NOVEL PRIVACY CONCERNS IN HEALTHCARE ANTITRUST

BY ANDREW STIVERS, EMILY WALDEN & SUBRAMANIAM RAMANARAYANAN[1]



1 Andrew Stivers and Emily Walden are Associate Directors in NERA's Antitrust and Competition Practice. Subramaniam Ramanarayanan is Chair of NERA's Healthcare Antitrust Practice and a Managing Director.

CPI ANTITRUST CHRONICLE MAY 2022

Visit www.competitionpolicyinternational.com for access to these articles and more!

NOVEL PRIVACY CONCERNS IN HEALTHCARE ANTITRUST

By Andrew Stivers, Emily Walden & Subramaniam Ramanarayanan

Healthcare antitrust practitioners are grappling with the increased value and prominence of patient data in competition. In many respects, this data can be examined using traditional antitrust concepts. However, antitrust authorities and other stakeholders have also raised questions about consumers' interests in mergers, or other competition practices from a privacy perspective. Privacy advocates have identified a range of possible welfare effects stemming from the commercial collection and use of personal data. Four of these – price discrimination, data security, intrinsic value and autonomy – seem likely to also be applied in some form to antitrust with varying degrees of overlap with traditional consumer welfare analysis. We examine these issues in the context of healthcare, but the analysis is likely to apply similarly to other areas of antitrust.

Personal health information that flows from patients and potential patients to providers and payers is an essential input to patient care and adjudication of payment. Those flows are also increasingly useful as inputs for improving the underlying technology and efficiency of healthcare delivery and as inputs for marketing and competition in the healthcare sector (finding and competing for customers). Because of its increased importance in both quality of service and in competition, antitrust regulators have been scrutinizing how proposed mergers and unilateral practices might affect that data landscape.

On one hand, this may simply mean ensuring that traditional antitrust analysis is applied to a firm's control of data assets and incentives for their use. Antitrust authorities have been signaling their heightened interest in digital markets and non-price attributes.[2] They have also been pushing to expand the scope of antitrust enforcement. That trend, with the concurrent rise in concern about privacy, and regulatory scrutiny of consumer data flows in general, have created some debate and confusion about how antitrust should be applied to patient data.[3]

As part of that debate, researchers have examined the specific privacy implications. For example, Price and Cohen lay out some of the challenges to privacy in the context of "medical big data."[4] Savage, Gaynor and Adler-Milstein examine how privacy and competition interact and may interfere with each other in the context of data security.[5] However, how antitrust intersects with consumer privacy interests, as foundational to the increasing range of global regulations and declarations of consumer rights over their data, has not been clearly articulated. This paper identifies four areas **– price discrimination, data security, intrinsic value and autonomy –** where competition and market structure may affect those interests that are novel to antitrust, and distinct from the traditional analysis of firm assets as applied to data.

I. FLOW OF HEALTHCARE DATA IN THE U.S.

Healthcare provision in the U.S. typically generates two overlapping but distinct streams of data relating to patients and their care. Electronic medical records ("EMR") are generated with a focus on clinical decision-making and practices. Business and claims data, often referred to by the underlying electronic data interchange ("EDI"), are generated with a focus on utilization management, payment administration and coverage.

An EMR is a digitized version of a patient's medical chart populated by the patient's provider, but often administered by a third-party vendor. That data includes "key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports."[6] These data are often accessible to the patient and providers via an online portal. Estimates suggest that 90 percent of providers have an EMR system.[7]

One of the key potential benefits of EMR use is improvement in clinical care quality, which may take place through a number of mechanisms, including decision support, information management, and care coordination.[8] EMRs enable providers to use decision support algorithms to prevent errors and follow care guidelines. For example, EMRs can allow a provider to check for drug allergies or interactions. EMRs may also facilitate information management, which can help providers monitor and diagnose patients with complex conditions. EMRs may improve coordination of care across providers and care settings, which can reduce errors, reduce duplication, and enable decision making. Empirical research suggests that EMRs may be successful at improving clinical care quality. Literature reviews have found that over half of empirical studies from 2007 to 2013 found a positive relationship between EMRs and quality of care compared to only about ten percent that found a negative relationship.[9]

2 FTC Virtual Press Conference for Merger Guidelines RFI Joint Announcement, Jan. 18 2022. https://www.ftc.gov/media/80865.

3 See, for a discussion: Douglas, Erika M. "The New Antitrust/Data Privacy Law Interface." Yale LJF 130 (2020): 647.

4 Price, W. Nicholson & I. Glenn Cohen. "Privacy in the age of medical big data." Nature Medicine 25, no. 1 (2019): 37-43.

5 Savage, Lucia, Martin Gaynor & Julia Adler-Milstein. "Digital health data and information sharing: A new frontier for health care competition." Antitrust LJ 82 (2018): 593.

6 https://www.cms.gov/Medicare/E-Health/EHealthRecords.

7 CDC National Center for Health Statistics, "2019 National Electronic Health Records Survey public use file national weighted estimates" https://www.cdc.gov/nchs/fastats/electronic-medical-records.htm.

8 Atasoy, Hilal, Brad N. Greenwood & Jeffrey Scott McCullough. "The digitization of patient care: a review of the effects of electronic health records on health care quality and utilization." Annual review of public health 40 (2019): 487-500.

9 Buntin MB, BurkeMF, Hoaglin MC & Blumenthal D. 2011. The benefits of health information technology: a review of the recent literature shows predominantly positive results. Health Aff. 30:464–71; Jones SS, Rudin RS, & Perry T, Shekelle PG. 2014. Health information technology: an updated systematic review with a focus on meaningful use. Ann. Intern.Med. 160:48–54.

EMR use can also improve clinical care efficiency and convenience. For example, providers can also use EMRs to send automated reminders to patients to get vaccinations or manage chronic conditions. EMR systems that track test results can also help providers avoid duplication of lab work and imaging. EMRs also provide convenience for patients by allowing them to access their medical records electronically rather than having to request paper records from their providers.

Because of all these potential benefits, government agencies have invested heavily in attempting to lower barriers to the flow of patient information to providers through subsidies and requirements for EMR adoption. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") provides a framework for establishing a protected space within which providers, payers and claims processors have relatively few regulatory limits on patient health information flows for treatment, administrative, and quality improvement purposes. This is consistent with an underlying presumption that patients are best served with very little privacy with respect to their providers', payers', and related processors' access to protected health information ("PHI") within the EMRs. Similar rules apply to the flow of EDI data to the extent it contains PHI.

EDI data in the context of health care refers to data relating to insurance coverage, claim adjudication, and payment. As its name implies, EDI data containing information on healthcare utilization and payment requests flows from providers through clearinghouses to the various payers - often to multiple firms as adjudication of payment is resolved. As a business focused system, the most direct potential benefit to consumers of EDI is in greater efficiency adjudicating and processing payments. Like EMR, claims and payment data can be used to develop automated decision tools, which in turn can analyze incoming data for inaccuracies, incompleteness, or fraud. An ability to cross-reference EDI data with EMR may allow more complete coding of patient conditions, which in turn may lower the cost of providing service to ACA or Medicare patients. De-identified data can be aggregated and used in-house or sold for business intelligence purposes.

Due to the personal and confidential nature of PHI contained in both EMR and EDI data, breaches are a significant risk of health information systems. This PHI is protected under HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act. HIPAA requires that PHI is protected with administrative, physical, and technical safeguards, while the HITECH Act prescribes a protocol for dealing with data breaches.[10]

II. TRADITIONAL ANTITRUST CONCERNS (INTERSECTING WITH CONSUMER DATA, BUT NOT "PRIVACY" CONCERNS PER SE)

The most well-articulated data-related antitrust concerns revolve around whether a firm has either exclusive control over certain kinds of essential data or has the scope and scale of access that yields uniquely valuable insights from such data.[11] A related concern may be that a firm serving as a third-party platform with access to rivals' EMR or EDI data could take unfair advantage of that access and utilize it for its own benefit.

As the research has shown, simple knowledge of data possession does not imply that one can draw any conclusions about anticompetitive effects. This is so for many reasons relating to the nature of the data and the context of its use, including contractual and regulatory controls. For example, the data at issue may not be unique, and similar (or identical) information may be available through other sources. This implies that even if a firm is trying to prevent access to its own flows or stores of essential data, rivals may not necessarily be harmed. As an example, if the essential data issue pertains to access to providers' information on healthcare claims, similar data may be accessed through the purchase of all-payor claims datasets made available by various states. Some essential pieces of information, like pricing or reimbursement of services, may also be publicly available through efforts such as CMS' price transparency initiative.[12]

In the context of access to data, unilateral conduct could raise concerns if such conduct were to adversely impact competition by a vertically integrated firm's refusal to provide essential data (or derivative downstream products) to rivals, or if the firm were to provide lower quality data inputs to rivals. In such cases, the incentive of the firm to engage in such conduct would be evaluated by the extent to which the data that rivals are being foreclosed from (or paying higher prices for) are unique, and not available from other sources such that these rivals would rather pay a higher price (or accept lower quality data) rather than switch vendors (which would result in a loss of revenues to the integrated firm). In

10 Kruse, Clemens Scott, Brenna Smith, Hannah Vanderlinden & Alexandra Nealand. "Security techniques for the electronic health records." Journal of medical systems 41, no. 8 (2017): 1-9.

11 See for example: Sokol, D. Daniel & Roisin E. Comerford. "Does antitrust have a role to play in regulating big data?." Cambridge Handbook of Antitrust, Intellectual Property and High Tech, Roger D. Blair & D. Daniel Sokol editors, Cambridge University Press, (2017); Tucker, Catherine. "Digital data, platforms and the usual [antitrust] suspects: Network effects, switching costs, essential facility." Review of industrial Organization 54, no. 4 (2019): 683-694; Hagiu, Andrei & Julian Wright. "When data creates competitive advantage." Harvard business review 98, no. 1 (2020): 94-101; Competition and Markets Authority, "Online platforms and digital advertising market study" (2020);

12 https://www.cms.gov/hospital-price-transparency.

addition, the incentives for the firm also depend on the extent to which these data may be truly integral to determining the quality of the services offered by rivals. It is important to recognize that there may be important scale-related benefits that may flow from the possession of larger amounts of data. Such greater volumes of data allow for richer analysis and the ability to draw more informative conclusions.

The above potential issues are relatively new in terms of their importance to antitrust analysis because of the massively shifted economies of data collection, storage and processing in recent years and have generated significant attention from researchers and regulators in applying the lessons of well-understood antitrust concerns. However, none of these raise novel issues specific to "privacy."

III. IMPLICATIONS FOR PRIVACY

In part because of the close, and highly regulated, relationship between healthcare provision and patient health information flows, there seems to be little widespread competition for privacy attributes in the healthcare space. However, there is also limited consumer-driven competition for privacy attributes in many other sectors – particularly online – where personally related data flows are necessary to transact. The retention and use of that data beyond the transaction are often opaque and feedback effects to the consumer are often diffuse.[13] Combined with preference heterogeneity and seeming indifference for many consumers, this means that privacy attributes often lack salience, demand may be unresponsive to changes in privacy-relevant attributes, and thus incentives to compete in this area are muted, at best.[14]

That said, shocks to consumer/patient beliefs about PHI data flows could plausibly lead to demand effects (including how willing patients are to provide their information), and as a result, firms may have incentives to conceal changes to the PHI data flows that risk triggering such demand effects. Similarly, and perhaps more importantly, shocks to consumer/patient beliefs could lead to regulatory backlash, which in turn could significantly restrict the existing data flows. Much of the recent change in privacy and data security practices across the market have been driven by nascent regulation.

If consumers are generally unresponsive to privacy attributes so that firms are not generally competing on those attributes without regulatory nudges, where does that leave us in the context of antitrust practice?

The antitrust policymakers at the state, federal and global levels have signaled their interest in reforming antitrust practice, with a particular interest in the aggregation of very large datasets and control of significant data flows as potentially anticompetitive tools. In addition, these policymakers have indicated an interest in broadening the scope of antitrust practice to deal with social issues beyond those directly implicated by the market. The form of that scope increase will take is as yet unknown but may include both changes to the antitrust framework itself and attempts to leverage antitrust regulatory gatekeeping as a way to influence company practices in other areas.

Either way, privacy is likely to be important to this debate, and here we focus on the following question:

> *What are potential/alleged privacy harms in healthcare that policymakers may try to alleviate – or already have rules in place to address – but that mergers or acquisitions might exacerbate?*

Privacy interests – or preferences, as economists conceptualize them – are idiosyncratic and context specific. People may experience concrete feedback effects or simply have strong preferences about how personal health information flows to, and is controlled and used by, payers, providers, and processors. To the extent that these interests are related to competitive or anti-competitive effects, they are generally understood to be captured by consumer welfare changes stemming from price or non-price attributes.

At least some consumers appear to have demand-relevant incentives and preferences for privacy-related attributes of the products and services that they purchase. We discuss four of the major potential concerns that could raise the cost of healthcare consumption. These are: future bargaining/discrimination concerns stemming from current PHI collection; data security concerns that unauthorized parties may gain access to PHI; intrinsic concerns relating to preferences about how PHI flows or is used independent of feedback effects; and autonomy/social concerns that are more diffuse in effect and may also be attenuated from immediate market choices.[15] To the extent that these concerns are salient, they may shift patient's valuation of health care because the flow of PHI is bundled closely with that consumption.

13 Jin, G.Z. & Stivers, A., 2017. Protecting consumers in privacy and data security: A perspective of information economics. Available at SSRN 3006172.

14 Acquisti, A., Taylor, C. & Wagman, L., 2016. The economics of privacy. Journal of economic Literature, 54(2), pp.442-92.

15 Others have offered more granular taxonomies, see, for example Citron & Solove "Privacy Harms" for an exhaustive list of the possible ways data flows could harm.

As noted, any actual effect on demand is likely to be both a function of idiosyncratic preferences and variable due to patient circumstances, knowledge, and beliefs about how PHI flows through the healthcare system. While, as noted above, aggregate demand effects in general may not be measurable, privacy advocates have argued that underlying consumer/patient interest in these flows are nonetheless strong enough to warrant significant interventions. Below, we examine each area of concern more closely.

1. Bargaining/Discrimination Concerns

One concern is that market actors with access to PHI could use it to differentially worsen patient bargaining positions or deny them access to coverage or care. In a health care setting, this could come at the point of insurance plan offerings or at the point of care decisions, delivery, and payment. Conceptually, a payer may have incentives to exclude riskier individuals or cohorts from coverage to reduce their costs. More information – less privacy – about potential members could allow a payer to identify riskier membership pools, and avoid, or soften, competition for those pools, which would tend to reduce availability and increase price for the affected population.

A merger could enhance a healthcare firm's bargaining position or ability to deny patients coverage through access to the other merging party's PHI (as each firm necessarily has access to PHI about its own customers). To some extent this issue is already covered under existing antitrust theories. First, most effects on consumers will be mediated through price, availability, and quality of care, which are well-understood effects of mergers in health care. Second, health data flows and discriminatory practices are both subject to significant existing regulatory control in health care. A potential new issue is whether patient fears of future bargaining effects would materially affect their willingness to seek care or share information with healthcare providers. If so, patient outcomes may be worse following the merger. We discuss each of these issues below.

In practice, the regulatory infrastructure in healthcare insurance is sensitive to the potential incentives to discriminate against sicker and more costly individuals or cohorts. For example, Medicare Advantage ("MA") and Affordable Care Act ("ACA") plans are subject to risk adjustment payments that are designed to reduce the incentives for discrimination in membership pools. Payers serving less risky populations in a geographic area pay in, and payers with more risky populations get pay outs. These risk adjustments are based on diagnostic coding that provide a proxy for the expected cost of providing health care to the payers' plan members.

For MA enrollees, the relevant diagnoses come from the previous year and CMS keeps a complete history of a beneficiary's diagnoses. This complete history is available to any payer serving that beneficiary, meaning that a MA enrollee's risk adjustment score will follow them if they change plans. A payer's ability to completely code for risk of an MA enrollee is in part a function of its technology for scanning claims and medical records for uncoded diagnoses. For ACA plans, risk adjustment is based on the current year's diagnoses, and an insurer will not necessarily have access to claims from prior insurers. That means that both available technology and increased access to pre-enrollment medical records and claims could influence the desire of a payer to insure a patient in the first place.

For both ACA and MA markets, the risk adjustment system means that payers have incentives to encourage complete coding to maximize their likelihood of payment from, rather than into, the risk adjustment system. In both markets more complete coding and thus increased risk adjustment subsidy for a population would allow more aggressive pricing. These incentives to completely code are especially acute for ACA plans, because risk adjustment payments are zero sum.

The existing regulatory framework to control such effects outside the antitrust apparatus likely means that greater access to data stemming from acquisitions may have ambiguous effects on price, quality, and coverage, holding market power concerns constant. To the extent that prices or quality of care are implicated in some way by increased access to patient data, the welfare effects of any such changes would typically be considered as part of a standard merger analysis. That is, they may arguably be privacy related in that they stem from use of PHI, but they are not different from price or quality effects that arise from other factors in the merger analysis.

Finally, one area that may deserve more study is whether the intensity of PHI data flows are affected. That is, whether consumers, in anticipation of future discrimination, significantly reduce the amount of information they provide through their healthcare service.[16]

2. Data Security Concerns/Personal Risk

In addition to concerns about how "authorized" users of PHI may use that data against patients' interests, concentrated repositories of PHI may create greater risk of data breaches and unauthorized use. The persistence and proliferation of PHI may increase the likelihood of a data breach by non-market actors that negatively affects patients. The business of providing coverage and care and adjudicating payment involves significant collection, sharing and use of PHI, whether from EMRs or claims data. Data security is never certain, and breaches across all types of players

16 Conitzer, Vincent, Curtis R. Taylor & Liad Wagman. "Hide and seek: Costly consumer privacy in a market with repeat purchases." Marketing Science 31, no. 2 (2012): 277-292.

in this sector have demonstrated the vulnerability. In addition to the risks associated with breached personally identified data generally – from SSNs, CCNs, and other identifying information that could be used for ID theft – breached PHI may increase risk of injury through embarrassment or negative social, employment, or other ill effects.

The effect of a merger or acquisition that increases access to patient data is generally ambiguous even if the merger is otherwise found to increase market power. First, as discussed above, data security is not necessarily a driver of competition. Second, a firm's own interest in protecting its assets – which would increase if data were a significant factor in a merger – may actually increase investment in data protection. Consolidation of processing may reduce threat surfaces for attack. On the other hand, such consolidation, and the potentially greater intensity of collection, may also create the perception of a richer target, and therefore increase incentives to attack. Finally, regulatory pressure (including indirectly through data partners' concerns about regulatory liability) may drive data security practices independent of competition issues.

3. Intrinsic Concerns

Patients may have preferences over the flow and use of personal health information independent of any feedback mechanism.[17] This means that some individuals may feel themselves to be worse off for an almost limitless set of reasons, including almost any detail of the flow of PHI, and incorporation of data related to them in the development of products or services. These are the most difficult to articulate and estimate, as they need not have any external reference or mechanism to benchmark to, at least in part because there is relatively little market data on how consumers might value such things.

4. Autonomy Concerns

Consumer interest in competitive effects themselves are not typically understood to enter preferences directly. However, critics of recent antitrust practice have argued that ill effects of mergers and acquisitions are not limited to consumer welfare calculations but extend to individual and societal autonomy and control. This concern has been specifically extended to large firms' access to and use of data related to individuals.[18] To the extent that these concerns arise socially and politically, they are even less likely to be considered at the individual demand level. Given the extensive regulatory structures outside of antitrust that attempt to manage the social benefits and costs of health care generally, and healthcare data in particular, it is not clear that concerns about autonomy related to patient data should, or will, fall to antitrust enforcement. Even if they do, the question of how antitrust regulators and the courts would attempt to incorporate these issues in merger review is unresolved, and if addressed, is likely to be on an *ad hoc* basis.

IV. DISCUSSION

Antitrust practitioners are grappling with the increased value and prominence of consumer data in competition and market strategy. As assets and important inputs into business decisions, consumer data can be examined using well-understood, traditional antitrust concepts of raising rival's costs or refusal to deal. However, antitrust authorities and other stakeholders have also raised additional questions about consumers' interests in their data from a privacy perspective, and whether there are antitrust implications specific to privacy. Privacy advocates have identified a wide range of possible welfare effects stemming from the commercial collection and use of personal data. Four of these – price discrimination, data security, intrinsic value and autonomy – have been prominent in the privacy debate. As such, they seem likely to also be applied in some form to antitrust analysis with varying degrees of overlap with traditional consumer welfare analysis. Here, we have examined these issues in the context of healthcare, but the analysis is likely to apply similarly to other areas of antitrust.

Price discrimination comports most closely as a part of market power analysis that may be amplified by the presence of data, but the potential feedback effect from consumers' willingness to share data may need to be assessed. Data security represents a more complicated issue, with the relationship between market power and data security risk ambiguous. In addition, accounting for external risks outside the relevant markets amplifies that complication. Intrinsic valuation similarly adds complexity, with consumers potentially having strong preferences about the state and flow of personal data, independent of any directly measurable affects. Market data for assessing the presence of such preferences is scarce and difficult to generate. Finally, there may be diffuse, non-market concerns about individual autonomy at a societal level that present another leap in the difficulty of assessing and thus applying a consistent analytical framework to individual antitrust matters.

17 Lin, Tesary. "Valuing intrinsic and instrumental preferences for privacy." Available at SSRN 3406412 (2019); also Joseph Farrell, "Can Privacy Be Just Another Good?" 10 Journal on Telecommunications and High Technology Law 251, 252-53 (2021).

18 Shoshana Zuboff, The Age of Surveillance Capitalism. Profile Books, 2019.

CPI COMPETITION POLICY™ INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.