—it is likely that there is only a small staff (or even a single person) managing the opt-out process, and that very few resources are dedicated to processing opt-out requests. This process is immensely more burdensome than most of the straightforward and consumer-friendly opt-out procedures prevalent in 2021, such as clicking a link to unsubscribe from an email list.

HIEs like Surescripts have incentives to make opt-out difficult, even impossible, because there is economic value in having as much prescription history data available on their database as possible. The more patients' prescription histories Surescripts holds, the more likely a provider using software connected to Surescripts' network will find the Medication History function useful. The preceding personal account of Surescripts' broken opt-out process illustrates why we

---

[28] *See* Surescripts Privacy Statement, Surescripts. https://surescripts.com/our-story/privacy

[29] This account is a condensed version of one of the author's attempt to opt out of Surescripts' Medication History service in December 2020. As of April 14, 2021, he is still not opted out, and his new medical provider can access his prescription information directly from Surescripts.

cannot rely on industry self-regulation or self-help measures to safeguard patients' medical privacy. We need government regulation.

IV. Three Recommendations for New HIPAA Regulations

We recommend that HHS amend the HIPAA Privacy Rule to address this pressing problem. While HHS did not include such amendments in the Proposed Modifications of January 21, it should include them in the Final Rule or in any future revision of the HIPAA Privacy Rule. Here are three solutions to provide patients greater control over the sharing of their medical history.

First, we recommend that HHS reform 45 C.F.R. § 164.506 to require healthcare providers to obtain prior patient authorization before disclosing any protected health information, including information related to TPO. Absent a general rule requiring patient authorization, HHS regulation should at least require providers to provide individual patients an efficient way to opt out of sharing of their health information with any third party without prior authorization. If an opt-out consent model is adopted, the opt-out method must be simple for patients to understand, be of minimal or no cost to the patient, and be effective.

As an alternative solution, we recommend that HHS implement HIE-specific regulations. HIE-specific regulations would be less disruptive to existing norms of medical data sharing but would nonetheless protect patients from the privacy-invading prescription drug history sharing described above. An HIE-specific regulation could require healthcare providers to obtain patient consent prior to accessing or sharing their information to HIEs. New York State has a rule that could serve as a template. New York State law requires patient consent before patients' information can be accessed within New York State-regulated HIEs. The relevant state regulation, NYCRR tit.10, § 300.5(a), permits qualifying HIEs to provide participating healthcare providers with access to patient information only with written authorization from the patient.[30] The requirements of New York's rule are strong; the rule requires providers to adequately informs patients about the usage of their data in HIEs and provides patients with a clear and meaningful way to opt out. In light of the rule, providers have adopted much better consent forms and opt-out processes than Surescripts'. One example of an adequate HIE consent form can be found on the website of a New York-based healthcare provider, NYU Langone.[31] This consent form is a clearly written, stand-alone form that asks patients to explicitly check one of two boxes to either opt in or opt out of providers accessing their health information in the HIEs that are part of the New York statewide initiative. This form also clearly communicates to the patient that their choice to opt out will not affect their ability to receive medical care or health insurance coverage.

---

[30] *Id* (citing N.Y. Comp. Codes R. & Regs. tit.10, § 300.5(a)). One major limitation of this rule is that this rule applies only to defined "qualifying entities," which are HIEs certified by New York State to participate in a statewide initiative overseen by the New York Department State of Health. Thus, this rule does not apply to Surescripts. *See* N.Y. Comp. Codes R. & Regs. tit. 10, § 300.4 for qualified entities.

[31] *See* Health Information Exchange Consent Form, NYU Langone, https://perma.cc/3F52-84RZ.

Though less ideal, a third possible solution would be to impose heightened restrictions on disclosure for some classes of prescription information, such as information that reveals sensitive health statuses that subject patients to greater risk of discrimination or deter patients from seeking care. This solution is less than ideal because all prescription information is arguably of a sensitive nature, and it can be difficult to identify which classes of medication can potentially reveal a health status that heightens a patient's risk of discrimination. However, this solution would potentially allow for greater information flow among providers without requiring their patients' prior consent, which might be in the providers' interest.

While HHS has not incorporated any of these recommendations in the Proposed HIPAA Rule published on January 21, HHS should carefully consider incorporating them into the final rule or in any future revision of the HIPAA Privacy Rule.

V. Conclusion

While there are many social and economic benefits to the growth of HIEs, it is important that patients, especially those with sensitive health information, be part of the conversation over how to govern the information that flows through HIEs. Patients with sensitive medical information, especially those subject to heightened risk of discrimination, should control access to their medical information. The lack of control over medical data deters people from seeking care and further compounds existing healthcare inequities. We urge HHS to reform 45 C.F.R. § 164.506 as we have recommended in this comment.

Thank you for the opportunity to submit this comment.

Sincerely,

/s/ Ethan Lin

Ethan Lin
NYU School of Law, '21
NYU Technology Law & Policy Clinic

Christopher Morten
Deputy Director
NYU Technology Law & Policy Clinic

Brett Max Kaufman
Adjunct Clinical Professor
NYU Technology Law & Policy Clinic

Jason Schultz
Director
NYU Technology Law & Policy Clinic