Frontiers of Health Policy: Digital Data and Personalized Medicine

Amalia R. Miller* and Catherine Tucker‡

March 15, 2016

Abstract

This paper argues that due to two unstoppable forces some of the most pressing future questions in health policy will relate to the use of digital technologies to analyze data concerning patient health. The first force is the shift away from a system where patient data was essentially temporary and not intended to be reused or easily accessed again, to a new digital world where patient data is easily transferred and accessed repeatedly. The second force is a fundamental deepening of the nature of patient data that enables increased personalization of healthcare for each individual patient based on not only their detailed medical history but also their likely future medical history that can be projected for their genetic makeup. We summarize our research investigating the potential consequences of policies in this new world where patient data is both virtually costless to store and share and individualize. We emphasize that issues of data management and privacy are now at the forefront of health policy considerations.

*Economics Department, University of Virginia, Charlottesville, VA, IZA and NBER.
†MIT Sloan School of Management, MIT, Cambridge, MA and NBER.
‡Catherine Tucker thanks NSF Career Award 6923256 for research funding. All mistakes are ours alone.

Contents

Digital data and digital technologies have the potential to transform medicine through two mechanisms. First, digital patient data is far easier to share and access than traditional paper records. This has many potential upsides but also raises the question of how the potential benefits of sharing patient data are moderated by privacy concerns. Second, the advent of digital storage has now made it possible to store, virtually costlessly, vast swathes of data about any one individual patient. Such individualized data also enables a patient-centric approach to medicine often referred to as 'personalized' or 'precision' medicine that is based on that individual patient's genetic makeup.

This article discusses the potential benefits and possible policy consequences of this digital shift. It emphasizes that the benefits of digital technologies are found when data is actually transferred and repeatedly accessed. This emphasizes the desirability of policies that encourage the easy transfer of data. Empirical evidence suggests that healthcare providers may not individually have the right incentives to share data, and therefore there is a need to not only subsidize the adoption of digital technologies but making sure that there are the right incentives to use these technologies to share data. Often well meaning policies towards data security and data privacy can hamper this process. We argue that there are distinctive and separate concerns related to the deepening and individualizing of data that is associated with personalized medicine and that while there is potentially a large upside in terms of medical outcomes, the risks associated with this data are unusual and warrant an approach to data management that gives control of the use of the data to the patient.

It is worth noting that the digital shift is a consequence of a combination of complementary factors. The digitization of medical records which allows them to be both be reused and be more comprehensive rely on three complementary trends: First, the emergence of EMR software, second the declining cost of storage and personal computers, and third the increased technological sophistication of doctors who were raised in a generation where computer use was commonplace. Though by themselves none of these trends appears profound,

in combination we will argue that they will profoundly shift the policy agenda in healthcare.

1 Potential Positive Consequences of Easy Transfer of and Access to Digital Medical Records

1.1 Effects on health outcomes

The theoretical foundation for why healthcare information technology (IT) or digital patient record keeping may improve the quality of care has been developed in many scholarly and popular articles, such as Brailer (2005) and Hillestad et al. (2005). Improvements may stem from reduced error rates, especially from drug interactions, as well as improved patient monitoring.[1]

In this article, we want to emphasize that there is a theoretical distinction between the internal benefits of healthcare IT use at a particular clinical encounter and the broader benefits of being able to share data created by digital technologies. The existing literature suggests that the positive effects of health IT are most likely to occur where there is a compelling need for both data sharing and the rapid access features of digital health information.

To show this, we start off with a detailed description of our own work in the area. Miller and Tucker (2011a) studies the adoption of electronic medical records (EMRs) across twelve years of data.[2] We relate the level of adoption of electronic medical records with neonatal mortality in that county. Overall, we find that a 10 percent increase in births that occur in hospitals with EMRs reduces neonatal mortality by 16 deaths per 100,000 live births. This is important because each year 18,000 babies die in the United States within their first 28 days

[1]We also acknowledge that beyond the direct clinical advantages, healthcare IT can improve quality through improved measurement and data aggregation, which are vital elements of national programs to assess hospital quality (Jha et al., 2006) or to design appropriate performance-based incentives.

[2]We use technology data from the 2005 release of the Healthcare Information and Management Systems Society (HIMSS) Analytics^{TM} Database (HADB). This is a database that uses annual surveys to record the state of technology adoption for US hospitals who are part of HIMSS. These hospitals tended to be more urban and larger than the hospitals that we did not have technology adoption data for, reflecting the membership of HIMSS.

of life. This high rate of neonatal mortality means that the United States is ranked 43rd in the world, equal with Montenegro, Slovakia and the United Arab Emirates, and behind 24 of the 27 members of the European Union (UNICEF, 2009). Rough cost-effectiveness calculations suggest that EMRs are associated with a cost of $531,000 per baby's life saved.

Though these headline figures are informative for the overall effects on neonatal mortality, from a forward-looking policy perspective, it is also useful to consider the specific cases we identified where health IT lead to improvements in neonatal mortality and those where it did not. We found that the majority of births were not affected by healthcare IT. Instead, it was the high-risk cases which required intervention from specialists in maternal-fetal medicine which drove the reduction we saw in the data. It was the cases in particular where the mother had a pre-existing condition that were aided by technology. We did not see benefits in cases where technology could offer little help because the reason the birth was high-risk was due to a chromosomal or genetic defect.

One example of the kind of cases where outcomes were particularly enhanced from the adoption of healthcare IT is conditions associated with problems with the placenta. For example, a condition like placenta previa which is described by Iyasu et al. (1993) as something that can cause 'serious, occasionally fatal complications for fetuses and mothers', had outcomes that were particularly positively affected by the adoption of healthcare IT. Placenta previa occurs when a baby's placenta partially or totally covers a mother's cervix. It is also a condition that is detectable prior to birth through an ultrasound. While it can be successfully managed through a caesarian section, it is a condition that requires a great deal of care and planning regarding how the mother's labor is managed. For such conditions, though, it is clear why healthcare IT can potentially improve outcomes. It is not the simple efficiency or reduction in error keeping associated with digital technologies and the storage of data that explains the improvement. Instead, it is the ability to share the data from the ultrasound to other healthcare providers quickly and seamlessly.

We also show that there are additional benefits from incremental digital technologies that go beyond a typical digital records system and instead enhance the system with obstetric-specific technologies, digital technology and decision support.

The other factor we found that was important for explaining when healthcare IT was successful was the likelihood of the mother to successfully advocate for herself in a healthcare setting. We found little improvement for birth outcomes for mothers who were well educated, white and who could speak English well. Instead, the biggest improvement in outcomes was focused on the less educated, those for whom English was not their first language and historically racially disadvantaged groups. This is an important finding. Often technologies are found to aggravate existing disparities (Acemoglu, 2003). However, this appeared to be a technology where inequality in outcomes were reduced. A potential mechanism for this effect is that white, highly educated mothers for whom English was their first language found it easy to communicate any pre-existing conditions or other considerations which might affect the nature of their delivery and birth. However, for groups for whom communication was either hampered by language or potentially unconscious biases within the medical profession (Schulman et al., 1999) were helped by the presence and sharing of an existing digital record which did not require their individual communication to the medical team.

We want to emphasize that this paper is just part of a growing literature that attempts to understand in which settings healthcare IT improves health quality outcomes. Large national studies have related hospitals' adoption of electronic medical records (EMRs) and other forms of health IT to higher quality care, measured by process improvements and lower mortality. Some of this work suggests that there is little positive effect - for example Agha (2014) found little effect on mortality, adverse drug events or readmission rates using medicare patients. Similarly, Spetz et al. (2014) found little positive effects on nursing-sensitive outcomes using Veterans Health Administration Data.

However, there are some more positive findings such as McCullough et al. (2013), who

find that benefits to electronic patient data tend to occur only in settings where there is a severe case mix, or in other words very ill patients. They emphasize that 'benefits from health IT are primarily experienced by patients whose diagnoses require cross-specialty care coordination and extensive clinical information management'. Freedman et al. (2014) find some positive effects from the adoption of Computerized Physician Order Entry applications on a non-senior population in terms of decreasing preventable adverse effects. Work such as Gresenz et al. (2016) has also expanded the literature and shows reductions in ambulatory care sensitive hospitalizations in ambulatory centers that have adopted digital technologies. One potential explanation for the mixed outcomes of these studies is provided by Lin et al. (2014) who find that often adoption of digital technologies does not equate to their practical use. They find evidence that if one focuses on meaningful use rather than simply adoption that there is a positive effect in particular for small, non-teaching, or rural hospitals - in other words the kind of hospitals that have historically been isolated from technology and where the benefits of data-sharing may be most profound.

Taken together, this work emphasizes that by itself health care IT cannot be presumed to automatically improve health outcomes. Instead, there needs to be a compelling case whether the sharing of, coordination across and easy access to data may prove beneficial in that particular health circumstance.

1.2 Effects on costs

There is also the potential for the sharing of patient data to help avoid unnecessary costs. An obvious potential example of a cost reduction is in the ability to avoid duplicative testing. Lammers et al. (2014) show that the use of repeat CT scans, chest X-rays and ultrasound scans was significantly lower when patients had both their emergency visits at two unaffiliated hospitals that took part in a health information exchange. Specifically, they found evidence that patients were 59 percent less likely to have a redundant CT scan, 44 percent less likely

to get a redundant ultrasound, and 67 percent less likely to have a redundant chest X-ray when both their emergency visits were at hospitals that shared information with other health providers across a health information exchange.

Other cost savings stem from lowering administrative costs. Of course, such cost savings are traditionally thought to be gained through efficiencies in administration related to a digital rather than a paper environment. However though such arguments seem superficially compelling, countervailing forces exist that may limit or negate the cost savings associated with healthcare IT. The installation of an IT system may prove unsuccessful if providers and other staff resist changing their work patterns, or if they find that the computerization adds to their administrative burdens, introduces redundancy to documentation procedures, or is cumbersome to use.

Given that it is not theoretically clear whether IT will by itself reduce costs, it is perhaps not surprising that a simple attempt to correlate the adoption of digital technologies with the operating costs reported by hospitals in the annual American Hospital Association survey suggests if anything that there is a marginal increase in costs associated with the adoption of electronic health records, as documented by both Agha (2014) and Dranove et al. (2014). Dranove et al. (2014) also provide a potential answer to why the cost savings of such technologies have been less than hoped for. In particular, they explore how operating costs change over time after adoption. They show that it is only hospitals in locations where there is a local labor market focused on IT that experience in a decrease in costs after three years. Other hospitals still face slightly higher costs after six years. This provides suggestive evidence that by itself digitization does not reduce costs. Instead it has to be introduced in an organization with the capacity to ensure that the IT enhances rather than interferes with existing work patterns.

Taken together these two papers suggest that cost savings from digital technologies are more likely to come from increased data sharing rather than simple administrative efficiency.

2 Potential Policy Questions Arising from the Easy Transfer of and Access to Digital Medical Records

2.1 Policies that enhance incentives for data sharing

Given that there is evidence that the major benefits to the switch to digital technologies are realized when they are used to share data, rather than the simple conversion process from paper to digital, it is of obvious interest to policy makers to consider how to ensure that data is shared. Attempts to leverage 'big data' in healthcare beyond the individual patient, such as the 'learning health' system (Smith et al., 2013), will depend crucially on the willingness of providers to share their data (Goodby et al., 2010). However, it is unclear what the best steps are to take to ensure that information exchange happens.

One commonly advocated strategy for kick-starting a platform for data exchange is to secure a large 'marquee' user to help attract other users to the platform. As described by Eisenmann et al. (2006), "the participation of 'marquee users' can be especially important for attracting participants." Gowrisankaran and Stavins (2004) set out a foundational economic framework for understanding this. Due to marquee users' scale, they can internalize some of the network effects inherent in the platform and in turn then attract more users to the platform. To see this, consider a network technology that connects multiple separate firms. Each firm will adopt a network technology based on whether it receives net benefits from being part of the network, but it will not internalize the positive effect that its adoption has for other firms in the network. If a subset of these firms merge, then adoption increases, because the newly merged firm is able to internalize the network benefits from adoption at different locations.

Given this economic framework, it might be natural to assume that as a health policy maker the easiest way of ensuring that data is actually shared is by convincing large hospitals and hospital systems to get on board and start using healthcare IT and create patient data.

Furthermore, larger hospital systems may be better able to internalize the high costs of ensuring compatibility with complex information exchange standards, making it cheaper for them to exchange data both internally and externally. However, Miller and Tucker (2014a) challenges this intuition. We use data on the exchange of electronic health data within a local health area and investigate how the number of hospitals within a hospital's system influences its likelihood of sharing data.

We find that hospitals with more hospitals in their system are indeed more likely to exchange electronic information internally. However, they are less likely to exchange electronic information externally with other nearby hospitals. This decision to exchange information externally does not seem to be driven by the systems' age or manufacturer, nor by the number of other hospitals they could potentially interact with. We argue that this contrast between a willingness to share data internally and a lack of willingness to share data externally reflects a tendency for larger hospital systems to create 'information silos.' An information silo is a data system that does not exchange data with other similar systems.

A potential explanation for larger hospital systems' propensity to create information silos is that they fear that by facilitating data outflow, they may lose patients. If the hospital allows data outflow, patients may seek more follow-up care in stand-alone or community hospitals, which may offer more convenience or lower costs to patients whose insurance imposes substantial cost-sharing (Melnick and Keeler, 2007). We offer three pieces of evidence, based on estimating heterogeneous effects of system size on data exchange, that suggest that strategic motivations like these at least partially drive our results.

First, we find a stronger negative relationship between hospital system size and external information exchange among hospitals that have insurance arrangements that make it easier for patients to leave their hospital system. Second, hospitals that pay their staff more are less likely to share their data with hospitals outside their system if they are part of a larger system. Third, specialty hospitals are less likely to share data outside their system if they

are part of a larger system. The first result suggests that if patients are likely to seek treatment elsewhere, hospitals are less likely to share data. The latter two results suggest that if hospitals invest valuable resources in patient care, they may also be less likely to be willing to share data. While not conclusive, these findings provide some evidence that the creation of information silos that we observe is linked to strategic concerns.

The anticipated benefits from widespread health IT diffusion, in terms of cost savings and improved health outcomes, depend in large part on the electronic exchange of patient information. The results of this research suggest that adoption of EMR systems alone, even of systems with the capacity for data sharing, may not be sufficient to ensure that the full value from health IT is realized. This provides a potential rationale for public policy specifically aimed at promoting the electronic exchange of clinical information across firms and hospital system boundaries.

To help coordinate this sharing of data, under current federal policy EMRs only qualify for aid if they fulfill government criteria for 'meaningful use.'[3] Currently the 'Eligible Hospital and Critical Access Hospital Meaningful Use Core Measure 13' states that to qualify, a hospital has to have 'Performed at least one test of certified EHR technology's capacity to electronically exchange key clinical information.'[4] To qualify, hospitals can simply use information of a fictional patient (Wolf et al., 2012). This measure reflects the current policy focus on technological inter-operability as being the most important barrier to the exchange of healthcare information. However, the kind of seamless data sharing we have discussed in terms of the potential cost savings and health-benefits, is not aided by policies that can be fulfilled if a hospital mails a CD-ROM with the patient records stored in pdf format.

This was highlighted in recent testimony by Christine Bechtel to the Senate Committee

[3]For more historical and policy background on the 'meaningful use' criteria, see Blumenthal and Tavenner (2010), Jha et al. (2010) and Adler-Milstein et al. (2011).

[4]`http://www.cms.gov/EHRIncentivePrograms/Downloads/13_Electronic_Exchange_of_Clinical_Information.pdf`

on Health, Education, Labor and Pensions on June 10, 2015.[5] She highlighted that when she requested her medical data from her primary care provider in order to share it with other medical providers she was first told she only could receive a paper copy despite the office having a digital health records system installed. After highlighting that legally she was entitled to an electronic copy since they had a certified Electronic Health Records system which had been subsidized by the federal government, after more than a week they created a file on a CD-ROM that she had to physically pick up and was only readable with a specialized app.

Our work, together with anecdotes such as this and others included in the April 2015 ONC report on 'health information blocking',[6] suggest a need for those who aim to ensure the full benefits of digital health technologies are obtained, also focus on making sure that providers are both willing and able to be able to share electronic patient data as well.[7]

Our results suggest for those who seek to ensure that electronic information is actually shared that a focus on compatibility or capability alone will not be enough. To succeed in ensuring comprehensive meaningful use, the federal government will have to address the fact that larger hospital systems that may be producing the best health outputs may also be less willing to exchange information. This reluctance to share information may stem from the notion that records are the property of the hospital. As quoted in Knox (2009), Dr. Delbanco, a primary care specialist at Beth Israel Deaconess Medical Center in Boston, states, "You can get it [the patient record] [...] But we do everything in the world to make

[5] `http://www.hiewatch.com/news/3-ways-make-health-data-and-hie-public-good`

[6] `https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf`

[7] The emphasis on data sharing is shared by industry leaders and consumer advocates (Clark, 2009). Jim Lott, Executive Vice President, Hospital Council of Southern California: "Looking for savings in hospitals that use EMRs is short-sighted. The real payday for use of EMRs will come with interoperability. Measurable savings will be realized as middleware is installed that will allow for the electronic transmission and translation of patient records across different proprietary systems between delivery networks." Johnny Walker, Founder and past CEO of Patient Safety Institute: "EMRs don't save money in standalone situations. However, EMRs will absolutely save significant money (and improve care and safety) when connected and sharing clinical information."

sure you don't get it." The findings of this paper suggest that this ethos may be echoed in the switch from paper to digital records.

To summarize, our research highlights that attempts to provide incentives for IT adoption, may inadvertently also be giving hospitals incentives to adopt systems that are incompatible with their ultimate aim of widespread sharing of health information. And this is worrying because as we have discussed, it is in the sharing of health information that the benefits of IT lie.

2.2 Does digitization make it harder to secure data?

We now move from the policy question of how to ensure that data is shared to the question of how to ensure that the data is shared only with those for whom such sharing is desirable. This discussion draws on the field of the economics of information security, which highlights that as data is more easily shared in a digital format it is also more vulnerable to access by outsiders who may have malicious purposes such as identify theft.

In Miller and Tucker (2011b) we explore whether the digitization of health records is correlated with data breaches, that is the loss of data, and whether policies designed to minimize the risk of data breaches hurt or help. A panel data set from 2005-2008 allows insight into what firm characteristics, legal regulations and IT protocols are correlated with data breaches. We find evidence that, perhaps unsurprisingly, when a hospital adopts electronic health records this increases the likelihood of a breach. Specifically, installation of clinical and financial data warehousing software is associated with an increase in customer data loss. In line with the emphasis of Dranove et al. (2014) we also find a role for human capital. Having highly paid employees is associated with a reduction in the likelihood of data loss (especially where fraud is involved).

Surprisingly, we find empirical evidence that the use of encryption software does not reduce the instances of data loss. Instead, its installation is associated with an *increase* in

the likelihood of data loss associated with fraud and loss of computer equipment.

This matters because encryption is a policy often emphasized in the world of information security. Firms are often encouraged to adopt and use encryption software in order to help minimize the risks of losing customer data. Encryption is a way to encode computer files so that only someone with access to a secret 'key' can read them. Theoretically, encrypting data should deter malicious hackers, because it makes the data difficult to read. Encryption should also minimize the risks of data being used maliciously if the data falls into the wrong hands.

The fact that we find the opposite effect can be explained if hospitals are less careful at controlling access internally to encrypted data, and also because employees are less careful with computer equipment when they believe that data is encrypted. This research also highlights the extent to which human error, rather than malicious external hackers, is responsible for data loss: Ponemon (2009) finds that 88% of data breaches in 2008 could be traced back to insider negligence.

Our research also emphasizes that a commonly used policy tool for trying to promote data security may not be effective. In most instances we find little correlation between data loss and the enactment of data breach notification laws, which states have passed to force firms to notify customers about any data breaches.

Building on these findings, we estimate jointly the likelihood of a data loss and the adoption of encryption software. As a source of external variation that drives the adoption of encryption software but not the loss of data, we use whether or not the state's breach notification law makes an exception for encrypted data. Many states have enacted regulations that require firms to notify customers if their data is breached. However, many of these states give a blanket exception or 'safe harbor' if the breached data were encrypted. The underlying identification argument is that a state-wide encryption exception should give incremental incentives to hospitals in that state to adopt encryption software, compared to

hospitals in states that do not have any such encryption exception. This increased incentive is not related to those hospitals' underlying propensity to lose data. When we control for the endogeneity of the adoption of encryption software in this manner, adopting encryption software is still positively associated with a greater likelihood of data loss. We also show that there is no such relative boost for states that give safe harbor to encrypted data but whose laws explicitly exclude hospitals from their laws. This offers reassurance that there is not something unobserved about the kind of states that put in exceptions to their data breach notification laws which may also be associated with security technology adoption and data loss.

Of course it is possible to argue that if the adoption of encryption software is associated with an increase in data loss then this matters little if encryption makes the lost data useless. If only unreadable data are lost, it is not clear whether an increased likelihood of data loss poses a security risk to firms. However, there are three lingering concerns over the loss of encrypted data which mean that the data loss may still harm firms.

First, our finding that the adoption of encryption software is associated with an increase in instances of fraud emphasizes that encryption software is not effective at preventing insiders from accessing readable data. For example, the financial firm Countrywide emphasize their use of encryption and access controls in their website privacy and security policies. However, these encryption techniques were not enough to prevent a Countrywide employee from 2006-2008 from downloading records on up to 2 million customers/prospects to sell to mortgage brokers who wanted them for sales leads.[8]

Second, even unintentional loss of encrypted data may not be harmless. When data are encrypted, users generally access the data either via a separate key on a USB drive or password. Getgen (2009) shows how easily keys can be lost or compromised. Their

[8]'Security oversight may have enabled Countrywide breach' By Nancy Gohring, IDG News Service, 08-04-2008

study showed that 8% of organizations (including those who have not had a security breach) experienced problems with a lost encryption key over the previous two years.

Third, there are many instances where firms encrypt some data, but leave other data un-encrypted, and instances when employees decrypt data and download it to laptops or other unsecured portable devices.

The findings of the paper matter because government policies emphasize encryption as a solution to the data security problems engendered by this new world which emphasizes the sharing of data. Ponemon (2009) suggests that 44% of companies who experienced a prior breach have expanded their use of encryption technologies following a breach. Our results suggest a broader set of policies that encompass training and awareness programs, manual procedures and controls, and strong identity and access-management deployments.

In particular, we want to highlight that exceptions or a 'Safe Harbor' for encryption are at the heart of recent modifications to HIPAA. Safe Harbor is a provision to the Final Breach Notification Rule that eliminates the requirement for an organization to notify affected parties and the federal government in the event of an electronic personal health information data breach.[9] To qualify, such data must be in a format that is unusable, unreadable, or indecipherable to unauthorized individuals (Source: 74 FR 42740). In such cases, the healthcare organization is exempted from having to pursue costly breach notification. If ePHI (electronic protected health information) data is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information' The efficacy of such laws has been under question since Romanosky et al. (2011) found only weak effects from state-level data breach notification laws on the number of identity theft cases in that state. We emphasize that if federal or state laws give safe harbor to all encrypted data, this may lead firms to focus on encryption to the detriment

[9]See `https://hipaacentral.com/Documents/Perspectives/HIPAA-Encryption-Requirements-Perspective.aspx`

of firm efforts that are focused on controlling internal access to data and employee caution when managing personal data. In other words, by promoting a technological solution, and not human-based firm processes which complement encryption's effectiveness, giving a safe harbor to encrypted data may not have the intended effect.

2.3 Does privacy regulation help or hurt the sharing of patient data?

Given the data security risks, and the uneasiness many patients feel about unfettered access to their data by medical professionals, it is unsurprising that as well as regulations designed to enhance data security, governments have also introduced regulation designed specifically to protect patients' privacy.

The most prominent federal policy on health data privacy is HIPAA (the 1996 Health Insurance Portability and Accountability Act). The HIPAA Privacy Rule established national standards to protect medical records, whether paper or electronic. The Rule requires safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Rule was first introduced in 2000. It was updated as a result of the 2009 HITECH Act and the final text was released in 2013, in a form that is stricter with larger fines for data breaches and more restrictions on the use of personal data as well as expanding the coverage and number of firms and sectors that need to comply.

In addition to HIPAA there is also a patchwork of state privacy regulation. The existence of this patchwork of state privacy regulation allowed us to explore how state-level privacy regulation affects the health technologies that allow the creation and sharing of patient data.

In our early paper, Miller and Tucker (2009), we examined how the presence or absence of state privacy regulation affected the adoption of digital records systems or EMRs by

hospitals. As we have discussed EMRs theoretically offer benefits that are *automatic* for the hospital regardless of whether or what other hospitals adopt. These stand-alone benefits include shorter hospital stays prompted by better-coordinated care within the hospital, less nursing time spent on administrative tasks and better use of medications in hospitals.

However, EMRs also offers benefits that are *contingent* on other local hospitals also adopting a technology that allows patient data to be shared across hospitals. These allow hospitals to provide better care to patients who have chronic conditions and are seeing a new specialist, or are in emergency room situations where they cannot communicate medical history or allergies (Brailer, 2005). In certain circumstances the ability to access a patient's medical file quickly and electronically can also lower healthcare costs, for example, if it avoids the need for duplicate tests.

We explore whether the presence of privacy regulation can affect whether these contingent benefits induce adoption of digital technologies by hospitals. This is of course related to the notion of network effects in economics - with that lens this paper explores whether the presence of privacy regulation suppresses the network effects that might otherwise be inherent in a digital technology designed to share data.

Our state law panel begins in 1996, covering the great bulk of the relevant period of EMRs adoption. During that period, there were 19 changes in laws: 4 changes to increase privacy protection and 15 to decrease it. In our empirical analysis we first observe whether a hospital is located in a state with a privacy law covering hospitals.[10] Hospitals in these states have explicit statutory requirements to protect the confidentiality of patient medical information, and are restricted in their ability to disclose such information to outside parties without express prior authorization from the patient. Hospitals in other states are not explicitly covered by state laws governing the privacy of medical information. We study the average effects of such laws and do not calibrate the substantial variations in the strength

[10]Data on privacy laws from Pritts et al. (2002), Pritts et al. (1999) and Gostin et al. (1996).

and content of these laws across states.

In our empirical analysis, we use the adoption of EMRs at other neighboring hospitals in the local health service area (HSA) as a proxy for contingent benefits. The 815 Health Service Areas are ideal for our purpose as they were constructed as a self-contained area for patient flow (Makuc et al., 1991).[11]

Hospitals trade off these automatic and contingent benefits against potential costs that include the upfront costs of software and hardware installation, training, ongoing maintenance and physician resistance (Groopman, 2007). In our regression analysis, we control for hospital-specific characteristics, such as the number of fully-staffed beds, organizational structure and number of outpatients, to capture variation in the stand-alone benefits from EMRs using the relevant annual data from the AHA. We find evidence that indeed there is an interaction between potential network effects and the presence of privacy regulation. In states without hospital privacy legislation, EMR adoption by one hospital increases the probability of a neighboring hospital's adoption by 7% overall by the end of the sample period.

We also look at relative effects over time. In this data panel, we group the technology adoption data into three time periods, ending in 1999, 2002, and 2005, reflecting the years of the privacy law data. In our regressions, we exclude hospitals who have previously adopted EMRs from our observations, though we include this adoption as an explanatory variable.[12] In this specification, we find that in states without hospital privacy legislation, EMR adoption by one hospital increases the probability of a neighboring hospital's adoption by 2% every

[11] Our findings in this paper might seem at odds with the findings of Miller and Tucker (2014a) that hospitals in large systems often dislike sharing data with competitors. We emphasize that these empirical results which suggest that privacy regulation inhibits adoption through the mechanism of inhibiting network effects, did not distinguish between attempts to share data within hospital systems and attempts to share data outside of hospital systems, but instead just looks at a geographical area. And, often hospitals within the same system are co-located.

[12] Adoption decisions before 1996 are not studied in the panel framework, but are included as explanatory variables. Divestiture of an EMRs system is rare - only 2.4 percent of EMRs were replaced. We assume that hospitals only consider past adoption and do not use forecasts of future adoption in their decisions.

three years.

However, and importantly, in states with hospital privacy protection, there is no measurable effect from one hospital adopting EMR on another hospital.

We also try and control for the fact that the enactment of privacy regulation is likely endogenous by instrumenting for the presence of privacy regulation using plausibly exogenous changes in the closeness of the composition of the state house and senate and measure similarly large effects.

Furthermore, we also find evidence that state-level privacy protections functionally lead to hospitals to choose systems which are incompatible with easy data sharing. These results are unpublished but given the current policy emphasis on compatibility and the emphasis of this article on the importance of data sharing it seems worth discussing them here.

To establish this result we used the same data and approach as Miller and Tucker (2014a) to study how state privacy protection affects hospital choices over the inter-operability of the software they buy. We use cross-state and time-series variation in state privacy protection to quantify the *interaction* between the presence of state privacy protection and whether a hospital chooses to install an EMR system that is inter-operable with other hospitals in the local health service area.

When hospitals buy EMRs from different vendors, the systems may be incompatible if they use different data formats. Therefore, sharing information electronically becomes cumbersome and expensive if two hospitals' EMRs software is not easily inter-operable. We gathered information on inter-operability from the IHE project, which promotes the coordinated use of established standards such as DICOM and HL7 to record information about patient care. The IHE project was an early global initiative that was set up with the aim of promoting the passing of health information seamlessly across multiple healthcare enterprises. It does not establish new standards, but instead aims to promote the adoption of existing standards in order to promote inter-operability. As of 2006, there were seven

vendors who had made explicit "integration statements." These statements are documents prepared and published by vendors to describe the intended conformity of their products with the IHE Technical Framework. The documents then set out how each EMR system conforms to broadly used standards such as HL7, DICOM or WS3. The vendors that had made such statements are Cerner Corporation, GE Healthcare, IDX, McKesson Provider Technologies, Philips Medical Systems and Siemens Medical Solutions.[13] We categorized hospital technology purchases into inter-operable and less-interoperable systems by whether they had purchased software from one of these vendors who had made a public statement that laid out their commitment towards integration, or from another vendor that had made no such commitment.

We studied whether a hospital located in a HSA where many other hospitals have chosen easily inter-operable systems is more likely to also choose an easily inter-operable system if there is no strong state law relating to patient privacy protection. Our underlying hypothesis is that privacy protection diminishes the size of potential benefits from the transfer of patient information that are contingent on adoption by other hospitals. Therefore, privacy protection should diminish the relative importance of installing an EMR system that is easily inter-operable with other hospitals. Correspondingly, privacy protection may imply that hospitals will be less deterred from choosing a system that is not easily inter-operable even if other nearby hospitals have easily inter-operable systems. While common unobservable factors can provide an alternative explanation for correlated adoption by vendor type, they cannot explain differences in responsiveness to different kinds of adoption by neighboring hospitals in the HSA by the status of state privacy protection.

We found that hospitals in states with privacy laws are twice as likely to adopt less easily inter-operable systems. Hospitals in states with privacy laws are also less likely to adopt systems that are more inter-operable with the systems already adopted by nearby hospitals.

[13] As listed by http://www.ihe.net/resources/ihe_integration_statements.cfm in July 2006.

This suggests that state-level privacy protection is associated with US hospitals adopting EMRs that are less inter-operable with each other.

Therefore, there is quantitative evidence that the enactment of state privacy protection reduces the responsiveness of electronic medical records adoption to the size and inter-operability of the EMR systems chosen by neighboring hospitals in the local HSA. When states restrict medical providers' ability to disclose information, hospitals are less likely to choose systems that are inter-operable with other neighboring hospitals in the HSA. As such, privacy regulation may not only hinder technology adoption, but it may also hinder the adoption of technologies that are compatible with each other and allow data flows in the future. We emphasize that while using established standards is a necessary condition for the exchange of information, it is not a sufficient condition. Indeed, there are frequently incompatibilities even within different versions of the same system that use exactly the same standards, especially when issues of identification, security and versioning arise.

Though there are many good reasons for states to enact privacy protection, our results suggest that those protections may encourage hospitals to be less likely to adopt digital technologies, and if they do adopt to be more likely to adopt less-interoperable EMRs.

3 Potential Positive Consequences of Personalized Data and Medicine

So far this article has focused on the potential benefits and policy consequences of the sharing of data. We now turn to consider the potential benefits and also policy consequences of the deepening of data. We start this discussion by highlighting what we believe will be one of the most profound changes in the nature of data use and storage surrounding patient care which is the potential use of genomic data to enhance patient care. The use of genomic data is often highlighted as being at the forefront of personalized medicine.

Personalized medicine, where patients receive individually tailored health treatment based on their unique genetic makeup, promises to revolutionize healthcare. Clinical applications

of genetic information can improve public health and medical care productivity by targeting preventive care and interventions where they are most effective.[14] The desirability of personalized medicine stems both from the fact that personal genetic information may one day be used by individuals to anticipate their disease risks, select investment in preventive care, and when facing illness, to select the most effective treatment, but there are also potentially large system-wide gains from analyzing personal genetic data on a large scale.

Currently, the usefulness of genetic testing for general purposes is questioned due to difficulty in identifying solid statistical correlations and questions over the usefulness of such results for the average patient (Evans et al., 2001). However, genetic tests can be extremely valuable to individuals in certain sub-populations. Genetic variations have been identified that predict increased risks of breast cancer, ovarian cancer, colon cancer and cystic fibrosis, among other diseases. A negative result would imply a normal cancer risk, while a positive result would be elevated.

For example, the official guidance for someone who has tested positive for the BRCA or BRCA2 mutation which elevates the risk of breast or ovarian cancer is that they should be offered 'enhanced screening' to try and detect breast cancer at an early stage.[15] It also suggests they also should be offered prophylactic surgery which removes as much 'at-risk' tissue as possible; this may involve a double mastectomy and the removal of ovaries and fallopian tubes. There is also the possibility of 'chemoprevention,' which is the use of drugs such as tamoxifen and raloxifene to try and reduce the risk of cancer. Though medical evidence is at an early stage on the effectiveness of such actions, there is evidence that taking these aggressive measures can greatly reduce the incidence of cancer. For example, studies suggest that tamoxifen can cut breast cancer incidence among healthy BRCA2 carriers by

[14]The potential value of personalized medicine is reflected in President Obama's Precision Medicine Initiative, announced in his 2015 State of the Union Address, to which his 2016 budget allocates $215 million. See http://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.

[15]http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA

62% (King et al., 2001). A double mastectomy can reduce breast cancer incidence by 90% (Hartmann et al., 2001).

4 Potential Policy Consequences of Personalized Data and Medicine

4.1 Privacy concerns raised by personalized data and medicine

As with the sharing of data, with the increased deepening and personalization of data there are natural privacy concerns. Therefore, the spread of potentially revolutionary genetic tests that form the basis of customized medicine may be stymied by privacy concerns.[16]

However, we would argue that there are privacy concerns connected with genetic testing data that go beyond those potentially of 'regular' health data.

First, the creation of a genetic record is permanent in a world of persistent digital data. However, at this time in 2016, the consequences of such data in the future are uncertain as is the speed at which the ability to project out health outcome accurately from the human genome will develop. At the same time, as more links are uncovered between genes and personality traits and future health risks, individuals may suffer from discrimination or other harms from having parts of their genetic information revealed to others.[17] Second, there are potential spillovers of the creation of this data for family members. For example, if someone through a genetic test is found likely to be carrying a BRCA1 or BRCA2 mutation this changes the expected probability distribution for her relatives also having that mutation. Third, genetic data is almost unique in the extent to which it is immutable. It is a piece of data about a person that can't be changed. While in theory an individual can improve his or her credit record by more judicious use of credit cards, or potentially improve a health

[16]Indeed, for the case of cancer risks where genetic links are well-established, and for high-risk populations where genetic testing is therefore most valuable, rates of adoption remain low. Data from the 2010 National Health Interview Survey suggests that, even among individuals who have been advised by their physician to obtain a genetic test for cancer, over 30% do not comply.

[17]Komarova et al. (2013) emphasizes the ability of firms to combine multiple different types of public data to identify allegedly anonymous profiles.

record by quitting smoking, for example, it is impossible to improve or enhance or change data from a genetic test.

In Miller and Tucker (2014b) we study the effects of privacy regulations that are designed to protect genetic privacy on the diffusion of personalized medicine. Strong privacy protection may increase the value of genetic testing to consumers because it assures that they will not suffer harm in future market interactions. However, privacy protection may sensitize consumers to privacy concerns, increase costs to providers of genetic testing services and reduce the value to insurance companies of covering the service. This makes the empirical effect ambiguous. Further, since privacy protection is not a binary, all-or-nothing, choice, it is important to understand which features of privacy regulations are most beneficial from the view of consumers and which are most costly to producers. The study therefore explores the different provisions within privacy laws to identify policies that are most favorable to the spread of personalized medicine. We use variation in state laws over time in the United States to estimate the effect of different kinds of genetic privacy laws on the use of genetic testing for cancer risks.

State genetic privacy laws, at a high level of generality, take three alternate approaches to protecting patient privacy: First, requiring informed consent on the part of the individual; second, explicitly restricting the use of genetic data by health insurance, employers or providers of long-term life care or insurance; and third, limiting redisclosure without the consent of the individual or defining genetic data as the 'property' of the individual.

Using individual-level panel data, we find that an approach which gives users control over redisclosure encourages the spread of genetic testing, whereas an approach of informed consent deters individuals from obtaining genetic tests. We find no effects of anti-discrimination rules that limit the use of genetic information in particular contexts. We summarize these results graphically in Figure 1.

We also show that there are no similar effects of genetic privacy protection on non-genetic

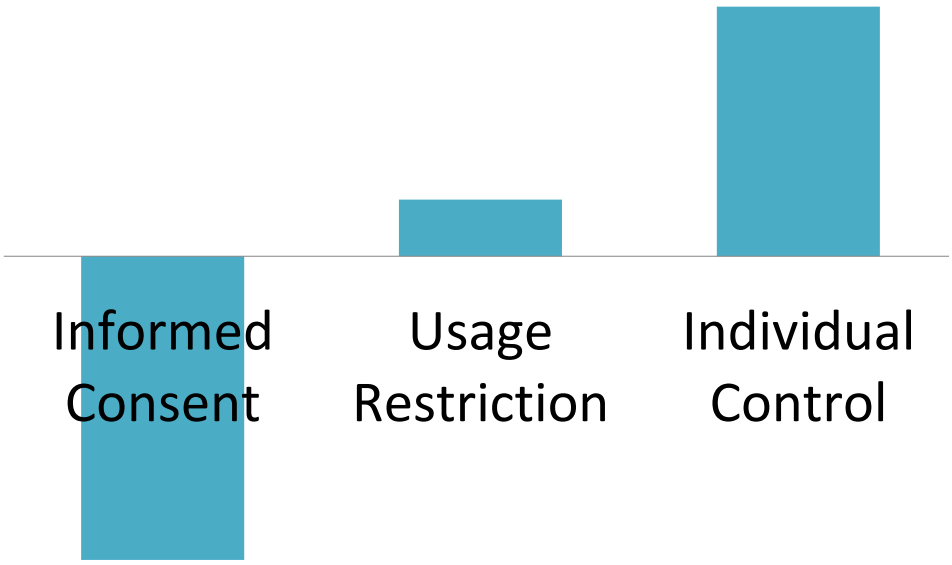

Figure 1: Summary of results of effects of different types of genetic privacy regulation on genetic testing

opt-in health testing (for HIV status) or use of preventive health care (getting a flu shot). We find larger effects for patients where the potential risks of genetic data being misused are highest, such as those who already know they have an elevated risk due to a family history of cancer (and individuals who show greater concern for their health privacy in other ways), but no effects for individuals who have already received a cancer diagnosis for one of the types predicted by genetic testing (breast, ovarian, colon or rectal). We show that the magnitude of the effect of the laws is driven by that individual's stated privacy concerns.

We then evaluate whether these results are driven by individual responses to privacy concerns, or by underlying changes in supply-side testing availability due to the laws. Genetic consent laws appear to reduce testing availability, suggesting that part of their negative effect stems from costs that complying with consent requirements impose on hospitals. However, there is no positive effect on genetic testing availability as a result of redisclosure laws, suggesting that particular kind of law derives its positive effect from its ability to provide consumer-side reassurance.

One unexpected part of this research was our finding that insurance type was not significantly related to the decision to have a genetic test. This is surprising given the emphasis in the economic literature on the effects of genetic testing on insurance markets ,such as Oster et al. (2010).[18]

In general our results are suggestive about the consequences of alternative approaches to regulating genetic privacy, given the perceived desirability of personalized medicine.

Public health and consumer advocates have argued for strong genetic privacy protections (Gostin, 1991). However, life insurance industry representatives have argued that all genetic information from applicants should be made available to them and that genetic insurance might be a viable solution (McEwen et al., 1993). By measuring the effects of genetic privacy

[18]Oster et al. (2013) discusses a possible psychological motivation for individuals with elevated risks for Huntington's disease to decline genetic testing, namely that a positive result limits their ability to maintain optimistic beliefs about their true risk.

on genetic testing rates and availability, this research provides the first empirical evidence on how public policy related to privacy affects the diffusion of genetic medicine. Generally, the empirical literature on privacy regulation has documented largely negative effects of privacy regulation for the spread and use of data-enriched technologies both in healthcare and elsewhere (Goldfarb and Tucker, 2011b, 2012). This research adds to this literature by not only studying a context where privacy concerns are paramount but also by emphasizing how different features of privacy regulation, in particular those that emphasize rights over data, can have different effects from more commonly found consent requirements, which previous studies have found to be associated with negative effects.

4.2 Is genetic data for personalized medicine different?

One other contribution of this work is to provide some of the first empirical evidence about 'genetic exceptionalism.' There has been substantial policy debate about whether genetic health data are distinct and different from regular health data and therefore needs a special class of protection (Yesley, 1998).[19] Genetic information can reveal more than a person's current health status; it contains information about their future health risks and traits that are unrelated to disease (Savitz and Ramesar, 2004). These concerns, specific to genetic (or genomic) information, can complicate the legal and ethical issues surrounding disclosure of personal information (Berry, 1997), and are the motivation for the new, targeted laws. Reflecting this, the new genetic privacy regulations that we study are explicitly incremental to existing state and federal laws protecting the privacy of personal health information.[20]

Our paper Miller and Tucker (2014b) provides the first empirical evidence on how individual behavior responds to regulations that protect the privacy of genetic information rather

[19] With respect to privacy, Washington is the only state that explicitly treats genetic information the same as other health information by including genetic information in the definition of health care information under the state health privacy law.

[20] Generally, the focus of these laws have been on data privacy rather than data security; see Miller and Tucker (2011b) for a description of the role of data-breach notification laws on the spread of information technology in healthcare.

than general health data. Our finding that genetic privacy laws have distinct effects above and beyond standard health data privacy laws provides some support for separate legislative action. To be clear, our paper does not argue that genetic data are different in function or from a medical perspective. Instead, it emphasizes that, from a patient's perspective, genetic information is regarded as something different that needs its own protections.

5 Beyond Healthcare

Much of this article has focused on the implications for the provision of healthcare of the shift towards digital data. However, in our concluding remarks, we want to emphasize that though we focus on how the sharing and deepening of individual patient data is an impetus for new policy emphasis in healthcare, the healthcare sector also provides a useful barometer for policy considerations in other data-driven parts of the economy.

There are two dimensions behind this observation. First, healthcare provides an unusually rich setting for empirical studies about the likely consequences of different types of policies for data-enhanced industries. Since healthcare is regulated at both the federal and state level this can provide useful variation in policy approaches for empirical researchers to study. Furthermore, the availability and comprehensive nature of data in the healthcare sector only enhances its appeal - we know of no other sector where there is an industry body such as the Healthcare Information and Management Systems Society (HIMSS) dedicated to collecting such detailed information about the current state of IT adoption by healthcare providers. Indeed in our own work, we have often documented the effects of policies surrounding data such as privacy protection in healthcare first, and then found that they are replicated in other sectors.[21]

Second, healthcare in also unusual in terms of how high the stakes are of getting policy right. Currently the US spends more than any other developed country on healthcare yet

[21] See Goldfarb and Tucker (2011a) for a discussion of the parallels of our work on privacy regulation in healthcare and in other sectors.

receives worse health outcomes (Bradley and Taylor, 2013). Furthermore, the potential consequences of policies towards ensuring that the upside of data sharing and deepening are felt and the risks are minimized are large in this sector. We would argue that the 'high stakes' of data in this sector, however, are the reason why policy in this area needs to quicker and more responsive than other sectors, even potentially providing leadership and guidance to other sectors about appropriate policy approaches.

References

Acemoglu, D. (2003). Technology and inequality. *Technology and Inequality*.

Adler-Milstein, J., D. W. Bates, and A. K. Jha (2011). A survey of health information exchange organizations in the united states: implications for meaningful use. *Annals of internal medicine 154*(10), 666–671.

Agha, L. (2014). The effects of health information technology on the costs and quality of medical care. *Journal of Health Economics 34*, 19 – 30.

Berry, R. M. (1997). The genetic revolution and the physician's duty of confidentiality. *Journal of Legal Medicine 18*(4), 401–441. PMID: 9433035.

Blumenthal, D. and M. Tavenner (2010). The 'meaningful use' regulation for electronic health records. *New England Journal of Medicine 363*(6), 501–504. PMID: 20647183.

Bradley, E. and L. Taylor (2013). *The American health care paradox: Why spending more is getting us less*. PublicAffairs.

Brailer, D. J. (2005). Interoperability: The Key To The Future Health Care System. *Health Affairs*, w5.19–21.

Clark, C. (2009, November). Four Health Leaders Weigh in on Whether EMRs Save Money . *Health Leaders Media*.

Dranove, D., C. Forman, A. Goldfarb, and S. Greenstein (2014). The trillion dollar conundrum: Complementarities and health information technology. *American Economic Journal: Economic Policy 6*(4), 239–70.

Eisenmann, T., G. Parker, and M. W. V. Alstyne (2006, October). Strategies for two-sided markets. *Harvard Business Review*.

Evans, J. P., C. Skrzynia, and W. Burke (2001). The complexities of predictive genetic testing. *British Medical Journal 322*(7293), 1052.

Freedman, S., H. Lin, and J. Prince (2014). Information technology and patient health: An expanded analysis of outcomes, populations, and mechanisms. *Available at SSRN 2445431*.

Getgen, K. (2009). 2009 encryption and key management benchmark survey. *Thales Group*.

Goldfarb, A. and C. Tucker (2011a, June). Privacy and innovation. Working Paper 17124, National Bureau of Economic Research.

Goldfarb, A. and C. Tucker (2011b). Privacy regulation and online advertising. *Management Science 57*(1), 57–71.

Goldfarb, A. and C. Tucker (2012). Privacy and innovation. *Innovation Policy and the Economy 12*(1), 65 – 90.

Goodby, A. W., L. Olsen, and M. McGinnis (2010). *Clinical Data as the Basic Staple of Health Learning:Creating and Protecting a Public Good: Workshop Summary*. IOM Roundtable on Evidence-Based Medicine (Series); Institute of Medicine. National Academies Press.

Gostin, L. (1991). Genetic discrimination: the use of genetically based diagnostic and prognostic tests by employers and insurers. *American Journal of Law & Medicine 17*, 109.

Gostin, L., Z. Lazzarini, and K. Flaherty (1996). Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization. Report to Centers for Disease Control and Prevention.

Gowrisankaran, G. and J. Stavins (2004). Network externalities and technology adoption: lessons from electronic payments. *RAND Journal of Economics 35*(2), 260–276.

Gresenz, C. R., S. P. Laughery, A. R. Miller, and C. E. Tucker (2016). Health it and ambulatory care quality. *Mimeo, University of Virgina*.

Groopman, J. (2007). *How Doctors Think*. Houghton Mifflin Company.

Hartmann, L. C., T. A. Sellers, D. J. Schaid, T. S. Frank, C. L. Soderberg, D. L. Sitta, M. H. Frost, C. S. Grant, J. H. Donohue, J. E. Woods, S. K. McDonnell, C. W. Vockley, A. Deffenbaugh, F. J. Couch, and R. B. Jenkins (2001). Efficacy of bilateral prophylactic mastectomy in brca1 and brca2 gene mutation carriers. *Journal of the National Cancer Institute 93*(21), 1633–1637.

Hillestad, R., J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville, and R. Taylor (2005, Sep-Oct). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs 24*(5), 1103–17.

Iyasu, S., A. K. Saftlas, D. L. Rowley, L. M. Koonin, H. W. Lawson, and H. K. Atrash (1993). The epidemiology of placenta previa in the united states, 1979 through 1987. *American journal of obstetrics and gynecology 168*(5), 1424–1429.

Jha, A. K., C. M. DesRoches, P. D. Kralovec, and M. S. Joshi (2010). A progress report on electronic health records in us hospitals. *Health Affairs 29*(10), 1951–1957.

Jha, A. K., T. G. Ferris, K. Donelan, C. DesRoches, A. Shields, S. Rosenbaum, and D. Blumenthal (2006). How common are electronic health records in the united states? a summary of the evidence. *Health Affairs 25*(6), w496–w507.

King, M.-C., S. Wieand, K. Hale, M. Lee, T. Walsh, K. Owens, J. Tait, L. Ford, B. K. Dunn, J. Costantino, et al. (2001). Tamoxifen and breast cancer incidence among women with inherited mutations in brca1 and brca2: National surgical adjuvant breast and bowel project (nsabp-p1) breast cancer prevention trial. *Jama 286*(18), 2251–2256.

Knox, R. (2009, Sep 21). Doctors don't agree on letting patients see notes. *NPR*.

Komarova, T., D. Nekipelov, and E. Yakovlev (2013). Estimation of treatment effects from combined data: Identification versus data security. In *Economics of Digitization*. University of Chicago Press.

Lammers, E. J., J. Adler-Milstein, and K. E. Kocher (2014). Does health information exchange reduce redundant imaging? evidence from emergency departments. *Medical care 52*(3), 227–234.

Lin, Y.-K., M. Lin, and H. Chen (2014). Beyond adoption: Does meaningful use of ehr improve quality of care? *Available at SSRN 2444054*.

Makuc, D., B. Haglund, D. Ingram, J. Kleinman, and J. Feldman (1991). Health Service Areas for the United States. DHHS Publication No. (PHS) 92-1386.

McCullough, J. S., S. Parente, and R. Town (2013, January). Health information technology and patient outcomes: The role of organizational and informational complementarities. Working Paper 18684, National Bureau of Economic Research.

McEwen, J. E., K. McCarty, and P. R. Reilly (1993). A survey of medical directors of life insurance companies concerning use of genetic information. *American Journal of Human Genetics 53*(1), 33.

Melnick, G. and E. Keeler (2007). The effects of multi-hospital systems on hospital prices. *Journal of Health Economics 26*(2), 400 – 413.

Miller, A. R. and C. Tucker (2009). Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. *Management Science 55*(7), 1077–1093.

Miller, A. R. and C. Tucker (2014a). Health information exchange, system size and information silos. *Journal of Health Economics 33*, 28 – 42.

Miller, A. R. and C. Tucker (2014b). Privacy protection, personalized medicine and genetic testing. *Personalized Medicine and Genetic Testing (July 31, 2014)*.

Miller, A. R. and C. E. Tucker (2011a, April). Can health care information technology save babies? *Journal of Political Economy 119*(2), 289–324.

Miller, A. R. and C. E. Tucker (2011b). Encryption and the loss of patient data. *Journal of Policy Analysis and Management 30*(3), 534–556.

Oster, E., I. Shoulson, and E. Dorsey (2013). Optimal expectations and limited medical testing: Evidence from Huntington disease. *American Economic Review 103*(2), 804–830.

Oster, E., I. Shoulson, K. Quaid, and E. R. Dorsey (2010). Genetic adverse selection: Evidence from long-term care insurance and Huntington disease. *Journal of Public Economics 94*(11-12), 1041 – 1050.

Ponemon, L. (2009). Fourth annual us cost of data breach study. *Poneomon Institute sponsored by PGP Corporation. Retrieved January 31*(2010), 2008–2009.

Pritts, J., A. Choy, L. Emmart, and J. Hustead (2002). The State of Health Privacy: A Survey of State Health Privacy Statutes. Second Edition.

Pritts, J., J. Goldman, Z. Hudson, A. Berenson, and E. Hadley (1999). The State of Health Privacy: An Uneven Terrain. A Comprehensive Survey of State Health Privacy Statutes. First Edition.

Romanosky, S., R. Telang, and A. Acquisti (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management 30*(2), 256–286.

Savitz, J. B. and R. S. Ramesar (2004). Genetic variants implicated in personality: a review of the more promising candidates. *American Journal of Medical Genetics Part B: Neuropsychiatric Genetics 131*(1), 20–32.

Schulman, K. A., J. A. Berlin, W. Harless, J. F. Kerner, S. Sistrunk, B. J. Gersh, R. Dube, C. K. Taleghani, J. E. Burke, S. Williams, et al. (1999). The effect of race and sex on physicians' recommendations for cardiac catheterization. *New England Journal of Medicine 340*(8), 618–626.

Smith, M., R. Saunders, L. Stuckhardt, J. M. McGinnis, et al. (2013). *Best Care at Lower Cost:: The Path to Continuously Learning Health Care in America*. National Academies Press.

Spetz, J., J. F. Burgess, and C. S. Phibbs (2014). The effect of health information technology implementation in Veterans Health Administration hospitals on patient outcomes. *Healthcare 2*(1), 40–47.

Wolf, L., J. Harvell, and A. K. Jha (2012). Hospitals ineligible for federal meaningful-use incentives have dismally low rates of adoption of electronic health records. *Health Affairs 31*(3), 505–513.

Yesley, M. S. (1998). Protecting genetic difference. *Berkeley Technology Law Journal 13*, 653.