Regulatory Disruption and Arbitrage in Healthcare Data Protection*  

Nicolas P. Terry**

I. Introduction

II. Background: Key Characteristics of U.S. Data Protection 4  
   A. Sectoral Data Protection 5  
   B. Upstream vs. Downstream Protection Models 7  

III. Regulatory Turbulence, Disruption & Arbitrage 11  
   A. Turbulence and Disruption 11  
   B. Arbitrage 15  
   C. Implications of Regulatory Disruption and Arbitrage 17  

IV. Exceptionalism and the Healthcare Data Protection Model 17  
   A. Sectoral Model 18  
   B. Downstream Protection Favored 20  
   C. Understanding Exceptional Healthcare Data Protection 23  
      1. History of Exceptionalism 24  
      2. Health Subdomain Exceptionalism 26  

V. Turbulence, Disruption, and Arbitrage in Practice 29  
   A. Professional Healthcare Domain vs. Consumer Domain 29  
   B. Example One: Big Data 33  
   C. Example Two: Mobile Health Data 37  

VI. Data Protection versus Data Liquidity 39  
   A. Clinical Interoperability 39  
   B. Medical and Population Health Research 41  
   C. Refuting the Binary 42  

VII. Responding to Disruption and Arbitrage in Healthcare Data Protection 43  
    A. When to Regulate, Leading Edge or Trailing Edge? 43  
    B. A Different Type of Laboratory, the States 45  

* © 2016 Nicolas Terry. All rights reserved.  
** Hall Render Professor of Law, Executive Director, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law. Email: npterry@iupui.edu. Frank Pasquale and Craig Konnoth were generous with their time in commenting on an early draft. I also thank all the workshop participants at the 2015 Amsterdam Privacy Law Scholars Conference.
I. Introduction

In 1994, two years before passage of the statute that authorized the HIPAA privacy and security rules, the Institute of Medicine (IoM) took the position that “legislation should clearly establish that the confidentiality of person-identifiable data is an attribute afforded to the data elements themselves, regardless of who holds the data.”¹ That exhortation was ignored and policymakers’ persistent, systemic failure to safeguard healthcare data outside the HIPAA domain is now exemplified by the minimal, sub-HIPAA data protection afforded healthcare data either held by data brokers or created by mobile apps and wearables outside of the conventional health care space.

The result of this policy misstep is an emerging narrative of regulatory disruption, and arbitrage. Simply put, disruption and arbitrage can occur when disruptive businesses in a lightly regulated domain create products previously associated with highly regulated domain incumbents. This is not just another story of emerging technologies exposing the lamentable state of data protection in the U.S. It is also an account of the deprecation of a healthcare-specific policy position that was hard won and as yet has not been refuted with any conviction. Historically, healthcare in the U.S. has benefited from domain-specific privacy exceptionalism. As a result, conversations about mainstream data protection have tended to ignore, even isolate healthcare, viewing the domain as sui generis and more than

---

adequately protected by the HIPAA Privacy and Security Rules.\textsuperscript{3} its specialized regulatory schemes such as HIPAA and state law analogues. HIPAA has been one of the most consistently criticized regulatory constructs.\textsuperscript{4} Yet, its levels of data protection and enforcement likely would provoke avarice from data subjects in other domains. Here, the complex nature of healthcare data protection exceptionalism is explained and defended.

They key to understanding current disruption and arbitrage is an appreciation of U.S. data protection and, obviously, its particular application to healthcare. While the sectoral nature of U.S. healthcare is generally understood, other properties such as the distinction between upstream and downstream data protection models may not be so well-known. Comprehension of multiple data protection models informs the current declining state of healthcare. Equally, understanding multiple models is helpful in refuting over-simplified binaries (for example, privacy vs. data liquidity) and provides insight into potential data protection reforms.

Two examples of regulatory disruption and arbitrage inhabit the analysis that follows. First, healthcare data collected, analyzed and sold by big data brokers. Some of those data are created within the highly regulated space but legally “exported” (for example they may have been deidentified). Other big data are medically inflected, created outside the highly regulated healthcare domain but once combined with other data points operate as data proxies for protected HIPAA data. In both scenarios data triangulation may defeat any deidentification. Second, wellness, fitness, and sickness data increasingly are created on mobile health platforms or by mobile health apps. Again, the picture is complicated (hence the disruption). Some data are created in a highly regulated space but then exported to a mobile device; other data are processed in the opposite direction.


The article takes the position that healthcare data exceptionalism remains a valid imperative and that even current concerns about data liquidity can be accommodated in an exceptional protective model. However, re-calibrating our protection of healthcare data residing outside of the traditional healthcare domain is challenging. A hybrid model is envisioned with downstream HIPAA model remaining the dominant force within the healthcare domain, but being supplemented by upstream and point-of-use protections applying to healthcare data in disrupted spaces.

II. Background: Key Characteristics of U.S. Data Protection

The dysfunctional nature of U.S. data protection is ironic given its often-heralded roots. Warren and Brandeis’s famous Harvard article,\(^5\) has achieved mythic fame for birthing its eponymous “Right to Privacy.” However, looking back at their article today it is striking to see the relatively narrow driver that led these famous lawyers to propose the recognition of the “right to be left alone.”\(^6\) Primarily, they seemed concerned about some members of the press (perhaps, in today’s terms, the paparazzi) and what the authors viewed as an inappropriate appetite for gossip and triviality.\(^7\) Indeed, Jill Lepore has described the article, “a manifesto against the publicity of modernity.”\(^8\) Today the article’s “Right to Privacy” title plays better than its substance and, perversely, that title now exists merely as a slogan inaccurately preserving the myth of strong U.S. data protection. Those seeking the source of the contemporary data protection debate are more likely to find it, albeit accompanied by dystopian contexts, in Alan Westin’s 1967 Privacy and Freedom or his 1972 preview of today’s data broker issues, Databanks in a Free Society.

With no little irony given the healthcare context of this paper, it was the U.S. Department of Health, Education, and Welfare (HEW), a precursor to the Department of Health & Human Services (HHS), which conceived the amelioratory legislation that was to follow.\(^9\) The HEW report discussed both government and non-governmental information practices\(^10\) and outlined one

\(^{6}\) Warren & Brandeis at 195.  
\(^{7}\) Warren & Brandeis at 196.  
\(^{10}\) Id., at 33-46.
of the first iterations of Fair Information Practice Principles (FIPPs). The tragedy was that report only recommended, and Congress only enacted, privacy legislation to control the data collecting practices of the federal government. Many of the issues discussed in this article can be traced back to this Pyrrhic victory, the Privacy Act of 1974. What Frank Pasquale has termed U.S. privacy law’s “original sin” was the failure to embrace a comprehensive rather than piecemeal approach to data protection.

A. Sectoral Data Protection

Thereafter, as acknowledged by the 2012 White House report, “most Federal data privacy statutes appl[ied] only to specific sectors, such as healthcare, education, communications, and financial services or, in the case of online data collection, to children.”

As is well known the Gramm–Leach–Bliley Act (GLBA) governs consumer privacy in the financial sector. GLBA, like HIPAA, is sectoral, applying to narrowly defined data custodians, specifically groups of financial entities. Just as HIPAA does not apply to all custodians of healthcare data, so GLBA does not apply to all who hold consumer financial data. And like HIPAA, GLBA is a downstream data protection model that erects a duty of confidentiality and requires notice to consumers of an institution’s privacy policies and practices. The FTC enforces the Fair Credit Reporting Act (FCRA) against consumer reporting agencies against narrow data quality,
transparency, and access.\textsuperscript{19} Other examples cover still narrower sectors such as video rental records.\textsuperscript{20} Even now, with the sectoral approach to data protection understood as causing severe regulatory gaps, calls for narrowly focused “fixes” continue, whether to protect student records from big data brokers\textsuperscript{21} or to prevent automobiles from “spying” on their drivers.\textsuperscript{22}

This sectoral limitation of substantive law spills over into rule making and enforcement. Inter-agency cooperation has never been a core strength of the federal government and regulatory gaps likely are exacerbated by turf wars. It is one thing not to have a comprehensive privacy model, it is another not to have a single data protection agency. For example, the European Union has had a (relatively) uniform law since 1995.\textsuperscript{23} The forthcoming General Data Protection Regulation\textsuperscript{24} has attracted interest because of its erasure\textsuperscript{25} and breach notification\textsuperscript{26} provisions. However, arguably its primary goal is to make enforcement and interpretation more consistent by designating a primary, “one-stop shop,” regulator\textsuperscript{27} and promoting additional coordination through the European Data Protection Board.\textsuperscript{28}

Of course, the observation that U.S. data protection is flawed because of its sectoral nature is only part of the story. The sectors (even healthcare) are narrowly defined and after conventional health and, arguably,\textsuperscript{29} financial services the drop off in protection is sharp. In large part this is because the

\textsuperscript{19} 15 U.S.C § 1681 et seq.
\textsuperscript{24} http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (this document does not yet synthesize the various changes required by other EU institutions, a documented expected in late 2015).
\textsuperscript{25} Id. Art 17
\textsuperscript{26} Id. Arts 31-32
\textsuperscript{27} Id. Arts 51-57
\textsuperscript{28} Id. Arts 64-72
U.S. has favored relatively low protection models, most of which are downstream. However, sectoral protection is itself damaging. Sectoral models inevitably encourage differential levels of protection and a race to the bottom rather than the top. Worse, high levels of protection can be characterized as outliers and targeted for “reform.”

B. Upstream vs. Downstream Protection Models

The upstream-downstream typology described here may appear somewhat complex. However, it’s origins can be traced to a much simpler relationship—that between privacy and confidentiality. According to Tom Beauchamp and James Childress:

> [A]n infringement of a person’s right to confidentiality occurs only if the person or institution to whom the information was disclosed in confidence fails to protect the information or deliberately discloses it to someone without first-party consent. By contrast, a person who, without authorization, enters a hospital record room or computer database violates rights of privacy but does not violate rights of confidentiality. Only the person or institution who obtains information in a confidential relationship can be charged with violating rights of confidentiality.\(^30\)

This description captures a clear process chronology. First, “privacy” protects against unauthorized collection of healthcare data. Subsequently, once the collection has been authorized, the recipient subsequently owes a duty of “confidentiality” not to disclose the data. That is, privacy (different flavors of which either prohibit or place limitations or conditions on the collection of data) protects data upstream of confidentiality.

\(^{30}\) **Tom L. Beauchamp and James F. Childress, Principles of Biomedical Ethics, 316-17 (7th ed 2013).** See also Humphers v. First Interstate Bank of Oregon, 298 Or. 706, 711-12 (1985), noting:

> Although claims of a breach of privacy and of wrongful disclosure of confidential information may seem very similar in a case like the present, which involves the disclosure of an intimate personal secret, the two claims depend on different premises and cover different ground, .... the most important distinction is that only one who holds information in confidence can be charged with a breach of confidence. If an act qualifies as a tortious invasion of privacy, it theoretically could be committed by anyone.
Thus, the lifecycle of data can be mapped to a timeline-based typology. That typology may be expanded beyond “privacy” and “confidentiality” to include other data protective models. In broad terms models that are applicable before or during collection are labelled “upstream,” while those applied post-collection are “downstream.”

To privacy (upstream) and confidentiality (downstream) I now add some other basic data protection models (which may or may not be deployed by ethical, legal, or technological systems) such as anonymization, breach notification, inalienability, point-of-use regulation, or security.

Anonymizing data prior to any collection or using something like an inalienability or market inalienability rule to reduce the use case/value of the data will tend to reduce the likelihood that the data are collected.

<table>
<thead>
<tr>
<th>Upstream Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
</tr>
<tr>
<td>Anonymization</td>
</tr>
<tr>
<td>Inalienability</td>
</tr>
<tr>
<td>Privacy</td>
</tr>
</tbody>
</table>

In contrast, point-of-use regulation (such as the prohibition of discriminatory uses), security, and breach notification are downstream, post-collection protective models.

<table>
<thead>
<tr>
<th>Downstream Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
</tr>
<tr>
<td>Point-of-Use Regulation</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Confidentiality</td>
</tr>
<tr>
<td>Breach Notification</td>
</tr>
</tbody>
</table>
This basic upstream-downstream relational structure may now be expanded to include other protective sub-models and also crosswalked to FIPPS.\textsuperscript{31}

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Data Protection Model</th>
<th>Sub-Models/FIPPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream</td>
<td>Anonymization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inalienability</td>
<td>Market Inalienability\textsuperscript{32}</td>
</tr>
<tr>
<td></td>
<td>Privacy (Broad Control of Collection)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Control/Consent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Purpose Specification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Minimization/Proportionality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparency</td>
<td></td>
</tr>
<tr>
<td>Downstream</td>
<td>Right of Erasure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>De-linking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Point of Use Regulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-discrimination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limited to purpose of collection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accounting/Audit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quality &amp; Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality (Broad Control of Disclosure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use Limitation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quality &amp; Integrity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>De-Identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prohibitions on Reidentification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access/Accuracy/Correction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accounting/Audit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Breach Notification</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{31} This synthesis is loosely based on the language provided in 2012 White House, Appendix B: Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles (FIPPs).

\textsuperscript{32} See generally Margaret Jane Radin, Market-Inalienability, 100 HARV. L. REV. 1849 (1987).
This more complex representation also reflects that some protections (for example transparency or, where they overlap, anonymization and deidentification) can occur at multiple times in the lifecycle of the data. Note also that some sub-models are complimentary; for example, the upstream privacy (collection) sub-model that prohibits collection of data other than for a disclosed purpose would likely be complemented by a downstream, prohibition on disclosure other than for the stated purpose.

I suggest several interrelated takeaways from this typology. First, and most obviously, policymakers (or, for that matter, data custodians) can and should choose from a broad array of data protection models. Having a comprehensive toolbox should help regulators finely calibrate their approach to particular data risks and help them be prepared to deal with evolving or as yet unknown data risks.

Second, a broad understanding of the various data protection models and their relative approaches to protecting data should make it less likely that policymakers and data custodians will resort to generalized statements about protecting data. For example, those who use “privacy” rhetoric should have their feet held to the fire about the specifics of their calls for more or less data protection.

Third, the complexity of this typology is worthwhile if it helps push back against the tendency to reduce policy discussions to binaries or other oversimplification. Even a creaking common law found room for both privacy and confidentiality models while today policymakers and regulators can choose from an array of upstream and downstream data protection models. For example, it has been common for mainstream data protection proposals to exclude data or data custodians subject to HIPAA.33 However, once it is appreciated that HIPAA is a downstream confidentiality model it makes sense to include healthcare in discussions the adoption of future upstream protective models.

Finally, this typology locates healthcare data protection within the mainstream of data protection. Mainstream data protection should embrace healthcare data protection as one of its own and learn from its experiences; the resolutely downstream, highly detailed, prescriptive HIPAA privacy rule is unique and the law and policy literature surrounding it is robust. This

is a two-way street. As argued below health care data protection needs to move beyond its HIPAA-centricity and see what additional models could be used to protect healthcare data generated or used both inside and outside of traditional healthcare environments.

III. Regulatory Turbulence, Disruption & Arbitrage

Regulatory turbulence, disruption and arbitrage presuppose the juxtaposition of at least two regulatory domains. In the simplest case one domain would be highly regulated; the other unregulated. Turbulence and disruption exist on a continuum. Regulatory turbulence may be only transient or, in the scheme of things, relatively benign. Regulatory disruption has more permanent and serious implications. Regulatory arbitrage occurs when a business purposefully exploits disruption, making business choices on the basis of the differential between the two regulatory domains.

A. Turbulence and Disruption

Regulatory turbulence, disruption and potentially arbitrage most likely will occur following some type of business disruption. True to Clayton Christensen’s classic disruption theory,\(^{34}\) such a business disruption frequently occurs because a disruptive technological innovation has empowered an entrant attacker to challenge mainstream industry incumbents.\(^{35}\) Disruptive technologies may initially underperform (or undershoot) incumbents’ sustaining technologies. However disruptive technologies “are typically cheaper, simpler, smaller, and, frequently, more convenient to use.”\(^{36}\) In contrast, “New-market disruptive innovations … occur when characteristics of existing products limit the number of potential consumers or force consumption to take place in inconvenient, centralized settings.”\(^{37}\)

\(^{34}\) See e.g., CLAYTON M. CHRISTENSEN, THE INNOVATOR’S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL (1997).
\(^{35}\) See generally Nicolas Terry, Information Technology’s Failure to Disrupt Healthcare, 13 NEV. L.J. 722 (2013).
\(^{36}\) CLAYTON M. CHRISTENSEN, THE INNOVATOR’S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL, xv (1997).
Regulatory turbulence and disruption, its more serious state, tend to follow. Take ride-hailing services typified by Uber or Lyft. They generally obey the business disruption model. Incumbent taxi services, although featuring (apparently) professionally-trained drivers, preferred locations at major locations, and liveried cabs, rely on sustaining technologies such as telephone bookings or in-person ride-hailing, and cash or often poorly implemented credit card payments. Disruptive ride-hailing services leverage spare capacity in private owners’ vehicles, ubiquitous mobile communication, location, and payment services deliver nimbler, more convenient services. Although, technologies aside, the core “assets” of ride-hailing or housing (such as Airbnb) businesses are traditionally-underused resources that modern technologies “add” to a “sharing economy,” their business models embrace disruption.

Ride-hailing services initially cause regulatory turbulence, based on uncertainty as to whether they were subject to existing regulatory models. Indeed, this appeared to be part of the disruptive strategy as Uber in particular challenged local regulations or argued they were ambiguous, their CEO noting in 2013 “It’s a regulatory disruption…We don’t talk about that a lot in tech. But you can disrupt from all sorts of directions.” These businesses, whether sharing unused automobile or housing resources at root are adopting business models that seek to reduce costs relative to incumbent competitors by avoiding or marginalizing self-regulatory organizations (such as guilds), governmental rationing (such as medallions), or regulatory models (such as licensure or employment laws). Initial

---

38 https://www.uber.com
39 https://www.lyft.com
40 https://www.airbnb.com
41 Uber CEO talks regulatory disruption, maintaining startup culture, Nov. 6, 2013, [http://mitsloan.mit.edu/newsroom/articles/uber-ceo-talks-regulatory-disruption-maintaining-startup-culture/](http://mitsloan.mit.edu/newsroom/articles/uber-ceo-talks-regulatory-disruption-maintaining-startup-culture/)
42 See generally Justin Fox, *The Problem with Guilds, from Silversmiths to Taxi Drivers*, HAY. BUS. REV., Dec. 04, 2014, [https://hbr.org/2014/12/the-problem-with-guilds-from-silversmiths-to-taxi-drivers](https://hbr.org/2014/12/the-problem-with-guilds-from-silversmiths-to-taxi-drivers) See also, Erik Engquist, *Judge rules on taxi industry lawsuit: Compete with Uber or die, Queens jurist dismisses case that yellow-cab interests said was crucial to their survival, leaving them to battle rideshare companies on their own*. Sept. 9, 2015, [http://www.crainsnewyork.com/article/20150909/BLOGS04/150909863/judge-rules-on-taxi-industry-lawsuit-compete-with-uber-or-die](http://www.crainsnewyork.com/article/20150909/BLOGS04/150909863/judge-rules-on-taxi-industry-lawsuit-compete-with-uber-or-die)
regulatory turbulence buys time during which the innovator can press for accommodating regulatory compromises (that themselves further continued disruption) or create or exploit regulatory gaps (enabling regulatory arbitrage).\textsuperscript{46} All the time the disruptive services and their technologies mature (cease undershooting), gain popularity and market share that regulators will fear to reverse.\textsuperscript{47} Former White House aide Ron Klain describes the phenomenon as follows:

[W]hat these Internet 3.0 companies are disrupting is not really technology, but regulatory regimes. What makes AirBnb exceptional is not any technological breakthrough, but how it is challenging local hospitality regulation, condo board rules, and all the other limitations on who can charge what and when for short-term housing usage. Crowdfunding sites likewise use technology that has been around for years: what they are disrupting is the vast array of federal and state regulations that govern who can invest in what, and under what terms. The same is true of so many other emerging Internet companies: their impact is far more in disrupting governmental and quasi-governmental rules than it is in technological breakthroughs.\textsuperscript{48}

While policy and political allegiances slowly determine a regulatory recalibration, incumbents and attackers operate in an uneven, even incoherent regulatory system that applies different rules to what should be competing services.
In the healthcare space some service providers claim or are hailed as having uber-like characteristics. For example, better links you to a personal health assistant, American Well promises 24x7 doctor consultations, while Heal delivers a pediatrician or family doctor to your door in less than an hour. However, these are far less disruptive than appears at first sight. They generally are respectful of regulatory systems and while leveraging mobile technologies do not attack incumbents’ features such as third party reimbursement, opting for more of a concierge model that has limited scalability.

Indeed, business disruption has generally failed in the healthcare space, the most conspicuous failure being Google’s failed challenge to the data hegemony of incumbent healthcare entities by offering low cost personal health records. The low level of business disruption probably explains the relatively low level of regulatory turbulence or disruption in the domain, at least until recently.

There are likely several reasons why technology companies have found healthcare difficult to disrupt. The dominant reason is healthcare’s primary financing model because “[t]hird-party reimbursement systems sap motivation for innovation—particularly disruptive innovation—out of the system.” However, there are additional, deep-seated causes. Thus, the “meaningful use” debacle suggests that while market failure was one explanation for the slow adoption of Electronic Health Records (EHRs), underperforming products may have been as salient. Further, information technologies may not be a good fit for current, unreformed healthcare; technology works best with processes, not healthcare’s flawed episodic nature, while information technologies thrive on liquid data which healthcare still struggles to promote.

It is also possible that technology companies, perhaps fooled by the presence of vertically integrated, positive

49 https://www.getbetter.com
50 https://www.americanwell.com/how-it-works/
52 Text accompanying note 110
outliers (such as the VA or Kaiser Permanente) underestimate the challenge of changing culturally constipated, heterogeneous providers.

Notwithstanding the absence of direct business disruption, two phenomena, big data collection and mobile health, are proving to be indirectly disruptive with the potential to move into more direct mode. Indeed, the argument can be made that mobile health is an example of Uber-like regulatory disruption or “uberfication,” a disruptive, tech-heavy approach that promotes “uber-convenience” through always-on mobile services that instantly match patient demand with healthcare supply. Both mobile health and big data analytics have developed primarily outside of (and sometimes in parallel to) traditional healthcare space. However, while their overlaps increase they are also providing technologically-mediated alternatives to traditional healthcare interactions, services, and data. In this regard they offer the potential for business disruption. As discussed below they are already disrupting regulatory models and exhibiting some arbitrage.55

B. Arbitrage

In Victor Fleischer’s words regulatory arbitrage “exploits the gap between the economic substance of a transaction and its legal or regulatory treatment…”56 However, Fleischer was primarily interested in “regulatory gamesmanship” and modeling the tradeoff between regulatory and transaction costs. The examination of regulatory arbitrage in this article more closely resembles leveraging differences in regulatory substance between different jurisdictions. For example, when a taxpayer shifts income out of a high-tax jurisdiction into a tax haven as with the well-known “double-Irish.”57 Examples in the healthcare domain would include Israeli gays, prohibited by domestic law from using surrogacy, using third world surrogates,58 a UK resident avoiding a healthcare shortage (wait-list) by having the procedure performed elsewhere in the European Union and subsequently requiring the UK to reimburse,59 and attracting patients to

55 Text accompanying note 172 et eq.
57 See e.g., Death of the Double Irish, THE ECONOMIST, Oct. 18 2014
59 See Case C-372/04, The Queen, on the application of: Yvonne Watts v. Bedford Primary Care Trust and Secretary of State for Health, Case C-372/04 (ECJ 2006). See generally
jurisdictions where CRISPR-Cas gene editing is available. Of course, the
issue discussed herein is not transnational, but rather domestic arbitrage
exploiting variances between U.S. regulatory silos.

An evolving example of domestic regulatory disruption/arbitrage in our
healthcare domain is the growing “off-label use” of FDA approved drugs.
Two “disruptions” enabled the regulatory arbitrage. First, business
disruption created massive (and highly profitable) markets for unapproved
uses. Second, the legal disruption (or “First Amendment opportunism”) caused by the rapid development of (commercial) speech jurisprudence.
In U.S. v. Caronia the Second Circuit overturned the conviction of a drug
representative for promoting an off-label use of a central nervous system
depressant. Applying strict scrutiny the court held the government could not
prosecute manufacturers or representatives for speech promoting the lawful,
off-label use of an approved drug. Dissenting, Judge Livingston
recognized the regulatory disruption caused by her colleagues, “the majority
calls into question the very foundations of our century-old system of drug
regulation.” The court recognized the regulatory gap exploited by the drug
company as follows: “To obtain FDA approval, drug manufacturers are
required to demonstrate, through clinical trials, the safety and efficacy of a
new drug for each intended use or indication” but that “[o]nce FDA-
approved, prescription drugs can be prescribed by doctors for both FDA-
approved and -unapproved uses; the FDA generally does not regulate how
physicians use approved drugs.” By marketing its regulated drug to unregulated (in this context) physicians the drug company created
regulatory disruption. Subsequently in Amarin Pharma, Inc. v. FDA a
district court rejected FDA’s narrow reading of Caronia and enjoined the
agency from threatening a misbranding action in another off-label use case


60 See e.g., On the Road (to a Cure?) — Stem-Cell Tourism and Lessons for Gene Editing, R. Alta Charo, J.D. February 10, 2016DOI: 10.1056/NEJMp1600891
61 Frederick Schauer, First Amendment Opportunism, in Eternally Vigilant: Free Speech in the Modern Era, 175, 176 (Lee C. Bollinger & Geoffrey R. Stone eds., 2001)
62 See e.g., Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011). See generally Robert Post, Transparent and Efficient Markets: Compelled Commercial Speech and Coerced
63 703 F.3d 149, 169 (2nd Cir. 2012)
64 703 F3d at 169 (citations omitted)
65 703 F3d at 153 (citations omitted)
because it chilled protected speech.\footnote{United States District Court, S.D. New York. August 07, 2015 Slip Copy 2015 WL 4720039} One of the FDA’s goals in pursuing such actions is to “encourage use of the FDA’s drug review and approval process” and “deter manufacturers from evading the FDA’s review process for additional uses of approved drugs.”\footnote{Id., at *6} By leveraging the differential regulatory models applied to drug manufacturers and doctors, industry is avoiding that very process.

C. Implications of Regulatory Disruption and Arbitrage

As discussed above, using ride-hailing and accommodation-sharing services as examples, regulatory turbulence tends to create uncertainty and so increased information costs among market participants, policymakers, and regulators. This may be followed by far more serious regulatory disruption where incumbents and attackers face uneven policy environments. These de facto differential regulatory environments may be a product of non-enforcement by regulators. For example, regulators may exercise discretion for fear of, say, frustrating innovation or the political cost of “interfering” with a popular new service. Equally, in an attempt to deal temporarily with disruption during a time of policy recalibration, agencies might issue sub-regulatory “guidances” that while seeking to be supportive of both incumbents and innovators can be unclear, creating ambiguity and so increasing disruption. In the data space regulatory disruption does not stop with similar data being subject to differential regulation. Additionally, data subjects may experience regulatory “churn” as, during their lifecycle, data repeatedly enter or exit regulated and lightly regulated spaces, further adding to the information costs in identifying a current regulatory state.

IV. Exceptionalism and the Healthcare Data Protection Model

HIPAA provides relatively robust protections against unauthorized uses of health information by a relatively narrow set of traditional healthcare provider data custodians. Its inherent limitations are because of its narrow domain inclusions (some traditional healthcare providers and insurers, not all custodians of healthcare data) and because it uses downstream data protection modes (that is does almost nothing to regulate the collection of health data). An accurately labeled HIPAA privacy rule would be something like “the doctor/hospital/insurer confidentiality rule. The other HIPAA rules, security and breach notification have the same limitations;
U.S. healthcare data protection is not only sectoral but also almost completely downstream.

A. Sectoral Model

As noted by the White House report on big data, “[i]n the United States during the 1970s and 80s, narrowly-tailored sectoral privacy laws began to supplement the tort-based body of common law. These sector-specific laws create privacy safeguards that apply only to specific types of entities and data.” When HIPAA was originally drafted there is every reason to believe that a domain-limited model was intended, in large part to separate healthcare data from financial services data. There could have been no delusion that all healthcare data custodians would be covered by the rule (in large part because of the limitations of the enabling legislation). The likely proof is that the coverage of outsiders such as law firms and marketing companies had to be “patched” with mandatory contracts between insider-covered entities and their outsider “business associate.” It was not until 2009 when additional statutory authority provided by the Health Information Technology (HITECH Act) allowed for their direct regulation. Similarly, it was apparent early on that neither life insurers, nor most employers (except to the extent that they were also health plan administrators) were covered. Those exceptions aside, HIPAA appeared to blanket healthcare, at least as we knew it in 1999. This was achieved using sector-specific language:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider who transmits any health information in electronic form in connection with a transaction.

---

69 See text accompanying note 123, et seq.
70 The legislation primarily was concerned with imposing e-commerce models on those engaged in traditional healthcare transactions. Hence, the regulatory authority was limited to providers, insurers and clearinghouses. See HIPAA Act, 1996 §262.
71 45 CFR §160.103, §164.502(e),.504(e),.532(d)(e)
73 §13041. See 45 CFR § 160.102(b).
74 45 CFR 160.102 (Protected Health Information)
75 45 CFR 164.504(f)
76 45 CFR 160.102
Ignoring the technical verbiage, HIPAA regulated health insurers and traditional HCPs such as doctors, hospitals and pharmacists. A couple of other limitations to the definition of protected data reduced the ranks of regulated providers. For example, the requirement of transmittal of “any health information in electronic form” may have excluded some technologically backward rural providers and, today, may still exclude “cash-only” mental healthcare providers.

Other exclusions are more implicit. For example, only “individually identifiable health information” is protected and “[h]ealth information that does not identify an individual… is not individually identifiable health information.” As a result de-identified data are not subject to HIPAA regulation. De-identification may be achieved by the use of the expert (aka statistical) method or the removal of certain identifying elements so as to trigger a safe harbor. Furthermore, an IRB can, in limited circumstances, act as a surrogate for individuals and waive consent/authorization for the use of identifiable data for research purposes. Taken together these provisions suggest that most, but not all, researchers fall outside of HIPAA regulation, their use of data instead being subject to the Common Rule.

As a result, HIPAA’s own “original sin” is easy to identify. The data protection model is structured around a group of identified healthcare data custodians rather than around healthcare data. Although HITECH expanded direct applicability and enforcement to business associates in 2009, it granted no additional expansion of the Privacy or Security Rules to deal with healthcare data existing outside of the HIPAA-zone. There was one exception, the nature of which illustrated rather than solved the HIPAA deficit. HITECH provided for a breach notification rule applicable to the providers of PHRs by some non-HIPAA-regulated entities. However, it did

---

78 45 CFR 160.103 (Covered Entity)
79 See also HITECH/Omnibus “cash-only” provision, permitting patients to opt out of EHR recording of encounter…
80 45 CFR §164.103
81 45 CFR § 164.514
82 45 CFR § 164.514(b)(1)
83 45 CFR § 164.514(b)(2)
84 45 CFR § 164.512
85 Cf. Limited data set recipients. 45 CFR 164.514(e)
86 See generally http://www.hhs.gov/ohrp/humansubjects/commonrule/
not extend the HIPAA rule\textsuperscript{87} to them, instead providing for distinct FTC rule-making for this limited group of non-HIPAA entities.\textsuperscript{88} This approach therefore highlights two of the problems associated with sectoral models; fragmentation of data protection by custodian type and sector/sub-specific regulators.

B. Downstream Protection Favored

Contemporary healthcare data protection is resolutely and almost exclusively downstream. The HIPAA Privacy Rule employs a downstream data protection model ("confidentiality") that seeks to contain the collected data within the healthcare system by prohibiting its migration to non-healthcare parties.\textsuperscript{89} Its complementary Security Rule imposes physical and technological constraints on patient data storage designed to impede those outside of the healthcare system from acquiring such data without consent.

The only upstream protection in HIPAA, patient consent at initiation of the provider-patient relationship was, as discussed below,\textsuperscript{90} removed even before the Privacy Rule came into effect. In modern law, HIPAA aside,\textsuperscript{91} only one healthcare data protection law, the Genetic Information Nondiscrimination Act of 2008 (GINA),\textsuperscript{92} has exhibited any upstream modeling.\textsuperscript{93}

Historically, some upstream, collection-centric data protection models such as the intentional tort of intrusion into seclusion have seen limited application in the healthcare domain. However, these have seen only limited build-out. Indeed, the seclusion tort seems has seemed most comfortable when applied to obviously intentional outlying factual situations such as unconsented-to photography by physicians.\textsuperscript{94} Routinely, now, courts seem

\textsuperscript{87} HITECH § 13402/Omnibus Rule
\textsuperscript{88} HITECH § 13407/Health Breach Notification Rule, Federal Register / Vol. 74, No. 163 / Tuesday, August 25, 2009
\textsuperscript{89} See, e.g., 45 C.F.R. § 164.502 (2012).
\textsuperscript{90} Text accompanying note 128
\textsuperscript{91} This is something of an exaggeration as HIPAA and GINA are tied together in some places, such as by the provisions of HITECH…
\textsuperscript{93} Text accompanying note 137, et seq.
to prefer the downstream breach of confidence tort as the dominant common law model of healthcare data protection.\textsuperscript{95}

Aside from mimicking the prevalent model of U.S. data protection, it is not hard to explain why healthcare data protection opted for a downstream path. Historically, the culture of medicine has seemed to favor collecting \textit{everything}. Such a model was likely uncomplicated given the available technologies and diagnostic practice. It was also likely uncontroversial in the context of a traditional, two-party physician-patient relationship; the patient exercised his or her autonomy rights and disclosed all (or most\textsuperscript{96}) data to the physician in return for more effective treatment and a promise of confidentiality.\textsuperscript{97} It is hard to imagine that upstream FIPPS such as context or data minimization would have been explored in this simple healthcare data exchange scenario. Rather, any conflicts that arose would tend to be dealt with in the framework of restrictions on data disclosure and the reach of exceptions from it.

It should have been relatively obvious that this model would not scale well to industrial healthcare. However, it is not particularly surprising that the eventual federal model would persist with downstream protections—it was after all based on state common law and statutes that also were primarily downstream. Even the latest addition to the healthcare data protection, the quintessentially downstream breach notification rule introduced in 2009, likely was inspired by state models given the absence of any federal example.

The problem, however, is that healthcare data protection has appeared increasingly blind to the impact of information technology. Looking through the healthcare industry lens this should not be too surprising. Almost every contemporary technological challenge thrown at the healthcare industry, Y2K,\textsuperscript{98} the HIPAA transactional mandate,\textsuperscript{99} HIT adoption,\textsuperscript{100} Meaningful Use,\textsuperscript{101} and ICD-10\textsuperscript{102} have been met with objection and prevarication.\textsuperscript{103}

\textsuperscript{95} See e.g., Biddle v. Warren General Hospital, 715 N.E.2d 518, 523 (Ohio 1999).
\textsuperscript{97} See further discussion on this dynamic at text accompanying note 30, et seq.
\textsuperscript{100} See generally Nicolas Terry, \textit{Information Technology’s Failure to Disrupt Healthcare}, 13 Nev. L.J. 722 (2013).
While it seems a truism that the common law has marched “with medicine but in the rear and limping a little,” the lag of regulation in the face of information technology has been even more marked. If the HIPAA architects thought they had a fairly good grasp on the healthcare domain in the 1990s, thereafter the vector between regulation and technology has increased considerably. In hindsight perhaps the greatest flaw in HIPAA is that it takes a pre-IT (maybe even pre-industrialized medicine) approach to data use; it is either permitted or prohibited. That binary may have been appropriate for the limited records of the Marcus Welby MD-era. After all, at the time the HIPAA rules were first promulgated, EHRs were barely visible and HHS was chasing ecommerce models already well established a decade before in other domains. The cycle then seemed to repeat. By 2009 the country was in the middle of a federal initiative to bring EHRs to all and the same legislation authorized an expensive subsidy program to catch-up. Yet, most of the data protection provisions in HITECH were designed to correct or tweak ten-year-old flaws in HIPAA.

The most “outside-the–box” provision in the HITECH Act was the discrete breach notification rule for non-HIPAA PHRs. This was the first acknowledgment that HIPAA-like data were being created or processed by data custodians who were not subject to HIPAA. For a brief period in the late 2000s PHRs seemed poised to gain some traction as an alternative to the slowing Bush administration ten-year EHR initiative. Of the PHRs that were launched in this period Google Health was by far the most potentially disruptive. Indeed, it was a clear example of incipient regulatory arbitrage because Google intended to avoid HIPAA by dealing directly with patients (data subjects) rather than covered entities (regulated data

---

101 See generally Nicolas Terry, *Meaningful Adoption: What We Know or Think We Know about the Financing, Effectiveness, Quality, and Safety of Electronic Medical Records*, 34 J. LEGAL MEDICINE, 7-42 (2013).


104 Mount Isa Mines v. Pusey, (1970) 125 CLR 383, 395 (Supreme Court of Queensland) per Windeyer J.

105 See [https://en.wikipedia.org/wiki/Marcus_Welby,_M.D.](https://en.wikipedia.org/wiki/Marcus_Welby,_M.D.)

106 HITECH 2009 Subtitle A

107 The exception was §13405(d) prohibiting certain sales of EHR data. See also 45 CFR §164.502(a)(5)(ii).

However, shortly after HITECH introduced Meaningful Use based around proprietary formats. Google, its technical model built around open web standards, shuttered Google Health. By the time most of the HITECH provisions found a regulatory form in the 2013 Omnibus Rule the ball had moved again, with concerns being raised about big data, mobile, and even more recently the Internet of Things.

The sector-based approach to data protection has led to today’s chronically uneven policy environment, causing, as discussed below, regulatory disruption and enabling arbitrage in the healthcare domain. However, it is an over-commitment to downstream rules that makes reform problematic. Arguably, tweaked downstream rules cannot deal with the challenges to healthcare data protection; upstream models also must be deployed.

C. Understanding Exceptional Healthcare Data Protection

The exceptional treatment of healthcare was dealt a blow in *NFIB v. Sebelius* when a Supreme Court majority rejected any special treatment under the Commerce or Necessary & Proper Clauses. Yet, three years later in *King v. Burwell* an exceptionalism argument found favor with the majority adopting a *Chevron* zero approach and then holding “Congress passed the Affordable Care Act to improve health insurance markets, not to destroy them. If at all possible, we must interpret the Act in a way that is consistent with the former, and avoids the latter.” Certainly, exceptionalism would explain Justice Scalia’s scathing comment in dissent, “We should start calling this law SCOTUScare.”

Healthcare data protection exceptionalism has had a far more consistent history and HIPAA still stands tall when compared to protections given to personal data in other sectors. This exceptional protection is of great importance. Outside of healthcare there is no history or expectation of strong data protection. Of course there are other protected sectors, but the

---

113 135 S.Ct. 2480, 2495 (2015)
114 135 S.Ct. at 2507
level of data protection is relatively low or favors data-custodian-favoring choice architectures (such as opt-out). Outside of healthcare, therefore, the mantras of “get over it,” self-regulation, and market solutions gain more traction. The health data protection model has a far stronger baseline that resists the arguments of privacy defeatists.

The story of exceptional healthcare data protection has one additional implication, the relative isolation of healthcare data protection from general data protection. Healthcare lawyers may not be to blame here. After all, HIPAA’s “more stringent than” cooperative preemption model accepts that HIPAA provides a privacy and security floor permitting federal law’s intersection with some state laws. Further, health privacy policymakers have recognized that HIPAA’s downstream models normatively are not the end of the line. Indeed, it has been recognized that healthcare entities also should conduct themselves by reference to FIPPS. If anything healthcare data protection has been shunned by those outside. HIPAA seems to been viewed as sui generis and healthcare data protection as having been “solved.” For example, two reports issued in 2012 by the White House and the FTC excluding healthcare data from their data protection proposals. However, this situation may be turning around. For example, in its 2014 Data Brokers report the FTC included the health domain in its study, even making a specific legislative recommendation to acquire the express consent of data subjects before adding healthcare data. Looking forward, general data protection should learn from healthcare’s experience in dealing with downstream protective models, while healthcare data protection needs to accept that many of its issues cannot be handled by older models such as HIPAA or common law confidentiality.

1. History of Exceptionalism

Neither historically nor in modern law has the action for breach of confidence been unique to healthcare relationships. Notwithstanding, actions involving physicians are disproportionately represented in the

---

116 45 CFR 160.203(b)
117 HITPC Transmittal Letter to National Coordinator for HIT Dr. David Blumenthal, Sept. 1, 2010, at 2-3
http://www.healthit.gov/sites/faca/files/hitp_transmittal_p_s_tt_9_1_10_0.pdf
119 FTC, Data Brokers: A Call for Transparency and Accountability (2014), at 52.
confidence jurisprudence and the physician-patient fiduciary relationship seems to have been a powerful rationale upon which the various doctrinal bases have been rested. Consider, for example, some the very earliest breach of confidence cases that based the action (too early to call a tort) on positive duties imposed by medical licensure statutes.¹²⁰ Later cases would:

[R]ely on various sources of public policy favoring the confidentiality of communications between a physician and a patient, including state licensing or testimonial privilege statutes, or the Principles of Medical Ethics of the American Medical Association (1957), Section 9, or the Oath of Hippocrates. Some note that while public policy considerations are a sound enough basis to support liability, a more appropriate basis can be found in the nature of the physician-patient relationship itself, either because of its fiduciary character or because it is customarily understood to carry an obligation of secrecy and confidence.¹²¹

Today, breach of confidence is recognized as a tort of general applicability.¹²² However, just as its genesis depended on healthcare-specific doctrines so its primary usage remains in the healthcare domain. Indeed, it can lay claim to being the first exceptional protection of healthcare data.

In 1999, representing physician organizations, Dr. Richard Harding testified before the House of Representatives argued, “It is critically important to recognize the difference between medical records privacy and financial privacy” because “damages from breaches of medical records privacy are of a different nature.” This he ascribed to the extremely sensitive nature of the information contained therein, “heart disease, terminal illness, domestic violence, and other women's health issues, psychiatric treatment, alcoholism and drug abuse, sexually transmitted diseases and even adultery” that, if disclosed “can jeopardize our careers, our friendships, and even our marriages.”¹²³ As a result of that and other testimony a proposal to protect some healthcare data held by insurers to be covered by GLBA was dropped.

The well-respected Institute of Medicine has long endorsed exceptionalism:

¹²⁰ See e.g., Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920). See also Smith v. Driscoll, 162 P. 572, 572 (1917).
¹²² 86 Ohio St.3d at 400.
For the most part, privacy law in [the U.S.] has been formulated under the assumption that holders of information about people may generally do with it what they please, constrained only by corporate ethics and the good taste of business, societal acceptance (or outrage), occasional attention by the government, pressures of consumer activist groups, and the consequences of legal actions brought by individuals or consumer groups. This historical view may prove inappropriate or even dangerous in regard to health data.  

Of course, the ultimate proof of exceptionalism is almost two decades of HIPAA itself and the simple fact that the largest industry in the U.S. is subject to the country’s most comprehensive (if flawed) data protection regulation and enforcement. Although disliked by powerful healthcare interests HIPAA has not faced any significant challenges. When President G.W. Bush came into office the HIPAA Privacy rule had only just been issued by Donna Shalala, President Clinton’s HHS Secretary. Incoming Secretary Tommy Thompson promised a thorough rethink of the rule. Yet only minor tweaks were made and the secretary soon announced “President Bush wants strong patient privacy protections put in place now. Therefore, we will immediately begin the process of implementing the patient privacy rule that will give patients greater access to their own medical records and more control over how their personal information is used.” In 2009 the bipartisan HITECH Act strengthened HIPAA privacy, broadened its scope to directly regulate “Business Associates,” and included authority to issue a healthcare data breach (recall that Congress has not been able to pass one of general applicability).

2. Health Subdomain Exceptionalism

128 For example, replacing the original 45 C.F.R. § 164.506(a) requirement of consent with a privacy notice §164.506(b)(1).
Obviously general healthcare data are exceptionally protected. However, a few of its subdomains exhibit additional levels of exceptionalism. One of these is actually provided for in the HIPAA Privacy Rule. Process notes taken by psychotherapists are personal notes and “typically are not required or useful for treatment, payment, or healthcare operations purposes, other than by the mental health professional who created the notes.” As a result the Privacy Rule therefore applies exceptional restrictions on patient access and healthcare provider disclosure.

Moving outside of HIPAA several subdomains exhibit enhanced exceptionalism. Thus, HIV-AIDS is treated exceptionally compared to other STDs. Generally-applicable federal law such as the Rehabilitation Act and the Americans with Disabilities Act apply to claims of discrimination. And, of course, HIPAA applies a data protection baseline. However, state laws tend to provide additional, exceptional data protection such as anonymous testing and heightened controls on disclosure.

GINA utilizes two models of data protection. First, GINA prohibits downstream point of use discrimination by employers (Title I) and health insurers (Title II). However, GINA also prohibits the requiring or (in many cases) acquiring genetic information. This is an upstream collection model of protection and has resulted in large settlements with the EEOC in cases

---

130 The list of examples that follow is not closed. For example, Stacey Tovino has floated neuro-imaging exceptionalism, Stacey A. Tovino, *Functional Neuroimaging Information: A Case for Neuro Exceptionalism?* 34 FLA. ST. U. L. REV. 415, 485 (2007). Further, Mark Rothstein has discussed the possibility for epigenetic exceptionalism. Rothstein, M. A. (2013), *Epigenetic Exceptionalism*. JOURNAL OF LAW, MEDICINE & ETHICS, 41: 733–736 at 735. See also, Nicolas Terry, *Developments in Genetic and Epigenetic Data Protection in Behavioral and Mental Health Spaces*, Behavioral Sciences & the Law (forthcoming 2016). Finally, some states have safe harbor rules that protect physicians who are diverted to physician health programs in the case of mental health or substance use disorders. See generally J. Wesley Boyd, MD, PhD and John R. Knight, MD, Ethical and Managerial Considerations Regarding State Physician Health Programs, J ADDICT MED 2012;00: 1.


132 §504


dealing with unlawful requests for family medical histories and a landmark $2.2 million jury verdict in the recent “devious defecator” case.

Less well-known are the Substance Abuse Confidentiality Regulations (often referred to by their citation, “45 CFR Part 2”) promulgated by HHS’s Substance Abuse and Mental Health Services Administration (SAMSHA). These regulations subject federally-assisted programs that maintain alcohol and drug abuse patient records to downstream disclosure restrictions that are considerably more stringent than those found in HIPAA. There is also a complex web of overlapping state mental health and substance abuse laws that further complicate the picture. Recently 45 CFR Part 2 has attracted considerable attention because of Congressional concerns over the information–sharing costs it imposes. For example, in a recent letter to a Congressional committee supportive of the 21st Century Cures Act the Patient Safety Movement urged, “At a minimum, this problem should be addressed by streamlining the consent process for the sharing medical records in integrated care settings.” Reform of Part 2 has also been targeted in Congressman Tim Murphy’s Helping Families in Mental Health Crisis Act of 2015, creating concern among some privacy advocates. In February 2016 SAMSHA published a proposed rule that would allow a broad “to whom” consent that it believed would increase the sharing of substance use records through EHRs and Health Information

---

139 Promulgated under the Drug Abuse Prevention, Treatment, and Rehabilitation Act, § 408 by
Exchanges. The proposed rule would also permit healthcare data custodians to share substance abuse data with researchers.\textsuperscript{144}

V. Turbulence, Disruption, and Arbitrage in Practice

A. Professional Healthcare Domain vs. Consumer Domain

In the words of a recent report by the HIT Policy Committee (HITPC), a FACA established by the HITECH Act,\textsuperscript{145} “[m]uch of the health-related information generated today is not regulated by [HIPAA]”\textsuperscript{146} and “The exact same health-related information is regulated differently based on the entity processing the information.”\textsuperscript{147} As already discussed the prerequisite for regulatory turbulence, disruption, and potentially arbitrage is the existence of differential regulatory models. For the purposes of the present analysis, two regulatory domains are posited, first, a professional healthcare domain and second, a consumer healthcare domain.

The professional domain is heavily populated with regulatory models. For example, it is home to state regulation of healthcare providers, custom-based quality and safety, medical malpractice doctrine, the federal regulation of Rx drugs and medical devices, state and federal regulation of professional data curators (HIPAA data custodians), unique “fraud and abuse” transactional regulations, specialized antitrust scrutiny, institutional review board/Common Rule scrutiny of human subjects research. Befitting the country’s most regulated industry there are considerably more examples.

In contrast, the consumer healthcare domain is larger, yet both less regulated and considerably more indeterminate. For example, OTC pharmaceuticals are only lightly regulated by FDA,\textsuperscript{148} a few issues


\textsuperscript{145} The Health Information Technology for Economic and Clinical Health (HITECH) Act, 2009 §3002.


\textsuperscript{147} Id. at 11.

\textsuperscript{148} See FDA, Drug Applications for Over-the-Counter (OTC) Drugs http://www.fda.gov/drugs/developmentapprovalprocess/howdrugsaredevelopedandapproved/approvalapplications/over-the-counterdrugs/default.htm
regarding consumer platforms may attract some FCC scrutiny, common law products liability or the Consumer Product and Safety Act may apply to a narrow range of safety issues, and mobile apps and wearables are either unregulated or currently benefiting from FDA discretion. Meanwhile, some parts of the domain, for example crowdsourcing research models, are barely regulated. Others, such as data-curation by data subjects, seem very hard to regulate.

Differentiated regulatory domains can tolerate some turbulence. Further, not all turbulence develops into disruption. Consider the following episodes of turbulence between professional and consumer domain. First, Google Glass; Google introduced (initially only to “Glass Explorers”) this augmented reality wearable in 2013. It was designed and sold as a consumer product.\(^{149}\) Increasingly, however, doctors joined the ranks of the “explorers” and soon Glass appeared in hospitals, used during surgeries, for EHR access, and training.\(^{150}\) The problem was that while Glass satisfied the minimal regulatory standards of the consumer domain, it caused regulatory problems in the professional domain. For example, it was not HIPAA-compliant, in some implementations it came close to FDA regulated device territory, and its “stealth” camera tempted marginal collection of health and personal data.\(^{151}\) However, before Glass could become an example of full-on regulatory disruption, Google announced it would cease selling the device.\(^{152}\)

23\textit{and}Me, a consumer-facing DNA test kit and analytic service, was launched in 2007.\(^{153}\) The product was stated to provide health reports on multiple diseases and conditions written with enough specificity to prompt FDA inquiry. 23\textit{and}Me featured genotyping, not sequencing (although those technologies are beginning to merge). Notwithstanding, here was an


The “Blue Button”\textsuperscript{162} is a federal government initiative permitting Medicare beneficiaries\textsuperscript{163} and VA patients\textsuperscript{164} to download their health records. The data may be downloaded in text, PDF, or Blue button formats. ONC and CMS are targeting similar models as a way of increasing patient engagement and data liquidity in Stages 2 and 3 of Meaningful Use.\textsuperscript{165}

What do we learn from these three examples of regulatory turbulence? Both Google Glass and 23\textit{andMe} were temporary phenomena. The former was a consumer domain product that caused some turbulence in professional space but which was withdrawn from the market before disruption could occur (or HIPAA indeterminacy or FDA device regulation were resolved). The latter was the inverse; a professional domain technology sold into consumer space. 23\textit{andMe} likely was subject to professional domain medical device regulation. It caused turbulence at a process level because its developer seemingly was oblivious to or unmindful of FDA regulation. As a result, for several years there was accidental disruption until regulator-regulatee information costs equalized. Once 23\textit{andMe} was forced to confront the FDA’s concerns it decided to stop marketing the kit and changed its reports to generic information rather than anything approaching diagnostics.\textsuperscript{166} Subsequently, FDA approved the company’s marketing of more narrowly focused tests for Bloom syndrome\textsuperscript{167} and autosomal recessive disorders.\textsuperscript{168} Furthermore, the FDA designation of the tests as

\begin{itemize}
\item \textsuperscript{162} HHS, About Blue Button, \url{http://www.healthit.gov/patients-families/blue-button/about-blue-button}
\item \textsuperscript{163} Download claims with Medicare's Blue Button, \url{https://www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html}
\item \textsuperscript{164} myHealtheVet, \url{https://www.myhealth.va.gov/mhv-portal-web/anonymous.portal?}
\item \textsuperscript{165} Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 FR 53968, 53973, Sept. 4, 2012. For more detail see e.g., Eligible Professional, Meaningful Use Core Measures, Measure 7 of 17, Stage 2, August, 2014, \url{https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_7_PatientElectronicAccess.pdf}
\item \textsuperscript{166} Brian Fung, Bowing again to the FDA, 23\textit{andMe} stops issuing health-related genetic reports, \textit{WASH. POST}, Dec. 6, 2013, \url{https://www.washingtonpost.com/news/the-switch/wp/2013/12/06/bowing-again-to-the-fda-23andme-stops-issuing-health-related-genetic-reports/}
\item \textsuperscript{167} FDA News Release, \textit{FDA permits marketing of first direct-to-consumer genetic carrier test for Bloom syndrome}, Feb. 19, 2015, \url{http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/UCM435003}
\item \textsuperscript{168} Andrew Pollack, \textit{23andMe Will Resume Giving Users Health Data}, \textit{NY TIMES}, Oct. 21, 2015, \url{http://www.nytimes.com/2015/10/21/business/23andme-will-resume-giving-users-health-data.html}. FDA continues to investigate other direct-consumer genetic tests; see e.g., \url{http://www.fda.gov/downloads/MedicalDevices/ResourcesforYou/Industry/UCM471784.pdf}
\end{itemize}
over-the-counter\textsuperscript{169} led to the obviation of some state law limitations on the services, making them available across the country.\textsuperscript{170}

Only the last of these three examples exhibits a transition from turbulence to disruption. The entirely well meaning, patient-autonomy-respecting Blue Button program has a seriously disruptive effect. It takes HIPAA-protected data and, with a single click from the data subject, moves it into almost completely unprotected domain. This is a model now being repeated by Stage 3 of Meaningful Use that adds the option of an application programming interface (API) linkage between a provider’s EHR and a patient’s app.\textsuperscript{171} It could be argued that there is simply no data protection issue when the data subject holds data. However, the data likely implicates persons other than the data subject (such as the subject’s family members) and so data compromise is not neither benign nor intrinsically limited. Further, there is disruption in fact and confusion when the “same” data are subject to both professional domain regulation (professional curation) and consumer domain-regulation-lite (personal curation). Clicking the Blue Button strips data protection from clinical data. Major questions arise as to how to adequately warn the data subject at the point of conversion and whether data subject expectations (and responsibilities) can be appropriately remodeled.

A parallel (potentially exacerbating) regulatory disruption can occur at the process level when different regulatory agencies operate in different domains. For example, HHS-OCR regulates professional domain data protection but FTC regulates consumer space. Similarly, FDA regulates medical devices but the Consumer Product Safety Commission or the FCC might deal with consumer domain. A further complication may be overlapping state and federal laws (e.g., state products liability law overlapping with FDA or state healthcare data protection legislation overlapping with HIPAA privacy or security) by the intersection of state & federal/member state & single market laws and regulators

\textbf{B. Example One: Big Data}


\textsuperscript{171} Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 3 and Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62762, Oct. 16, 2015, §495.24
Observations as to either the sectoral limitations of U.S. data protection or the rise of commercial data brokers are hardly novel. A decade ago Dan Solove and Chris Hoofnagle noted, “Although most industrialized nations have comprehensive data protection laws, the United States has maintained a sectoral approach where certain industries are covered and others are not. In particular, emerging companies known as “commercial data brokers” have frequently slipped through the cracks of U.S. privacy law.”\textsuperscript{172} Solove and Hoofnagle did not use the terms disruption or arbitrage but probably had something similar in mind when stating, “Many companies brokering in data have found ways to avoid being regulated by [FCRA].”\textsuperscript{173} More recently Kate Crawford and Jason Schultz observed, “Not only does Big Data's use have the potential to circumvent existing antidiscrimination regulations, but it may also lead to privacy breaches in health care…”\textsuperscript{174}

As reported by FTC “data brokers… purchase information about individuals from wide-ranging commercial sources. For example, the data brokers obtain detailed, transaction-specific data about purchases from retailers and catalog companies. Such information can include the types of purchases (e.g., high-end shoes, natural food, toothpaste, items related to disabilities or orthopedic conditions), the dollar amount of the purchase, the date of the purchase, and the type of payment used.”\textsuperscript{175}

In most cases data brokers will not find dealing directly with HIPAA covered entities (or their business associates) to be a good source of clinical data. Generally HIPAA entities would be unable to supply clinical data without data subject (patient) authorization,\textsuperscript{176} a heightened form of consent. Or, if the brokers request for a “limited data set,” was agreed to, the disclosure would be restricted to “research” only processing and subject to a re-identification-limiting data use agreement.\textsuperscript{177}

\textsuperscript{173} Solove and Hoofnagle at 359.
\textsuperscript{174} Kate Crawford and Jason Schultz, \textit{Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms}, 55 B.C. L. REV. 93, 99 (2014)
\textsuperscript{176} 45 CFR §164.508
\textsuperscript{177} 45 CFR §164.514
Not surprisingly, therefore, data brokers construct their clinical data “proxies” from other data pools, pools that like the public records and other databases they mine, exist outside of HIPAA-protected space. They do not completely ignore data that has been subject to HIPAA protection. For example, they acquire de-identified data; HIPAA data that once de-identified are no longer subject to HIPAA. Also they acquire HIPAA data that have been legally shared with public health authorities who then make anonymized or de-identified data sets available.

As discussed elsewhere these data are supplemented by medical-inflected data, what McKinsey refers to as “Patient behavior and sentiment data that describe patient activities and preferences, both inside and outside the healthcare context.” These data are culled from social media interactions, retail stores, web trackers, online transactions, mobile phone location trackers, fitness wearables, and so on. Data brokers subsequently leverage their sophisticated algorithms and the breadth of their triangulation databases to re-identify the data.

Increasingly, our everyday interactions will trigger unrealized or unconsented collection of data about us from IoHT devices, specifically our location and physical, even medical condition. As pointed out by Elizabeth Pike another likely data pool is the “non-consensual collection of genetic material.” Pike identifies regulatory disruption because “In many ways, commercial endeavors are less heavily regulated than federally funded research endeavors outside the Common Rule’s reach. And commercial entities are unlikely to be “covered entities” subject to HIPAA’s Privacy Rule.”

---

178 Text accompanying note 80, et seq.
179 45 CFR §164.512(b)
181 See Nicolas Terry, Big Data Proxies and Health Privacy Exceptionalism, 24 HEALTH MATRIX 65, 84-87 (2014)
182 http://www.pharmatalents.es/assets/files/Big_Data_Revolution.pdf
183 See generally Nicolas Terry, Developments in Genetic and Epigenetic Data Protection in Behavioral and Mental Health Spaces, BEHAVIORAL SCIENCES & THE LAW (forthcoming 2016).
185 Id. at 8 (references omitted)
These disparate, essentially unregulated data pools make possible the following claim by one major data broker:

We have one of the largest and most comprehensive collections of healthcare information in the world, spanning sales, prescription and promotional data, medical claims, electronic medical records and social media. Our scaled and growing data set, containing over 10 petabytes of unique data, includes over 85% of the world’s prescriptions by sales revenue and approximately 400 million comprehensive, longitudinal, anonymous patient records. We standardize, organize, structure and integrate this data by applying our sophisticated analytics and leveraging our global technology infrastructure to help our clients run their organizations more efficiently and make better decisions to improve their operational and financial performance.\(^\text{186}\)

The regulatory disruption is clear and arbitrage highly likely. Data brokers, generally shut out of protected healthcare data are able to create proxies for those data in a lightly regulated HIPAA-free zone. Crawford and Schultz go further, noting that the “predictive privacy harms” caused by big data are such that traditional upstream and downstream data protection models (“collection, processing and disclosure”) can be circumvented.\(^\text{187}\)

Health data acquired in this manner can also be looped back into healthcare space for discriminatory purposes. As is well known the ACA prohibits pre-existing condition exclusions, discriminatory premium rates, and generally requires guaranteed issue.\(^\text{188}\) Guaranteed issue and related regulations generally do not apply to life insurers who are customers for big data proxies. So, somewhat surprisingly are health insurers who use data-mined prescription drug data to continue their discrimination against high cost patients.\(^\text{189}\) For example, there is evidence that insurers move drugs associated with patients with expensive chronic conditions to high cost-

\(^{187}\) Kate Crawford and Jason Schultz, Big Data and Due Process: Toward A Framework To Redress Predictive Privacy Harms, 55 B.C. L. REV. 93, 106 (2014)  
\(^{189}\) See e.g., Jordan Robertson, The Pitfalls of Health-Care Companies’ Addiction to Big Data, BNA BLOOMBERG HEALTH IT LAW & INDUSTRY REPORT, Sept. 23 2015, http://news.bna.com/hil/HILNWB/split_display.adp?fedfid=76390826&vname=hitrbulalli\issues&jd=a0h3f2f8b60&split=0 (paywall)
sharing tiers in the hope of discouraging those patients from applying for coverage. As a result unregulated big data has the potential to frustrate some of the mainstay policies of our healthcare system.

C. Example Two: Mobile Health Data

The defining characteristic of mobile health is that it is patient-facing. That is, unlike most examples of digital health, patients or pre-patients interact directly with mobile health hardware and software, frequently without the direct involvement of conventional health-care providers. Most of these relationships are formed and interactions occur in consumer rather than professional space. As a result, serious turbulence even regulatory disruption can occur. In some ways emerging mobile healthcare services mirror the Uber-Lyft model. Like those car services mobile health steps around bureaucracy-laden incumbents that have been slow to adopt information technologies, reform their guilds, modernize their financing, or offer coherent alternatives to inconvenient centralized locations.

As a result, mobile health, a combination of mobile health apps, wearable devices, and the rapidly iterating Internet of Health Things, suggest some healthcare business disruption. Specifically, mobile health promises personalized care, improved convenience, and lower cost.

Of course, the HIPAA privacy and security rules apply to traditional healthcare providers such as doctors and hospitals. Therefore, if a hospital or health insurer (or a business associate) builds a patient portal app to provide access to EMR or claims information HIPAA likely applies. However, the vast majority of health apps are not curated, sold or implemented by HIPAA “covered entities”; they are built by technology companies and sold through app stores. As a result, much of the fitness and health data collected by mobile apps and wearables have very thin legal protection.

This also seems to be the case with mobile platform health data aggregators and APIs such as those offered by Apple with its “Health” app and HealthKit SDK. Platform developers appear to take the position that their


\[191\] See generally https://developer.apple.com/healthkit/
apps do not access any HIPAA-protected data but merely act as traffic cops working at the direction of the data subject. Take as an example a patient who uses a tracker to collect health data and who wants to share that with his or her healthcare providers’ patient portal app. The sharing is facilitated through the mobile platform health app. If that app is only opening and closing doors at the instructions of the patient then, the argument is made, the platform app is not “touching” the any HIPAA data.\(^{192}\)

Tens of thousands of mobile health apps are now collecting vast quantities of healthcare data. However, the majority of these apps are operating in the HIPAA-free zone with little or no regulation as to how they should share data with third parties or what the security is expected of any off-device data storage. Of course, some app/wearable developers (no doubt with an eye on the growing market for “wellness” products being promoted or required by insurers and employers) are beginning to advertise HIPAA-compliance.\(^{193}\)

The mobile health app space is a perfect breeding ground for regulatory disruption and arbitrage. The professional domain is highly regulated by HIPAA but the consumer domain is either unregulated or less regulated (limited to \textit{ab initio} app store\(^ {194}\) or \textit{ex post facto} FTC\(^ {195}\) regulation). Disruption and arbitrage in this mobile space are ongoing, as can be seen from the dysfunctional state of medical device regulation.\(^ {196}\)

Privacy and security issues are mounting. One recent study found that “that on average 87.7\% of Android devices are exposed to at least one of 11 known critical vulnerabilities.”\(^ {197}\) More pointedly, Huckvale and colleagues recently examined the privacy and security risks of mobile health apps that

had been accredited (for clinical safety) by the English National Health Service (NHS) Health Apps Library. Overall the study found a low level of encryption of user data at rest (on the device) or in motion and a lack of transparency in privacy policies. In a 2016 report funded by the Office of the Privacy Commissioner of Canada Hilts and colleagues documented how fitness trackers (Apple’s Watch aside) emitted persistent unique identifiers that could enable tracking of users and that several also had other basic security flaws, including a failure to encrypt data in motion.

VI. Data Protection versus Data Liquidity

Calls for increased data liquidity to further fuel the information society are hardly new. In the healthcare domain they frequently translate into public goods arguments. Further, in the traditional healthcare space there are some critically important policy initiatives that often are cast as at odds with existing HIPAA protections, let alone any increased upstream data protection. Currently these include clinical interoperability and medical research.

A. Clinical Interoperability

Interoperability began with a plan announced by President Bush in 2004 “to ensure that most Americans have electronic health records within the next 10 years.” Moving from paper to electronic records merely substitutes electronic solos for their file room predecessors. Thus, that 10-year plan rotated around the implementation of interoperable records. However, by 2009 “information systems in more than 90% of U.S. hospitals [did] not even meet the requirement for a basic electronic-records system.” Not surprisingly therefore the federal government’s Meaningful Use subsidy

---


program, introduced by the HITECH Act, made interoperability a major goal, albeit one that has proven particularly difficult to execute on.

The search for the magic bullet that will make clinical data more liquid within professional healthcare space has implicated HIPAA privacy. Specifically, there are concerns that rigorous downstream data protection models impede data sharing. For example, a 2015 ONC report found that “privacy and security laws are cited in circumstances in which they do not in fact impose restrictions” such as when “providers … cite the HIPAA Privacy Rule as a reason for denying the exchange of electronic protected health information for treatment purposes, when the Rule specifically permits such disclosures.”

In its interoperability roadmap ONC has laid out a ten-year plan for converting U.S. healthcare into a truly interoperable learning healthcare system. Throughout, the report stresses that data protection will not suffer:

It is essential to maintain public trust that health information is safe and secure. To better establish and maintain that trust, stakeholders will strive to ensure that appropriate, strong and effective safeguards for electronic health information are in place as interoperability increases across the industry.

Interestingly the report also calls on stakeholders to “support greater transparency for individuals regarding the business practices of entities that use their data, particularly those that are not covered by the HIPAA Privacy and Security Rules, while considering the preferences of individuals,” a

203 See Deth Sao, J.D., Amar Gupta, Ph.D., M.S., David A. Gantz, J.D., Interoperable Electronic Health Care Record: A Case for Adoption of a National Standard to Stem the Ongoing Health Care Crisis, 34 J. LEGAL MED. 55 (2013).
208 Id.
somewhat dejected admission that a dysfunctional regulatory system increasingly is hopeful of corporate stakeholder empathy.

Notwithstanding the pressure to increase data interoperability and exchange policymakers will continue to embrace claims to reduce some of the exceptional protections granted healthcare data. The most likely initial casualty is the additionally exceptional protections currently granted behavioral health records. Although SAMSHA delivered on its promise to deliver an updated draft regulation this year an updated regulation within the next eighteen months, its Congressional critics remain unimpressed.

In the next few years the increasingly difficult task for policymakers will be to distinguish between first, the “noise” of overstating HIPAA barriers, second, attempts to use the goal of enhanced interoperability as a straw man designed to increase commercial expropriation of clinical data and third, genuine, nuanced policy collisions that require resolution (including data protection deprecation).

B. Medical and Population Health Research

Claims on clinical and medically inflected and health-determining data for research purposes are also increasing. Much of the research is taking place within clinical space (particularly outcomes research which healthcare providers claim is covered by HIPAA’s permitted use exception for “healthcare operations”). Other research involves big data analytics (examples include the President’s Precision Medicine Initiative and the NIH’s Big Data to Knowledge program) and typically uses deidentified clinical data or an identified “limited data set” subject to a data use agreement. As noted by Barbara Evans, “A major challenge in twenty-first century privacy law and research ethics will be to come to terms with

209 Text accompanying note 139 et seq.
210 Text accompanying 139
211 “This regulations [sic] continues the redundant multiple-step process that makes it a huge burden for patients, providers, and health care professionals that could make it difficult for a provider to get relevant information quickly and it is a barrier to integrated care,” Morning eHealth, Politico, Feb. 8, 2016 (quoting email from office of Rep. Murphy), http://www.politico.com/tipsheets/morning-ehealth/2016/02/senate-help-alters-its-health-it-draft-212591
212 45 CFR §164.506
213 https://www.whitehouse.gov/precision-medicine
214 https://datascience.nih.gov/bd2k
215 45 CFR §164.514
the inherently collective nature of knowledge generation in a world where large-scale informational research is set to play a more prominent role."

Jane Bambauer goes further, arguing (with no apparent support) that, because HIPAA “attempt[s] to anticipate and account for every public policy override, and set an otherwise inflexible rule of nondisclosure,” its “privacy provisions have had perverse effects on access to critical research data, quality of care, and overall public health.”

That tension between data protection and responsible research will only increase. Furthermore, technology continually chisels away at the professional-consumer healthcare space divide. For example, the IoM has recommended that some social and economic determinants of health should be recorded in EHRs, adding social media to clinical data shows promise, while, increasingly, clinical research is occurring outside of recognized professional spaces using crowdsourcing or mobile apps such as those built around Apple’s ResearchKit.

C. Refuting the Binary

Overall arguments about clinical operability, medical research, or positive disruption suffer from one consistent flaw. They all posit unsupported, simplistic binaries, painting “privacy” as oppositional to innovation or progress.

Take a recent opinion piece David Agus seemed to be adopting the anti-HIPAA rhetoric of medical research trumping privacy when he argued: “Patients understandably don’t want their acquaintances and employers to know all their private health information. But we cannot let these fears

---

suppress the powerful insights medical data can offer us.”\textsuperscript{221} Yet, elsewhere in the piece he argued for increased data encryption and other security, careful protection against healthcare data-driven discrimination and generally seemed to be arguing for the sharing of deidentified information. Indeed, and as argued above, “privacy” is not a single concept but rather is descriptive of a broad array of upstream and downstream protective. As a result, different tools can be used to protect “privacy” of particular data types or when used for particular purposes.

Any positive disruption argument is similarly flawed. We can have data market disruption or mobile health disruption, but neither need to endanger properly calibrated healthcare data protection.

VII. Responding to Disruption and Arbitrage in Healthcare Data Protection

In the face of the regulatory disruption and arbitrage described above it should be no surprise that additional data protection is required to safeguard healthcare information that resides outside of traditional, highly regulated space. First, however, some timing and stylistic considerations need to be dealt with, together with the question whether additional protections need to continue the tradition of exceptionalism.

A. When to Regulate, Leading Edge or Trailing Edge?

Is it possible to put a positive spin on disruption? Returning once again to the analogy of mobile health and ride-hailing apps, there seems little doubt that the traditional taxi industry presents with serious anti-competitive properties; a guild mentality, non-market limitations on the number of market participants via medallions, and agency capture to name just a few.\textsuperscript{222} Is there an argument to be made that regulatory disruption does what policymakers often fail to do; to take a clean-sheet look at the regulation of innovative businesses rather than simply apply or add to the sedimentary layers of outdated laws.

\textsuperscript{221} David B. Agus, Give Up Your Data to Cure Disease, NY TIMES, Feb. 6, 2016, http://www.nytimes.com/2016/02/07/opinion/sunday/give-up-your-data-to-cure-disease.html?_r=1

Of course, healthcare makes the taxi industry look like a candidate for a Nobel prize in economics. Indeed, there is nothing novel about the observation that healthcare fails to obey most market norms. Equally it is well known that at various times physicians, hospital administrators, and insurers have held market controlling positions. Examples are legion and regulators such as the FTC do rail against some of the worst market abuses. For example, in North Carolina State Bd. of Dental Examiners v. F.T.C., Justice Kennedy denied application of state antitrust immunity when government “abandon[s] markets to the unsupervised control of active market participants, whether trade associations or hybrid agencies.” However, for every attempt to limit, say, guild power there are defeats elsewhere. For example, the Federal Trade Commission and the Antitrust Division of the U.S. Department have been sharply critical of healthcare’s “medallion” systems such as state requirements for Certificates of Need (CON): “CON laws raise considerable competitive concerns and generally do not appear to have achieved their intended benefits for health care consumers. For these reasons, the Agencies historically have suggested that states consider repeal or retrenchment of their CON laws.” Yet, most courts seem unimpressed by legal challenges to these relics of 1970s centralized planning.

Are, therefore, big data and mobile health disruptions positives? After all, entrenched stakeholders (incumbents) seem to have little interest in positively reforming data protection regimes. This is not always because of a genuine commitment to patient privacy. Rather healthcare stakeholders frequently view patient data as proprietary and will use the excuse of privacy to keep such valuable assets close. “Disruption as laboratory” is also a tempting model because of the current tension between data protection and data liquidity. In the words of Cisco executive Shanti

---

224 See e.g., PAUL STARR, THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE (1982).
228 See e.g., Colon Health Centers of America, LLC v. Hazel, _ F.3d _ 2016 WL 241392 (4th Cir. 2016).
Gidwani, “Disruptive is a good thing… It moves us to be transformational and innovative.”

B. A Different Type of Laboratory, the States

With federal law showing disruption and arbitrage and the absence of any clear legislative or regulatory paths could might state law fulfil its laboratory goal while also providing some stopgap measures? Clearly states do operate in this space, although they may not conceptualize their actions as data protection. Take, for example, the impact of past criminal records on employment decisions. Federal law, represented by EEOC Guidance, takes the position that the overrepresentation of persons of color in “contact with the criminal justice system” could impact some discriminatory hiring or other employment decisions. In contrast, several states have taken a far more direct approach, enacting “second chance” laws that permit convicted persons to withhold information about expunged crimes.

In the healthcare data protection space few states have moved far from the HIPAA norm. Even California’s CMIA, long held out as the model for regulation that goes beyond HIPAA does little to deal with the disruption and arbitrage discussed here. At first sight the statute’s inclusion of “[a]ny business that offers software or hardware to consumers … shall be deemed to be a provider of health care” suggests the obvious. However, additional verbiage and a cross-reference suggest that in reality regulatory coverage is only extended to some PHRs.

Texas goes further, more successfully increasing the scope of healthcare data protection (albeit still concentrating on downstream models). For example, the Texas statute uses a far broader definition of “covered entity” than HIPAA to include a “business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person

---

229 Jeremy Hainsworth, Disruptive technologies can enhance privacy and improve health-care. BNA SNAPSHOT, Feb. 8, 2016.
232 Cal. Civ. Code D. 1, Pt. 2.6
233 Cal. Civ. Code §56.06(b)
who maintains an Internet site.”\textsuperscript{234} The statute also prohibits unconsented to reidentification\textsuperscript{235} and the sale of PHI.\textsuperscript{236}

The “laboratory of the states” argument is always attractive during a time of Congressional logjam. Clearly some stakeholders are paying careful attention to forthcoming state privacy legislation (although for now there is little in the way of healthcare data protection). For example, the Tenth Amendment Center and the ACLU recently participated in the coordinated announcement of various state data protection measures, primarily aimed at reducing surveillance.\textsuperscript{237}

C. What Style of Regulation is Appropriate for Disruptive Technologies?

Nathan Cortez has offered a thoughtful critique of the conventional wisdom as to how agencies should regulate disruptive businesses.\textsuperscript{238} His starting point is Tim Wu’s context-based defense of “agency threats,” sub-regulatory signals that include “statements of best practices, interpretative guides, private warning letters, and press releases”\textsuperscript{239} directed at industries facing uncertainty or disruption.\textsuperscript{240}

Threats are not intended as a permanent solution, but rather as part of a longer process. If successful and widely respected, it is possible that a threat may create an industry norm, removing the need for rulemaking at all. Alternatively, a threat regime may be a pilot, as it were, for eventual lawmaking. The law created by rulemaking or adjudication will then benefit from the facts developed under the threat regime.\textsuperscript{241}

\begin{flushright}
\textsuperscript{234} V.T.C.A., Health & Safety Code § 181.001(a)(2)
\textsuperscript{235} V.T.C.A., Health & Safety Code § 181.151
\textsuperscript{236} V.T.C.A., Health & Safety Code § 181.153
\textsuperscript{237} Tenth Amendment Center, 16 States Simultaneously Announce Efforts to Protect Privacy, #TakeCTRL, Jan. 20, 2016, \url{http://tenthamendmentcenter.com/2016/01/20/16-states-simultaneously-announce-efforts-to-protect-privacy/}. See generally Hamza Shaban, 
\textsuperscript{238} Nathan Cortez, Regulating Disruptive Innovation, 29 BERKELEY TECH. L.J. 173 (2014).
\textsuperscript{239} Tim Wu, Agency Threats, 60 DUKE L.J. 1841, 1841 (2011).
\textsuperscript{240} Id. At 1848.
\textsuperscript{241} Id. At 1851.
\end{flushright}
Cortez’s opposing argument is that agencies “agencies need not be so deliberate and tentative with regulating innovations—even disruptive ones.” Rather “[t]he public interest demands that agencies maintain their fortitude in the face of regulatory disruption. And, somewhat counterintuitively, new technologies can benefit from decisive, well-timed regulation.”

Cortez argues, “The trick is to craft enduring policy under high uncertainty,” suggesting the use of “sunsets” and “deadlines.”

An early sign of regulatory disruption in the mobile health space was with regard to patient safety. The app/wearable industry first took a gamification approach with their fitness and wellness apps and wearables. were achieving positive health results because of. The FDA essentially ceded its regulatory territory with a sub-regulatory Guidance as to which mobile apps it would choose to regulate under section 201(h) of the Federal Food, Drug, and Cosmetic Act. Under this Guidance FDA elected to exercise regulatory discretion over common health related apps such as trackers.

Rather than solve problems the guidance seems to have had the opposite effect (arguably supporting Cortez’s arguments). For example, Apple omitted health-monitoring features such as blood pressure and stress level when it launched Apple Watch in 2015. It is widely believed that this decision was made, at least in part, because of regulatory concerns. Subsequently, Apple CEO Tim Cook stated:

We don’t want to put the watch through the Food and Drug Administration (FDA) process. I wouldn’t mind putting something adjacent to the watch through it, but not the watch, because it would hold us back from innovating too much, the cycles are too long. But you can begin to envision other things that might be adjacent to it -- maybe an app, maybe something else.

---

242 Cortez, supra at 225.
243 Cortez, supra at 177-78.
244 Cortez, supra at 215.
247 Allister Heath, Apple's Tim Cook declares the end of the PC and hints at new medical product, DAILY TELEGRAPH, NOV. 10, 2015,
In fact, FDA practice suggests a very light regulatory hand, featuring not only sub-regulatory guidance but also under-enforcement. For example, so far the agency has only reined in one mobile app developer.\textsuperscript{248} Not surprisingly developers are selling apps that apparently perform medical device functions yet which are “saved” from regulation by “small print” characterizations. For example, take the app “Instant Blood Pressure.” Its developer includes the following in its FAQ:

> Instant blood pressure is not a medical device. It is for recreational use only. It is not a replacement for a medical grade blood pressure monitor. It is not intended for use in and should not be used for the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease.\textsuperscript{249}

As a matter of law this statement is not determinative as the manufacturer’s intent is objectively determined.\textsuperscript{250} However, statements like this, and there are many similar statements included with other app store apps, at least temporarily allow for arbitrage as the app is characterized as consumer rather than professional in nature.

Regarding healthcare data protection HHS simply lacks regulatory authority over most of the mobile health activity. Even a guidance likely would be viewed as overreaching. The furthest HHS’s Office for Civil Rights has been to post a lightly-trafficked Q&A page for health app developers.\textsuperscript{251}

The FDA has entered the data protection space with a series of sub-regulatory guidances on device security.\textsuperscript{252} In a recent draft guidance, FDA

\textsuperscript{248} Letter to Biosense Technologies Private Limited concerning the uChek Urine Analyzer, http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm
\textsuperscript{249} http://www.instantbloodpressure.com/support/
\textsuperscript{250} 21 CFR §801.4
\textsuperscript{251} HHS-OCR, Health app developers: Questions about HIPAA? http://hipaaqsportal.hhs.gov/a/home
“emphasize[d] that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.”\footnote{And recently Draft Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices, Jan. 22, 2016, at 4, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf} Presumably, however, even this guidance would not apply to mobile medical apps that are currently excluded from device regulation under the 2015 Guidance.\footnote{Text accompanying note 245}

In 2013 the FTC published a lower-level sub-regulatory “guide,” \textit{Marketing Your Mobile App: Get It Right from the Start}, that urged transparency, truthfulness, consent and data minimization:

Under the law, you still have to take reasonable steps to keep sensitive data secure. One way to make that task easier: If you don’t have a specific need for the information, don’t collect it in the first place. The wisest policy is to:

1. collect only the data you need;
2. secure the data you keep by taking reasonable precautions against well-known security risks;
3. limit access to a need-to-know basis; and
4. safely dispose of data you no longer need.\footnote{https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start}


\footnotesize

\textsuperscript{254} Text accompanying note 245  
\textsuperscript{255} https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start  
\textsuperscript{257} See e.g., In the matter of Nomi Technologies, Inc., https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter  
Because of the threats to healthcare data protection legislation providing for data minimization and context-based limitations is urgently required. However, in the interim highly targeted legislation providing for explicit consent is worth consideration. In its data brokers report the FTC urged:

Congress should … consider imposing important protections for sensitive information, such as certain health information, by requiring that consumer-facing sources obtain consumers’ affirmative express consent before collecting and sharing such information with data brokers.\textsuperscript{259}

Such baseline legislation likely would satisfy Cortez’s “enduring policy” goal while other, more comprehensive proposals are explored through guidances and codes of conduct.

\section*{D. The Level of Regulation: The Case for Continued Exceptionalism}

There seem to be few arguments that healthcare data are not sensitive and deserving of protection. However, in today’s environment should health privacy advocates throw in their lot with those arguing for heightened protection across all domains? This section asks whether continuing calls for health data protection exceptionalism have any particular salience? Several claims seem to have merit.

First, from earliest times the physician-patient-data relationship has involved special data obligations. A patient holds health information (either literally or as data that can be released during diagnosis). The patient’s rights over this data are protected by both ethical and legal (for example, the seclusion tort) principles; an autonomy model requiring consent to data sharing.\textsuperscript{260} Thus, in both the legal and ethical senses the patient (instrumentally) exercises this right of privacy when the patient gives a physician access to these data. In exchange for that consent the physician agrees to hold the data in confidence, an obligation sourced in ethical


\textsuperscript{260} “The primary justification seems closer to respect for autonomy… We owe respect in the sense of deference to persons’ autonomous wishes not to be observed, touched, intruded on, and the like. The right to authorize or decline access is basic.” TOM L. BEAUCHAMP AND JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS, 313-14 (7th ed 2013).
frameworks, the confidence tort, and ethical-legal hybrids such as the duty owed by fiduciaries.\textsuperscript{261} In the words of Bill Gardner:

[H]ealth services data are the residue of the touches of living persons against the health care system. As such, they reflect the experience of those patients, even if such effects are often obscure to the analyst. The data are lit from from within by the experience of patients, even if only faintly. Medical data are the relics of human suffering, recovery, and death. We wouldn’t be looking at them if there wasn’t a signal there.\textsuperscript{262}

In the healthcare domain, therefore, there is a deep, culturally significant, relationship-based demand for the strongest level of data protection. As noted by the HITPC in 2010, “The relationship between the patient and his or her healthcare provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information.”\textsuperscript{263}

Second, patients have been conditioned to disclose all data to their healthcare providers on the basis of this very promise; that such data will be protected like no other. This somewhat reductionist argument should not be dismissed lightly. Patients have grown up with a system that has seemed impervious to even basic data sharing. Almost every visit to a provider involves filling out a new intake form or, at least, updating insurance and other personal information. As had been argued, “[p]atients should not be surprised about or harmed by collections, uses, or disclosures of their information.”\textsuperscript{264} For the past 15 years almost every healthcare encounter will have been marked by the production of a HIPAA privacy notice,\textsuperscript{265} the right to inspect and obtain copies,\textsuperscript{266} and receive an accounting of

\textsuperscript{261} See generally Nicolas Terry, What’s Wrong with Health Privacy? 5 J. HEALTH & BIO. L. 1-32 (2009). See also SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2012) (describing operation of “communication privacy management” such that “when a person confides, the recipient is held responsible for the information and a set of expectations is communicated by the discloser.”) (at p.28)
\textsuperscript{265} 45 CFR 164.520
\textsuperscript{266} 45 CFR 164.524
disclosures.\textsuperscript{267} Think of the surprise, the dashed expectations if a patient was to find that his or her data no longer was exceptionally protected because of an informational accident as to where they were created (e.g., on a smartphone) or who was their curator (a data broker).

Third, exceptional protection is deserved in the face of exceptional threats. Healthcare data is a hot commodity on the dark web.\textsuperscript{268} It is the fastest growing target for cyber attacks\textsuperscript{269} accounting for 21\% of data breaches globally,\textsuperscript{270} data brokers see a strong market for health-based ratings products, and app stores are being populated by tens of thousands of health and wellness apps often of dubious provenance. However, even respectable outcomes and human subjects researchers covet clinical data at a time when the choice architecture for patient consent has not been agreed upon.

Fourth, healthcare data seems particularly susceptible to discriminatory and other harmful uses. As noted in the 2015 HITPC report, under U.S. law some “discriminatory uses of health information are either not prohibited or are expressly permitted (for example, use of health information in life and disability insurance decisions).”\textsuperscript{271} The report also acknowledged, “a lack of consensus on which uses are “harmful,” particularly with respect to health big data analytics, as well as an inability to predict which future uses could be harmful and which beneficial, creating challenges to enacting policies to prohibit or place additional constraints on such uses.”\textsuperscript{272} However, the real issue here is that the use of healthcare data outside of the clinical setting with the potential for real or perceived harms will devastate the trust that accompanied the initial patient sharing of data with the provider. Without

\textsuperscript{267} 45 CFR 164.528
\textsuperscript{268} See generally \url{http://www.huffingtonpost.com/entry/what-is-the-dark-web_55d48c50e4b0ab468d9f17d7}
\textsuperscript{271} Health IT Policy Committee Privacy and Security Workgroup, Recommendations on Health Big Data, at 12 \url{http://www.healthit.gov/facas/sites/faca/files/HITPC_Draft_PSWG_Big_Data_Transmittal_2015-08-11.pdf}
\textsuperscript{272} Id. 12-13
trust patients will share less, and both their clinical care and the responsible research that could be performed using those data will suffer. 273

Finally, while as citizens we may generally view the market as the best available solution to our problems and support the liquidity of data that fosters innovation, we continue to stake out some limits. Policymakers have spent untold energy in trying to reverse healthcare’s chronic market failure274 and make it work more like other “normal” products and services. But in the words of David Blumenthal, “[p]eople feel differently” about healthcare “than they do about the myriad other things that get bought and sold, without controversy, in normal markets.” And, as result “[g]overnment is involved in health care because Americans deeply desire the health care protections government provides.”275 In short, data protection regarding our healthcare is important enough to us to warrant exceptional protection.

VIII. Moving Beyond HIPAA, Exploring the Potential of Multiple Data Protection Models

Privacy policymakers and champions for regulation have pushed back against data brokers accusing them of expropriation276 and encouraging data determinism.277 In many cases the same accusations can be made against those collecting data with mobile apps (particularly those selling the data to big data brokers). In the The Black Box Society Frank Pasquale described how those data-gathering and analytic tools can impact healthcare data subjects:

[A] “body score” may someday be even more important than your credit score. Mobile medical apps and social networks offer powerful opportunities to find support, form communities, and

273 “Failing to pay attention to these issues undermines trust in health big data analytics, which could create obstacles to leveraging health big data to achieve gains in health and well-being.” Id at 13.
address health issues. But they also offer unprecedented surveillance of health data, largely ungoverned by traditional health privacy laws (which focus on doctors, hospitals, and insurers). Furthermore, they open the door to frightening and manipulative uses of that data by ranking intermediaries—data scorers and brokers—and the businesses, employers, and government agencies they inform.278

In its 2014 report on data brokers’ practices the FTC noted how health information or medically-inflected data was used to create “potentially sensitive categories [that] highlight[e] certain health-related topics or conditions, such as “Expectant Parent,” “Diabetes Interest,” and “Cholesterol Focus.””279 In Here’s looking at you, the California HealthCare Foundation noted:

Consumer scores are now ubiquitous across people’s activities: financial and credit, energy use, law enforcement, environmental, social clout, tax returns, environmental “green-ness,” and health. In 2014, there were at least a dozen health scores available in the marketplace, including the Affordable Care Act (ACA) Individual Health Risk Score, FICO Medication Adherence Score, several frailty scores, personal health scores (e.g., WebMD, One Health Score), and medical complexity scores (e.g., Aristotle for scoring of surgery for congenital health conditions). Consumers are largely unaware of the existence and use of these scores and the algorithms that create them.280

Notwithstanding its flaws HIPAA was a reasonable approach to healthcare data protection in the last decade of the twentieth century. Then, both “privacy” and security threats primarily arose from inside the health care system. Data protection required an update from haphazard nature of state confidentiality-based protections as the industry swapped PCs for paper, while hospital IT needed a solid nudge to lock some doors and reduce the number of stolen laptops and thumb drives. As such combining a solid (if

exclusively downstream), national HIPAA floor and compliance-based policing made some sense.

Fast-forward to 2009 and policymakers seemed unable to look to the future. The HITECH Act was designed to improve the HIPAA system just enough to absorb the EHRs the unprecedented growth of which the same legislation was about to subsidize.\textsuperscript{281} The only attempt to think outside the hospital-based technology box was the introduction of a breach notification rule for PHRs. Yet, the implications of big data mining and data aggregation were already being discussed and the iPhone’s introduction in 2007\textsuperscript{282} followed year later by its app store\textsuperscript{283} suggested the birth of a mobile revolution.

The closing argument of this article is that today the traditional, exceptional, justifiably high protection of healthcare data is seriously threatened by the disruption and arbitrage displayed in big data and mobile spaces. Waiting in the wings are other threats from emerging, more autonomous technologies such as the IoT, self-driving vehicles, and robots.\textsuperscript{284}

By far the most appropriate solution would be for Congress to enact a new (hopefully FIPPS-rich) federal privacy code and/or give rule-making power to the FTC or some new data protection agency (perhaps a model based on Senator Elizabeth Warren’s Consumer Financial Protection Bureau\textsuperscript{285}). Any code or regulations could apply equally to all data types. Or, as seems more likely, could also single out certain sensitive data types such as health data for additional protection.

In large part (but not exclusively) framed by the explosion of big data services, various branches of the federal government published privacy reports and proposals between 2012-2015. All favored increased regulation (including data brokers), yet failed to agree on much else.\textsuperscript{286} Thereafter, and

---

\textsuperscript{281} See generally Nicolas Terry, \textit{Meaningful Adoption: What We Know or Think We Know about the Financing, Effectiveness, Quality, and Safety of Electronic Medical Records}, 34 J. LEGAL MEDICINE, 7 (2013).
\textsuperscript{283} http://techcrunch.com/2008/07/10/app-stor
\textsuperscript{285} http://www.consumerfinance.gov

Absent broad privacy legislation what health-specific provisions would be most effective in reducing or eliminating regulatory disruption and arbitrage in healthcare data protection?

One obvious approach would be to extend HIPAA applicability to all custodians or processors of healthcare data. Consider for a moment an analogous, superficially attractive yet ultimately naïve approach to healthcare reform; Medicare for All, achieved simply by removing the remove age eligibility from federal coverage and, with a single stroke of the pen, thereby creating a single payer, universal care healthcare system.\footnote{Nancy Altman, \textit{How and Why Medicare for All Is a Realistic Goal}, Huffington Post, Jan 24, 2016, \url{http://www.huffingtonpost.com/nancy-altman/how-and-why-medicare-for_all_9063970.html}} Yet, whether judged though political, constitutional, or organizational lenses it isn’t that simple. As Harold Pollack notes,

Medicare for All cannot offer itself as the replacement of our depressing health politics. It would have to arise as another product of that very same process, passing through the very same legislative choke points, constrained by the very same path dependencies that bedevil the ACA.\footnote{Harold Pollack, \textit{Medicare for All—If It Were Politically Possible—Would Necessarily Replicate the Defects of Our Current System}, JHPPL, Jun. 29, 2015.}
Similarly, the answer to whether HIPAA should be broadened with a single stroke of the pen also must be “no.” Such an extension of HIPAA is not rejected on normative grounds. Healthcare data residing outside traditional healthcare space should receive no less protection than that inside it. Indeed, a good argument can be made that the former deserves more legal protection because healthcare insiders are additionally constrained or policed by professional standards and ethics thus reducing data subjects’ privacy risks. HIPAA’s approach to data protection is exclusively mapped to and calibrated for the traditional healthcare domain. The existential threats to healthcare data protection are from outside of the professional domain and they are not threats that can be countered (only) with downstream data protection models. HIPAA was specifically designed to map (whether successfully or not) to professional healthcare workflows and issues. Any fundamental broadening of its scope would be highly problematic. Of the greatest importance, however, is that the data protection problems highlighted by big data and mobile health suggest that upstream regulatory models are required, not the types of downstream protections (HIPAA privacy, security and breach notification) offered by HIPAA.

The preferred solution (again assuming the absence of a modern, generalized data protection law such the forthcoming EU General Data Protection Regulation[290]) is to keep HIPAA, albeit with some modifications, but to supplement it with highly targeted provisions aimed at both upstream and downstream issues exploited by health privacy disruptors.

The HIPAA Privacy Rule should be amended as follows to require:

- Any deidentified data derived from patient clinical information should be subject to a data use agreement prohibiting reidentification.
- Opt-out consent of patients with regard to the research use by covered entities or NIH-funded entities of any data derived from patient clinical information.
- Opt-in consent of patients with regard to the research use by other entities of any data derived from patient clinical information.

At the minimum new federal legislation should provide:

- Any wellness, health, sickness, or medically-inflected data collected by non-HIPAA covered entities must only be used for the limited purpose for which it was collected.

(this document does not yet synthesize the various changes required by other EU institutions, a documented expected in late 2015).
• Consumer-facing sources must obtain consumers’ affirmative express consent before collecting and sharing such information with data brokers.291
• Expanded point-of-use prohibitions on discriminatory uses of wellness, health, sickness, or medically-inflected data.
• Data custodians are prohibited from re-identifying or attempting to re-identify any individual who is the subject of protected health information that has been deidentified.292
• All custodians of health, sickness, or medically-inflected data or data derived from health, sickness, or medically-inflected data must provide access to the data upon request from any identified or identifiable data subject and implement systems enabling correction or deletion of such data.
• All consumer-facing applications (apps) that collect, process, or transfer data must use encryption for data in motion and at rest.

IX. Conclusion

At the root of the arguments advanced in this article is one unassailable fact; vast quantities of healthcare data are now being exported to, or created outside of HIPAA-protected space. The upshot is a dramatically uneven policy environment. Vast amounts of healthcare-like data increasingly benefit from low or no data protection. These “protections” are being applied to similar data not on the basis of any rational distinctions but on the basis of an accident of creation or current, possibly transient, state. Healthcare professionals, patients, pre-patients and responsible data processors all suffer mightily from this uneven policy environment.

There is little doubt that increasingly our “medical selves” will (and should) exist outside of the traditional (and HIPAA-regulated) healthcare domain. However, as regulatory disruption and arbitrage increase, this will create increasingly exploitable confusion as health information moves in and out of differentially protected domains. There is now massive commercial value to be extracted from healthcare data leading data aggregators and processors to perform an end-run around healthcare’s domain-specific protections by creating medical profiles (HIPAA proxies) of individuals in HIPAA-free space. This will only increase as the possibilities of the IoT, robotics,

291 The FTC proposal from 2014 discussed above.
292 Based on the Texas provision discussed above.
autonomous vehicles, and technologies not yet imagined interact with our medical selves.

Unfortunately, as Fleischer recognized, “[i]n the [last] twenty-five years… the administrative state has increased substantially, and the amount of time lawyers devote to regulatory matters has grown apace.” As a result “[t]he complexity of the modern administrative state provides more opportunities for regulatory arbitrage—another form of value creation for the client--than ever before.” Yet, as Brad Smith, Microsoft’s Chief Legal Officer, recently noted in the context of the collapse of U.S.-EU safe harbor, “privacy rights cannot endure if they change every time data moves from one location to another. Individuals should not lose their fundamental rights simply because their personal information crosses a border.”

Or, in this case from a hospital EHR to an iPhone.

Some policymakers now recognize (albeit belatedly) that the protection of healthcare data is diminished when it is created in or migrates to the HIPAA-free zone; a place of considerably reduced, even zero data protection. There has also been some recognition that this new state results in regulatory turbulence, disruption, and, at least in the case of big data, regulatory arbitrage. However, it less clear whether policymakers recognize the multi-faceted nature of the problem. Although a downstream, compliance-based data protection model such as HIPAA can deal with a relatively cohesive domain, it is ill-prepared for the variety of challenges when data are created outside of the that domain. As a result, merely extending the domain protection is unlikely to work well. Further, the dangers associated with a HIPAA-free zone are not limited to disruption because of uneven data protection domains, but are exacerbated by the chronic weaknesses of the non-HIPAA data protection models.

In 2009 the HITECH Act instructed HHS and FTC to “conduct a study, and submit a report … on privacy and security requirements for entities that are not covered entities or business associates.” This was to be followed by the HHS Secretary reporting to Congress “the findings of the study under … include[ing] in such report recommendations on the privacy and security requirements described in such paragraph.”

---

required this within one year of HITECH’s passage no report has materialized. The need for that report and proposals for legislation, particularly FIPPS-infused upstream protections, have never been greater.

In the meantime, the exceptional protection of health data is being deprecated. There are many reasons and forces conspiring to make this happen. Some are decisions that go back to the U.S. “original sin” of eschewing a comprehensive privacy law of general applicability. Some are instrumental-competing forces for data, be they commercial big-data brokers or the National Institutes of Health. Some are historical such as the traditional ways U.S. data protection has been structured-sectoral and downstream, characteristics that tend to create regulatory turbulence, even arbitrage. Some are technological as we come to terms with new generations of personal connected devices and the vast power of cloud-based data storage and analysis. Whether at root this is an issue of healthcare privacy exceptionalism or of the general inadequacy of data protection in the U.S. is somewhat moot. Exceptional health data protection must be re-energized and re-formulated.