View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Digital Commons @ UM Law

SETON HALL | LAW
Center for Health &
Pharmaceutical Law & Policy

The Future of HIPAA in the Cloud

A white paper by Frank Pasquale and Tara Adams Ragone
June 30, 2013

The Future of HIPAA in the Cloud

Abstract

This white paper examines how cloud computing generates new privacy challenges for both healthcare providers and patients, and how American health privacy laws may be interpreted or amended to address these challenges. Given the current implementation of Meaningful Use rules for health information technology and the Omnibus HIPAA Rule in health care generally, the stage is now set for a distinctive law of "health information" to emerge. HIPAA has come of age of late, with more aggressive enforcement efforts targeting wayward healthcare providers and entities. Nevertheless, more needs to be done to assure that health privacy and all the values it is meant to protect are actually vindicated in an era of ever faster and more pervasive data transfer and analysis.

After describing how cloud computing is now used in healthcare, this white paper examines nascent and emerging cloud applications. Current regulation addresses many of these scenarios, but also leaves some important decision points ahead. Business associate agreements between cloud service providers and covered entities will need to address new risks. To meaningfully consent to new uses of protected health information, patients will need access to more sophisticated and granular methods of monitoring data collection, analysis, and use. Policymakers should be concerned not only about medical records, but also about medical reputations used to deny opportunities. In order to implement these and other recommendations, more funding for technical assistance for health privacy regulators is essential.

TABLE OF CONTENTS

The Future of HIPAA in the Cloud

Frank Pasquale & Tara Adams Ragone[1]

I. Introduction

Corporations are increasingly turning to cloud computing solutions for storage, communication, and analytical needs. The logic of specialization is irresistible for many. Outsource information technology (IT) to a third party, and let it worry about security, deduplication, archiving, backup, and other critical issues.

The cloud has its dangers, to be sure—outages may be rarer, but more devastating when they do occur, given the centralization of storage and related services. This centralization of data also makes cloud providers a target for hackers. But the logic of efficiency and specialization is compelling.[2] Just as Amazon effectively consolidated the business of thousands of individual book retailers into a single platform, some futurists envision a mass migration of business records to a small number of cloud service providers.

Whatever their merits in other areas of business, cloud models have come under scrutiny when used in the healthcare arena. Patients are rightly concerned about critical health data being lost or inappropriately accessed.[3] On the one hand, cloud service providers may reduce those risks by deploying their unique expertise. On the other hand, the more entities access data, the more chances there are for *something* to go wrong. Risks along many dimensions—legal, reputational, medical, among others—need to be addressed.

This white paper examines one particular dimension of that risk: dangers to health privacy interests caused by inappropriate data access, storage, transmission, or analysis. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) provide a general framework of federal law to help deter and reduce the likelihood that such issues will occur; state laws often

---

[1] Pasquale is Schering-Plough Professor in Health Care Regulation and Enforcement at Seton Hall Law School. Ragone is Research Fellow and Lecturer in Law at Seton Hall Law School and its Center for Health & Pharmaceutical Law & Policy. We would like to thank the Center for Health & Pharmaceutical Law & Policy and Microsoft Corporation for sponsoring this research. We also wish to thank Melissa Goldstein, Melissa Markey, Bill Pewen, and Nicolas Terry for commenting on the white paper.

[2] *See, e.g.*, Michael Hugos & Derek Hulitzky, BUSINESS IN THE CLOUD: WHAT EVERY BUSINESS NEEDS TO KNOW ABOUT CLOUD COMPUTING (2010) (describing the factors "driving business to the cloud and away from corporate data centers," including that "cloud computing enables clearer focus on the business," "cloud computing reduces dependence on internal infrastructure and the capital expense that goes with that infrastructure," "cloud computing automatically scales up and down with business volume, and this variable cost operating model reduces financial risks," "in-house systems can be migrated to the cloud with relative ease if the process is well designed," and "cloud computing . . . allow[s] customers to buy only what they consume").

[3] Gina Stevens, CONG. RESEARCH. SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2010); Lucas Mearian, *'Wall of Shame' Exposes 21M Medical Record Breaches*, COMPUTERWORLD (Aug. 7, 2012), http://www.computerworld.com/s/article/9230028.

reinforce those patient protections.[4] After years of being dismissed as a toothless tiger, HIPAA has come of age of late, with more aggressive enforcement efforts targeting wayward healthcare providers, payers, and other covered entities.[5] Nevertheless, more needs to be done to assure that health privacy and all the values it is meant to protect are actually vindicated in an era of cloud computing, given the ever faster and more pervasive data transfer and analysis that technological change is now bringing to the healthcare sector.

This white paper surveys some important areas in health privacy regulation and data protection standards. After describing how cloud computing is now used in healthcare, it examines nascent and emerging cloud applications (Part II). Current regulation addresses many of these scenarios but also leaves some important decision points ahead (Part III). The white paper offers some recommendations for future policy, reflecting the concerns of diverse U.S. stakeholders and lessons from both state law and international policy (Part IV). It concludes with some reflections on the clash of cultures between the healthcare sector and the Silicon Valley giants now dominating the cloud (Part V).

II. The Role of Cloud Computing in Healthcare

A. How Cloud Computing Is Now Used in Healthcare

Virtually every healthcare provider, health plan and healthcare clearinghouse has used information technology, if only for revenue cycle management. The diffusion of electronic health records (EHRs) has now reached a critical mass, assuring that more healthcare entities are dealing with digitized records of protected health information (PHI). Meaningful use regulations soon will also move from "carrot" to "stick," taking a bite out of Medicare reimbursements for eligible healthcare providers who fail to get on the digitization bandwagon.

Traditionally, healthcare providers have invested in desktop computers, servers, routers, and storage devices *on site.*[6] They have also licensed software, which is installed onsite. The

[4] The Health Information Technology for Economic and Clinical Health Act (HITECH) is Title VIII of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009) (codified in various sections of 42 U.S.C.). The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA). The Privacy Rule protects the privacy of individually identifiable health information, while the Security Rule sets national standards for the security of electronic protected health information. HIPAA applies to covered entities and business associates, as defined in 45 C.F.R. § 160.103.

[5] *See, e.g.*, Mary Anne Pazanowski, *HHS Breaks New Ground with $43 Million Penalty for HIPAA Privacy Rule Violation*, 20 HEALTH LAW REPORTER 277 (BNA) (Feb. 24, 2011).

[6] Third party EHR vendors come in many varieties. Attorney Michael J. Daray describes two general competing models of EHR vendors. *See* Michael Daray, *Negotiating Electronic Health Record Technology Agreements*, 22 No. 2 Health Law 53 (2009). The "traditional model" involves a healthcare provider acquiring a license in EHR software from a third party vendor. The software is then installed on the physician's computer hardware or network, and patient data is then stored on the physician's premises. The advantage to this model is that the physician retains control over the data, but cost can be a downside. *Id.* at 54.

healthcare provider, as a buyer of hardware and software licensee, has had the responsibility to coordinate these systems and to optimize their utilization and management. An on-site IT infrastructure can be costly and hard to manage, especially in comparison to specialized cloud service providers. Healthcare professionals have enough difficulty keeping up with the newest medical research and applying it to their care settings; understanding the latest trends in IT (even if deciphered and presented by a dedicated IT staff) may prove to be a task few are well-qualified for. Further, the increasing emphasis on health IT has created a significant dearth of well-qualified health IT staff, placing such staff largely outside the grasp of smaller healthcare providers such as physician offices. Many healthcare providers, particularly physicians, clinics, and stand-alone hospitals, do not want the responsibility of owning and managing hardware and software for electronic health records, practice management, and revenue cycle management.

Early steps toward the modern cloud computing paradigm offered another alternative. The use of browser-based applications and data centers became of particular interest to healthcare providers. As internet connectivity became more pervasive and reliable for many commercial entities, the ability to run applications remotely became a reality. The availability of software through hosted solutions, such as "Software as a Service" ("SaaS"), allows the investment in hardware and hosting services to be made by the vendor, while the healthcare provider's investment is limited to subscription payments. The users do not own hardware or software, other than the machines used locally to access the SaaS vendor.[7] Rather, they are often

[7] Generally, a cloud service provider manages information on behalf of (or regarding) another entity. There are several different service models for storing information in the cloud. First, the EHR vendor may use the SaaS model discussed above to allow customers to access the software on a cloud infrastructure, with the cloud provider responsible for the software. *See* H. Ward Classen, *Cloudy with A Chance of Rain: Avoiding Pitfalls in Cloud Computing*, 45 MD. B.J. 18, 20 (2012). Second, the Infrastructure as a Service (IaaS) model allows customers to access data held on the cloud through the internet with their own software. *Id.* Third, the Business Process as a Service (BPaaS) model allows customers to access an entire business on the cloud, such as billing. *Id.* In the fourth model, Platform as a Service (PaaS), "the cloud vendor provides all of the services provided in IAAS, but also provides the operating system and storage and network capacity management. . . . Essentially, the customer has outsourced to the cloud vendor full data center operations, while retaining applications-level responsibilities, including maintenance of databases, patch administration, and similar activities." Melissa Markey, Esq. & Margaret Marchak, Esq., "Chapter 15: Security Considerations in Technology Contracting," at 19 (draft chapter on file with authors). Melissa Markey reports that Security as a Service (SecaaS) is another model that has been gaining popularity. *See* Notes from Melissa Markey, Esq. (on file with authors). SecaaS, which is a segment of the SaaS market, permits customers to outsource security management over the internet, including services such as anti-virus and anti-malware. *See* "Introduction to Security as a Service," Cloud Security Alliance, https://cloudsecurityalliance.org/research/secaas/ (last visited May 20, 2013); "Definition: Security as a Service (SaaS)," SearchSecurity, http://searchsecurity.techtarget.com/definition/Security-as-a-Service (last visited May 20, 2013). As Markey and Marchak point out, the different models involve varying levels of control over software and hardware, which affects what contract terms may be appropriate to address responsibility for data security:

> [T]he relative degree of control over the environment, both hardware and software, vary significantly depending on the service model procured by the customer. In IAAS, the cloud vendor has control of the physical environment and hardware, and thus should be contractually obligated to implement reasonable security controls over related risk areas. Because the customer has

paying for access to the SaaS programs and/or for new computational capabilities, and all the accompanying data processing and assistance that implies.[8] Use of SaaS solutions permitted healthcare providers to invest in more technology, as the need for capital investment in hardware decreased, thus developing richer data sets. As this model matures, moving beyond native applications to more collaborative platforms can lead to co-creation of value (as in, say, concurrent or shared access by both primary care and specialist physicians to a record set).

The National Institute of Standards and Technology (NIST) has defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[9] If cloud computing were merely a form of IT outsourcing, it might not be worthy of much legal note. The contractual arrangements and laws of agency surrounding such outsourcing processes are well-established. Rather, cloud computing services involve new innovations in both technology and business models that create new opportunities—and perils—for healthcare providers and contractors alike.[10]

Moreover, there are unique issues in the healthcare industry that can make the implementation of cloud computing more of a challenge.[11] As A.K. Soman observes,

> The Healthcare industry is however different from most other industry verticals. Healthcare data is highly sensitive—any breach of privacy and security in the context of healthcare data can have serious consequences. Secondly, there are multiple entities that have to deal with healthcare data. This includes care providers,

---

> control over the operating system and applications, the customer must accept greater responsibility for security with respect to those elements. The opposite is true, however, for SAAS implementations, wherein the cloud provider should be contractually obligated to implement reasonable security controls for the entire environment.

Markey & Marchak, *supra* note 7, at 20.

[8] In SaaS, the physician subscribes to the software that is remotely hosted on a server, and uploads patient data that is stored on that server. Given the use of technology here, "concerns aris[e] if the vendor ceases business operations." Bulletin, American College of Surgeons, at http://www.facs.org/fellows_info/bulletin/negotiatingehr.html. For this reason, the contract with the cloud provider must address data back up and provide a clear right to data if the contract expires or terminates. *See* Markey & Marchak, *supra* note 7, at 34; Notes from Melissa Markey, Esq. (on file with authors). Data ownership and limited rights of use clauses may also help clarify expectations in such scenarios.

[9] National Institute of Standards and Technology, *Cloud Computing*, at http://csrc.nist.gov/groups/SNS/cloud-computing/.

[10] Delivery models for the cloud infrastructure itself come in four varieties: public, private, hybrid, or community. *See* Classen, *supra* note 7, at 20-21.

[11] Chris Preimesberger, *Storing Health Records in the Cloud: Ten Reasons Why It's a Bad Idea*, http://www.eweek.com/c/a/Data-Storage/Storing-Health-Records-in-the-Cloud-10-Reasons-Why-Its-a-Bad-Idea-290388/ (Aug. 17, 2010) (but note that the key source for the story is the founder of a client/server-based health-care record software maker).

> hospital administration staff, payers, labs, [and] patients themselves. There are extensive regulations governing the healthcare industry and many of these regulations impact the nature of the information technology solutions adopted by the industry. The fact that cloud based solutions are being reliably used in other industry segments does not automatically imply that they can be used in the healthcare industry.[12]

Nevertheless, cloud-based practice management software has taken on such sensitive issues as patient account management, managing patients, HIPAA compliance, patient portals,[13] and appointment scheduling.[14] Cloud-based ePrescription systems may also help providers meet HIPAA's meaningful use requirements.[15] Whether the preceding functionalities (of practice management, revenue cycle management, or EHRs) are cloud-based or not, a healthcare provider might choose to back up its system in the cloud using a web storage service—or its contractors may choose to do so.

Cloud services suffer from certain vulnerabilities. For example, cloud services are at the mercy of internet access. Prolonged internet outages, such as recently experienced during Hurricane Sandy, create real risks that healthcare providers will not be able to access critical information when it is most needed.[16] Privacy is also a renewed concern, as breaches of massive databases, even if they are less likely to occur than scattered breaches, are far more menacing to privacy and security.[17]

---

[12] A.K. Soman, CLOUD-BASED SOLUTIONS FOR HEALTHCARE IT, 84 (2011).

[13] Such portals can include functionality to "1) Schedule new appointments or modify previously scheduled appointments with the care provider; 2) Register or complete any forms (including medical history) online …; 3) Send messages to physicians or ask questions, 4) Request prescription medication refills; 5) Review billing information and make payments online; 6) Review further educational information pertaining to their condition." *Id.* at 94.

[14] *Id.* at 92.

[15] *Id.* at 95 ("An ePrescription system is a computerized system in which the prescription is either entered by the physician/nurse practitioner or generated on the basis of data available to the system. The prescription can be automatically communicated to pharmacies associated with the healthcare provider.").

[16] Compare discussion in Foley & Lardner LLP, *Cloud Computing for Health Care Organizations* (2012). Foley & Lardner recommend explicitly mapping out the "mission criticality" of aspects of a cloud service before committing to it. *Id.* at 5. On the other hand, "Datacenters are typically located in places where the risk of natural disasters (such as earthquakes, floods, hurricanes, etc) and man-made disasters (such as riots, explosions, etc.) is minimal. They are located in places with abundant availability of resources such as water and electricity." SOMAN, *supra* note 12, at 75.

[17] Designers of cloud computing services are taking this risk into account. *See, e.g.*, Siani Pearson, Taking Account of Privacy when Designing Cloud Computing Services § 3.1 (Hewlett Packard Labs., HPL-2009-54, 2009), http://www.hpl.hp.com/techreports/2009/HPL-2009-54.pdf; Microsoft Private Cloud Computing; Miranda Mowbray & Siani Pearson, *A Client-Based Privacy Manager for Cloud Computing*, 4 Proc. Int'l ICST Conf. on Comm. Sys. Software & Middleware 5, § 1 (2009). Some experts note the appeal of "private cloud" computing, given these concerns. SOMAN, *supra* note 12, at 77 ("The Private Cloud entails incurring the cost disadvantages associated with in-house IT, since you have to put up the entire infrastructure for the use of your organization alone. On the other hand the benefit of the Private Cloud is the security it offers. The Private Cloud is subject to the policies of the

Cloud systems thus offer a significant number of tradeoffs. In exchange for control and ownership, users are offered expertise. Yet it is important not to overstate the change here. In many ways the users never really "owned" the software they operated—it was licensed. The EHR literature abounds with worries and complaints from providers that they were "locked into" a certain software system. If they contractually promote platform-independence and data portability, some cloud services may help alleviate such concerns. But they also raise a whole new set of issues.

B. Nascent and Future Applications of Cloud Computing

Both cutting edge providers and informed patients are likely to demand more cloud computing services (or at least connectivity and interoperability with them) in the future, especially as self-tracking devices proliferate.[18] As the possibilities of big data analysis inform the development of health information technology, the computational prowess of centralized and remote IT providers becomes particularly important.[19] Several nascent and emerging applications of computation in healthcare suggest the intensification of this trend.[20]

Over a decade ago, David Eddy was using a computer model, Archimedes, to model human drug trials.[21] The American Diabetes Association asked him to project how well a given drug was likely to work, based on extant information in his databases and models based on past experiences with similar compounds. Now, similar technology can be repurposed to identify

---

organization, just as its operation is under the organization's control. Therefore, data really never 'leaves' your premises. This addresses the key concern pertaining to (public) Cloud services, namely, control over the data.").

[18] Emily Singer, *The Measured Life*, MIT TECH. REV., July/Aug. 2011, *available at* http://www.technologyreview.com/featured-story/424390/the-measured-life/ ("The new generation of devices rely on inexpensive, low-power wireless transceivers that can automatically send data to the wearer's cell phone or computer. Compared with the limited snapshot of health that is captured during an annual visit to the doctor's office, these tools and techniques could reveal the measures of someone's health in context, and with a much richer resolution.").

[19] Viktor Mayer-Schonberger & Kenneth Cukier, BIG DATA: A REVOLUTION THAT WILL CHANGE THE WAY WE LIVE, WORK, AND THINK (2013) (discussing three key characteristics of the new opportunities in data: "more" data is available, and while it's "messier" than prior data sets, that doesn't matter in an era when "correlations rather than causation" are the key desiderata of analysts); *see also* Chris Anderson, *The End of Theory*, WIRED (2008), *available at* http://www.wired.com/science/discoveries/magazine/16-07/pb_theory ("This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves.").

[20] Of course, one should be wary of overestimating the impact of these trends. *See, e.g.*, Nicolas P. Terry, *Information Technology's Failure to Disrupt Health Care*, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2118653 (examining "four possible explanations for the difficulties faced by HIT in disrupting health care").

[21] Jennifer Kahn, *Modeling Human Drug Trials--Without the Humans*, WIRED, Dec. 2009, at 156, 157, 194, *available at* http://www.wired.com/magazine/2009/11/ff_archimedes/all/ ("In early 2004 . . . the American Diabetes Association asked a physician and mathematician named David Eddy to run his own . . . trial [on atorvastatin]. He would do it, though, without human test subjects, instead using a computer model he had designed called Archimedes.").

optimal treatment approaches to particular cases. For example, there is growing excitement about the use of advanced computing systems in clinical decision support. The partnership between IBM and Memorial Sloan-Kettering Hospital is one of the most noted of these developments.[22] By integrating medical records, treatment guides, public research, and private insight, "Watson-like" technology may be able to assist physicians in assessing treatment options. Given the appeal of new technologies to patients, and the increasing difficulty for physicians to maintain currency in new developments and consider all of the possible diagnoses for each patient, we are likely to see widespread demand for this type of clinical decision support in many treatment areas.

It will also be tempting for the giants behind public and hybrid cloud computing platforms to begin to study the correlations emerging in massive data stores. Geoffrey Miller recently commented on the extraordinary divergence in the research capacities of academics (who are often hamstrung by IRB requirements) and large internet companies (which face no similar hurdles).[23] Researchers have already demonstrated that big data-enabled pharmacovigilance might reveal problems sooner than ordinary adverse event reporting systems.[24]

Sharona Hoffman and Andy Podgurski's article, *Improving Health Care Outcomes through Personalized Comparisons of Treatment Effectiveness Based on Electronic Health Records*, gives a taste of future applications that patients may demand to optimize their healthcare. They have detailed how personalized programs of research on effectiveness could work:

> We propose the development of a broadly accessible framework to enable physicians to rapidly perform, through a computerized service, medically sound personalized comparisons of the effectiveness of possible treatments for patients' conditions. A personalized comparison of treatment effectiveness . . . for a given patient (the subject patient) would be based on data from EHRs of a cohort of patients who are similar to the subject patient

[22] Jonah Comstock, *IBM's Watson Interns at Memorial Sloan Kettering*, MOBIHEALTHNEWS, *available at* http://mobihealthnews.com/20255/ibms-watson-interns-at-memorial-sloan-kettering/ ("shows how Watson might help an oncologist diagnose and treat a cancer patient").

[23] Geoffrey Miller, *N=Billions: The Smartphone Revolution in the Behavioral Sciences*, Berkman Center (Mar. 12, 2013), *available at* http://cyber.law.harvard.edu/events/luncheon/2013/03/miller ("Smartphones will empower behavioral scientists to collect terabytes of ecologically valid data from vast global samples – easily, quickly, and remotely. Smartphones can record where people are, what they are doing, and what they can see and hear. They can run interactive surveys, tests, and experiments through touch screens and Bluetooth peripherals.").

[24] Ryen White, *et al.*, *Web-scale Pharmacovigilance: Listening to Signals from the Crowd*, JAMIA (Jan. 13, 2013), *available at* http://jamia.bmj.com/content/early/2013/02/05/amiajnl-2012-001482.abstract ("The results demonstrate that logs of the search activities of populations of computer users can contribute to drug safety surveillance.").

> (clinically, demographically, genetically), who received the treatments previously and whose outcomes were recorded.[25]

As they explain, such a database query could identify, "for a given patient, an appropriate reference group (cohort) of similar, previously treated patients whose EHRs would be analyzed to choose the optimal treatment for the patient at issue."[26] Research has already demonstrated that pharmacogenetic algorithms can outperform algorithms that consider only clinical factors.[27]

The President's Committee Advising on Science & Technology (PCAST) has also endorsed aggressive use of health data to ensure new research opportunities.[28] The PCAST authors conclude that many clinical research studies today are "out of date before they are even finished," "burdensome and costly," and too narrowly focused.[29] They endorse health information technology that is enabled for "syndromic surveillance," "public health monitoring," and "adverse event monitoring" by aggregating observational data.[30]

Efthimios Parasidis also describes how the development of health information technology infrastructures in the United States can enable forms of surveillance that are more rigorous, comprehensive, and actionable in the world of policy and more user-friendly for patients.[31] As he observes, "EHR systems now permit advanced data-entry options such as 'free text [entry], templated data entry, dictation, speech recognition, and freehand graphic input.'"[32] Rather than getting between doctor and patient, advanced EHR stands poised to silently monitor and improve their relationship.[33] The same record systems that are designed to digitize health diagnoses and interventions can also generate outcome data if they are configured appropriately. Such data would help ensure patients and authorities are truly informed about the risks and benefits of drugs.[34] A complete record of "demographics, progress notes, vital signs, medical history, immunization history, and laboratory and radiological reports" can contribute greatly to

---

[25] Sharona Hoffman & Andy Podgurski, *Improving Health Care Outcomes through Personalized Comparisons of Treatment Effectiveness Based on Electronic Health Records*, 39 J.L. MED. & ETHICS 425, 425 (2011).
[26] *Id.* at 426; *see also* INST. OF MED., CHALLENGES FOR THE FDA: THE FUTURE OF DRUG SAFETY 52 (2007), *available at* http://books.nap.edu/openbook.php?record_id=11969) (calling for more targeted comparative effectiveness research).
[27] J. Woodcock and L. J. Lesko, *Pharmacogenetics--Tailoring Treatment for the Outliers*, 360 NEW ENG. J. MED. 811, 811 (2009).
[28] President's Council of Advisors on Sci. & Tech., REPORT TO THE PRESIDENT REALIZING THE FULL POTENTIAL OF HEALTH INFORMATION TECHNOLOGY TO IMPROVE HEALTH CARE FOR AMERICANS: THE PATH FORWARD 64 (2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf (recommending use of "large datasets" to address numerous issues in clinical research).
[29] *Id.* at 63.
[30] *Id.* at 64.
[31] Efthimios Parasidis, *Patients Over Politics: Addressing Legislative Failure in the Regulation of Medical Products*, 2011 WIS. L. REV. 929, 966-67 (2011).
[32] *Id.* at 965.
[33] *Id.*
[34] *Id.* at 967-68.

"evidence-based decision support, quality management, and health-outcomes reporting at both the individual and population levels."[35]

In the realm of health information technology, Parasidis, Hoffman, and Podgurski are among the first legal academics to convincingly merge literatures of health system transformation, practical implementation, and legal guidance. They suggest the practical feasibility of transforming healthcare generally, and post-market pharmaceutical surveillance in particular, into an information industry with the types of productivity gains we usually associate only with Silicon Valley.[36] As Parasidis notes of the U.S. Food and Drug Administration's (FDA) deployment of "Mini-Sentinel:"

> Rather than creating a centralized database, Mini-Sentinel uses a distributed data network that is linked by a coordinating center. The Mini-Sentinel data network incorporates EHRs from diverse data sets that are maintained by public and private stakeholders. Each data partner retains control over its own patient-level data and permits others to access its aggregated and de-identified medical data.[37]

Just as the U.S. Department of Homeland Security and the National Security Agency have advanced domestic intelligence capabilities by querying distributed databases from diverse public and private sector partners, the FDA now can apply such technology toward improving population health.[38] For example, consider the deficiencies in America's system of pharmacovigilance -- "the science and activities relating to the detection, assessment, understanding and prevention of adverse effects or any other drug-related problem."[39] The tactics and methods developed by leading information industries could be applied to the assessment of drugs and devices, raising very difficult issues under health privacy laws.

---

[35] *Id.* at 964.

[36] *See id.* at 984-86 (proposing integration of post-market drug surveillance into an extant health IT infrastructure); Hoffman & Podgurski, *Improving Health Care Outcomes, supra* note 25, at 425 (proposing the development of a "broadly accessible framework" that enables doctors to quickly perform comparisons of treatments); Hoffman & Podgurski, *Finding A Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J. L & TECH. 103, 151 (2008) (recommending regulations that require doctors to use information technology to improve practices).

[37] Parasidis, *supra* note 31, at 971.

[38] For an account of the DHS approach, see Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L. J. 1441, 1449 (2011) (discussing the close ties of private entities to state and federal "fusion centers," which collect and share information and intelligence).

[39] World Health Organization, THE IMPORTANCE OF PHARMACOVIGILANCE 7 (2002), *available at* http://apps.who.int/medicinedocs/pdf/s4893e/s4893e.pdf.

Observational research (based on actual patients' experience with drugs and procedures) may turn out to be more useful than clinical trials in many ways once a critical mass of outcomes has been recorded and researchers can control for environmental and other variations.[40] Digitized health data should enable extraordinary new possibilities for medical research.[41]

Efthimios Parasidis's article, *Patients Over Politics*, examines the implications of new technologies for pharmacovigilance.[42] Parasidis envisions taking the type of analysis in comparisons of treatment effectiveness to a population-wide analysis. He convincingly argues that post-approval surveillance will only reach its full potential if a wider array of stakeholders begins to take advantage of the emerging health data infrastructure to critically evaluate the effects of various treatments.[43] The free flows of data elevated to constitutional status in the case of *Sorrell v. IMS Health Inc.*[44] may also eventually improve pharmacovigilance.[45] But just as *Sorrell* eviscerated a Vermont patient privacy law in order to promote data flows, so future decisions in this area may end up limiting efforts by policymakers to define and enforce the proper restrictions on data flows.[46]

Finally, there is the growing pressure from patients to develop control over medical records for their own purposes. While HITECH split responsibility for EHRs and personal health records (PHRs) between the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), the centrifugal pressure toward integrated and comprehensive databases may not make this a sensible decision for long. While the "sharing or exchange of data between PHRs and healthcare providers or their EHRs" was "speculative" as of 2009,[47] the interfaces between PHRs and EHRs will be tested by new applications and mobile health (mHealth) developments.[48] For example, members of the "quantified self" movement can

---

[40] *Id.* at 66-67.
[41] President's Council of Advisors on Sci. & Tech., *supra* note 28, at 5 (describing potential improvements in care).
[42] Parasidis, *supra* note 31, at 977 (proposing "reform measures that mitigate risk-enhancing aspects of the regulatory framework for medical products").
[43] *Id.* at 970–74.
[44] 131 S. Ct. 2653 (2011).
[45] *Id.* at 2670-72 (ruling that drug companies have a constitutional right to access certain types of data without undue state interference). For a critical description of the stakes of *Sorrell*, see David Orentlicher, *Prescription Data Mining and the Protection of Patients' Interests*, 38 J.L. MED. & ETHICS 74, 81 (2010) ("When people develop relationships with their physicians and pharmacists, they are entitled to the assurance that information about their medical condition will be used for their benefit and not to place their health at risk or to increase their health care costs."); Frank Pasquale, *Privacy as a First Amendment Value*, THE HEALTH CARE BLOG (Apr. 29, 2011), http://thehealthcareblog.com/blog/2011/04/29/rethinking-ims-health-v-sorrell-privacy-as-a-first-amendment-value/.
[46] Beverly Cohen, *Regulating Data Mining Post-Sorrell: Using HIPAA to Restrict Marketing Uses of Patients' Private Medical Information*, 47 WAKE FOREST L. REV. 1141, 1148 (2012); Orentlicher, *supra* note 45, at 74; Michael Heesters, *An Assault on the Business of Pharmaceutical Data Mining*, 11 U. PA. J. BUS. L. 789 (2009).
[47] Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers*?, 1 DREXEL L. REV. 216, 226 (2009).
[48] Ethan Katsh, *et al.*, *Is there an App for That? Electronic Health Records and a New Environment of Conflict Prevention and Resolution*, 74 LAW & CONTEMP. PROBS. 31, 34 (2011) (describing translational difficulties between

track their pulse, sleep time, weight, mood, and meters walked per day, based on smartphone-enabled self-monitoring.[49] Isn't some or all of this data (properly summarized or visualized) something that a physician or wellness coach would want some access to? Yet providers may not be building in the type of "privacy by design" necessary to make this type of data exchange safe for all involved in it.

More modest forms of clinical decision support may also merge with marketing. Cash-strapped practices are also liable to want to try to buy in to "free" EHR models which are ad-based. Even once HITECH subsidies are accounted for, physicians will still often treat their IT spend as a fixed cost to be minimized. One of the most successful cloud-based email hosting services, Gmail, capitalizes on data analyzed in its records to serve targeted ads. Some EHRs are based on this model, and may well be aiming to synthesize multiple records (or a whole practice's records) to sell high-impact advertising opportunities to pharmaceutical firms, device makers, or other entities. Given the technological flavor of much recent fraud enforcement effort at the Centers for Medicare & Medicaid Services (CMS) and its various contractors, such data may also be very useful for their purposes as well.[50]

III. Health Privacy and Data Security in a Cloud Computing Context

Cloud computing may fuel a convergence of research, treatment, and marketing opportunities. But before it can do so, healthcare providers, health plans, and other healthcare entities covered by HIPAA ("covered entities" or CEs) must be assured that they will be able to abide by longstanding privacy and security obligations under HIPAA. This section explores how aspects of HIPAA will affect both covered entities' and patients' views of cloud computing options. Part A examines the role of business associate agreements (and regulation of business associates (BAs)) in assuring accountability in a networked cloud computing environment. Part B explores some of the issues patients are likely to raise (and face) as cloud computing becomes more popular.

A. HIPAA in the Cloud from a Covered Entity's Perspective

EHRs and PHRs, and noting that "the transition from paper to digital in the healthcare field is still . . . an extremely complex transition involving patients, doctors, and a variety of old and new stakeholders."); Lisa Wangsness, *Electronic Health Records Raise Doubt*, BOSTON GLOBE, Apr. 13, 2009, at C1 (describing mistake in downloading of EHR information to a PHR).

[49] Anita Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47 (2008) ("The lifelog could easily store data pertaining to purely biological states derived from continuous self-monitoring of, for example, heart rate, respiration, blood sugar, blood pressure, and arousal.").

[50] Kathleen Sebelius, Sec'y Dep't Health & Human Servs., Address at the Stop Medicare Fraud Summit (Aug. 26, 2010), *available at* http://www.hhs.gov/secretary/about/speeches/smfsummit.html ("Under the new law, we're also making it easier for law enforcement officials to see health care claims data from around the country in one place, combining all Medicare-paid claims into a single, searchable database.").

Among the Omnibus HIPAA Rule provisions most significant for cloud computing are those pertaining to liability.[51] The final rule makes clear that liability extends down the chain well beyond covered entities to reach business associates, which include certain subcontractors.[52] While the prior HIPAA model of enforcement focused on CEs, after the HITECH Act, a business associate is regulated directly by HIPAA, making BAs directly liable for civil monetary penalties for their violations.[53] HIPAA also contains a breach notification rule, which binds CEs and BAs.[54] As discussed below, a cloud service provider that creates, receives, maintains, or transmits PHI on behalf of a covered entity comes within HIPAA's definition of business associate,[55] and thus it is important for cloud service providers to understand the magnitude of these liability provisions.

1. Responsibilities of Covered Entities

Under the Omnibus HIPAA Rule, CEs remain responsible for a host of Privacy Rule and Security Rule requirements aimed at safeguarding protected health information.[56] For example, the Privacy Rule requires a CE, among other things, to adopt written privacy policies and procedures; designate a privacy official to implement these policies and procedures; and train its

[51] The recent Omnibus HIPAA Rule is designed to "strengthen the privacy and security protections established under [HIPAA] for individual's health information maintained in electronic health records and other formats." Modifications to the HIPAA Privacy, Security, Enforcement, and Breach-Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013) [hereinafter Final Omnibus HIPAA Rule Preamble, 78 Fed. Reg at X]. In addition, the rule intends to "increase flexibility for and decrease burden on the regulated entities." *Id.*

[52] The HIPAA Privacy Rule regulates covered entities' use and disclosure of protected health information. The covered entities regulated by HIPAA include most health plans, healthcare providers, and health care clearinghouses. The term "health care provider" is defined by the Rule as "a provider of services . . . , a provider of medical or health services . . . , and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103. Under HIPAA, any time a covered entity uses or discloses protected health information, the use or disclosure must comply with HIPAA's privacy provisions. The term "use" is broadly defined as "the sharing, employment, application, utilization, examination, or analysis" of health information protected by HIPAA. *Id.* "Disclosure" is also broadly defined as "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information." *Id.*

[53] 42 U.S.C. § 17931 ("In the case of a business associate that violates any security provision . . . [the civil monetary penalties rules] shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision."); *see also* 45 C.F.R. § 160.402.

[54] After HITECH, any BA or "third party servicer," upon discovery of a breach, must notify the CE within a reasonable time (not to exceed 60 days). 42 U.S.C. § 17932(b), (d)(1) (2012). The CE, then, must notify the patient of the breach within a reasonable time (not to exceed 60 days). 42 U.S.C. § 17932(a), (d)(1) (2012). Moreover, if the data breach affects more than 500 people, the CE also must notify HHS and the media. 42 U.S.C. § 17932(e)(2), (3). The responsibilities of the parties with respect to notification should be outlined and described in the agreement between the CE and the cloud servicer. Foley & Lardner, *supra* note 16, at 13-14 ("Beyond establishing the procedural requirements and timeframes for reporting to the customer, the agreement should set forth the procedures and role of the parties with respect to investigation of the breach and notification of individuals."). *See also* 45 C.F.R. §§ 164.400414 (HIPAA breach notification rules).

[55] *See* 45 C.F.R. § 160.103.

[56] The Omnibus HIPAA Rule defines protected health information in 45 C.F.R. § 160.103.

workforce with respect to these policies.[57] The Security Rule requires a CE "to maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure." [58] Among the Security Rules requirements is an obligation for CEs to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity . . . ."[59] CEs are permitted to disclose PHI to a BA "if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information," although they are not required, however, to obtain satisfactory assurances from a BA that is a subcontractor.[60] In the event of a breach of unsecured PHI, a CE is responsible for making the notifications to individuals, the media, and the Secretary, as applicable, as set forth in Subpart D of the Omnibus HIPAA Rule.[61]

If a CE fails to comply with an administrative simplification provision, it is directly liable for civil, and in some cases criminal, penalties, as discussed in Section 3(A)(iii), below.[62] The Omnibus HIPAA Rule eliminated an affirmative defense that had allowed a covered entity to avoid a penalty if it "did not know and with the exercise of reasonable diligence would not have known of the violation (since such violations are now punishable under the lowest tier of penalties)." [63] It also eliminated an exception to liability "for the acts of its agent in cases where the agent is a business associate, the relevant contract requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations."[64] In addition, a CE "must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule."[65] But as long as a violation occurring after February 18, 2009 is not due to willful neglect

[57] *See* 45 C.F.R. §§ 164.520, 164.530(a)(1), (b); Alden J. Bianchi *et al.*, Mintz Levin, *Advisory: The New HIPAA Omnibus Rule & Your Liability* (Feb. 15, 2013), http://www.mintz.com/newsletter/2013/Advisories/2663-0213-NAT-HL/index.html.
[58] Bianchi *et al.*, *supra* note 58; *see* 45 C.F.R. §§ 164.302-318 (Security Rule).
[59] 45 C.F.R. § 164.308(a)(1)(ii)(A); *see also* Bianchi *et al.*, *supra* note 58.
[60] 45 C.F.R. § 164.502(e)(1)(i).
[61] *See id.* §§ 164.400-414.
[62] *Id.* § 160.402(a); Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5589.
[63] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5585; *see also* James Swann, BNA Health IT Law & Industry Report, *Final HIPAA Enforcement Rule Includes Increased Civil Money Penalty Structure* (Jan. 21, 2013).
[64] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed Reg at 5580; James Swann, *supra* note 63.
[65] Bianchi *et al.*, *supra* note 57.

and the CE corrects it within thirty days, HHS may not impose a civil monetary penalty on the CE.[66]

2. Provisions Allocating Responsibility and Liability to Business Associates

HIPAA's Privacy Rule has long required CEs to have contracts or other arrangements with BAs "to ensure that the business associates safeguard protected health information, and use and disclose the information only as permitted or required by the Privacy Rule."[67] The Security Rule similarly has required CEs to "have contracts or other arrangements in place with their business associates that provide satisfactory assurances that the business associates will appropriately safeguard the electronic protected health information they create, receive, maintain, or transmit on behalf of the covered entities."[68] Prior to the Omnibus HIPAA Rule, if BAs violated these requirements, CEs could seek damages for breach of the business associate agreement (BAA), but BAs were not subject to penalties from HHS if they violated HIPAA.[69]

As required by HITECH, the Omnibus HIPAA Rule makes BAs *directly liable* for compliance with certain of the HIPAA Privacy and Security Rules.[70] A BA will be directly liable, for example, for any uses or disclosures of PHI that violate the Privacy Rule or the terms of its BAA.[71] BAs also are required to provide notification to the CE in the event of a breach of unsecured PHI; to comply with the minimum necessary rule; to cooperate with the Secretary during complaint investigations and compliance reviews; to provide an accounting of disclosures of PHI; and to make an electronic copy of PHI available to an individual or CE when an individual requests it.[72]

BAs also must comply with all facets of the Security Rule, which Joy Pritts, chief privacy officer at the Office of the National Coordinator for Health IT, has called "the most significant

---

[66] *See* 45 C.F.R. § 160.410(c); James Swann, *supra* note 63.
[67] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5567.
[68] *Id.*
[69] *See* Robert Belfort *et al.*, Bloomberg BNA Health IT Law & Industry Report, *HIPAA Omnibus Rule Reshapes Landscape for Health Care Privacy, Security Compliance* (Jan. 28, 2013), *available at* http://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/HealthLaw@Manatt/BNA%20Article_HIPAA%20Omnibus%20Rule.pdf.
[70] *See* 45 C.F.R. § 160.102(b); *see also* Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5566, 5568.
[71] *See* 45 C.F.R. § 164.502(a)(3); Final Omnibus HIPAA Rule Preamble, supra note 51, 78 Fed. Reg. at 5568; Carlos Leyva, *HIPAA Omnibus Rule Summary* (Feb. 3, 2013), http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php.
[72] *See* 45 C.F.R. §§ 160.310(b), 164.410, 164.502(a)(4)(ii), (b),164.528; Bianchi *et al.*, *supra* note 57; Belfort *et al.*, *supra* note 69; Leyva, *supra* note 71. BAs are not subject to all Privacy Rule requirements. For example, they are not required to provide notice of privacy practices or to designate a privacy official, unless required by the applicable BAA. *See* 45 C.F.R. §§ 164.520, 164.530(a)(1)(i); Employee Benefits & Executive Compensation, *ADVISORY: New HIPAA Omnibus Rule: Issues for Employer Plan Sponsors and Group Health Plans* (Mar. 11, 2013), http://www.alston.com/Files/Publication/19c1650b-c278-4abf-9c1b-9fff28d27c4a/Presentation/PublicationAttachment/7ed0617b-c6b1-4350-8e38-a5295c262cd1/13-195-HIPPA-Omnibus-Rule.pdf.

security provision in the massive new Omnibus HIPAA Rule."[73] Thus, BAs are responsible for completing a risk analysis and complying with HIPAA's administrative, physical, and technical safeguard provisions, among other requirements.[74]

The Omnibus HIPAA Rule also revised the definition of BAs to expressly include particular entities, including many cloud service providers. First, it expressly includes "[a] Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information."[75] Citing the evolving nature of what organizations will qualify as health information organizations, HHS declined to define this term, but it indicated its intention to publish additional guidance.[76]

HHS did, however, provide guidance in the preamble to the Omnibus HIPAA Rule as to what it means to have access on a routine basis to PHI. This fact-specific determination looks to "the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity."[77] While mere conduits of PHI do not satisfy this requirement, HHS emphasized that the conduit exception is narrow and "intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs), providing mere data transmission services."[78] Mere transmission includes "temporary storage of transmitted data incident to such transmission."[79] Conduits transport PHI but "do not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law."[80] But an entity that requires access to PHI to perform a service for a covered entity – "such as a Health Information Organization that manages the exchange of [PHI] through a network on behalf of covered entities through the use

[73] Howard Anderson, *The Security Highlight of HIPAA Omnibus Shining a Spotlight on Business Associates* (Mar. 1, 2013), http://www.bankinfosecurity.com/blogs/security-highlight-hipaa-omnibus-p-1431.
[74] 45 C.F.R. §§ 164.302-318 (Security Rule); Employee Benefits & Executive Compensation, *supra* note 72.
[75] 45 C.F.R. § 160.103; Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5571. The Rule defines "person" to mean "a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public of private." 45 C.F.R. § 160.103.
[76] *See* Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5571. As discussed in the text below, while the old rule had no mention of a company that merely stored data, leading to much industry confusion, the Omnibus HIPAA Rule states a BA is a person who, on behalf of a CE: "creates, receives, *maintains*, or transmits protected health information for a function or activity regulated by this subchapter." *Id.* at 5688. HHS makes clear that "an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information." *Id.* at 5571.
[77] *Id.*
[78] *See id.*
[79] *See id.*
[80] *See id.* at 5572.

of record locator services for its participants" -- is not a mere conduit and instead is a business associate.[81]

Entities need not access PHI, however, to be deemed business associates. Rather, an entity that *maintains*, as distinguished from an entity that merely transmits, PHI on behalf of a covered entity is a business associate, even if the entity does not access the PHI. For example, "a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis."[82] HHS explained that although conduits and entities that maintain PHI both have the opportunity to access PHI, "the difference between the two situations is the transient versus persistent nature of that opportunity." To reflect this distinction, HHS amended the definition of business associate to include creating, receiving, *maintaining*, or transmitting PHI on behalf of a covered entity.[83]

At a recent conference, David Holtzman of HHS's Office for Civil Rights (OCR) indicated that cloud service providers are BAs if among their functions performed on behalf of CEs is to maintain PHI, even if the contract does not "'contemplate any access or access only on a random or incidental basis,'" because "[t]he test is persistence of custody, not the degree – if any – of access."[84] Yet he also reportedly acknowledged a potential qualification to this rule related to encryption. According to Holtzman, OCR has not yet determined whether HIPAA will bind an entity that maintains encrypted data for a CE but does not have the key to access that data.[85] It is crucial for OCR to clarify its position on this issue, given that it is not uncommon for cloud service providers to maintain encrypted PHI without the key.

The Omnibus HIPAA Rule also makes plain that "[a] person that offers a personal health record to one or more individuals on behalf of a covered entity" also is a business associate for purposes of HIPAA obligations and liability.[86] Not all personal health record vendors are business associates, however, and HHS expects to issue future guidance on this issue.[87] Whether a vendor offers personal health records on behalf of a covered entity is a fact-sensitive inquiry.[88] HHS opined that it is insufficient for a vendor and covered entity to enter "an interoperability relationship" by, for example, establishing the electronic means (*i.e.*, an interface) for a covered

[81] *See id.*
[82] *See id.*
[83] *See* 45 C.F.R. § 160.103; Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5572.
[84] Kendra Casey Plank, *Cloud Providers Often Are Business Associates under HIPAA, Officials Say*, 22 HEALTH LAW REPORTER 858 (BNA) (June 6, 2013) (quoting Holtzman at "Safeguarding Health Information: Building Assurance through HIPAA Security," a conference sponsored by OCR and the National Institute for Standards and Technology on May 21-22, 2013).
[85] *See id.*
[86] 45 C.F.R. § 160.103; Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5571.
[87] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5572.
[88] *Id.*

entity's electronic health record to send PHI to the vendor.[89] Even where an individual has given written authorization to share data, and the covered entity and vendor have agreed on details regarding data sharing, such as technical specifications for the exchange of data and the need for confidentiality, the vendor is not necessarily offering the record on behalf of the covered entity.[90] But a vendor hired by and given access to PHI by a covered entity to permit the vendor "to provide and manage a personal health record service" for the covered entity's patients or enrollees is a business associate.[91] Where a vendor offers personal health records both directly to individuals and on behalf of covered entities, the vendor is deemed a business associate only in the latter capacity.[92] HHS explained that the conduit exception does not apply to a vendor offering a personal health record to an individual on behalf of a covered entity because such a vendor is maintaining PHI and not serving as a mere conduit.[93] Consistent with its treatment of data storage companies, such a vendor is a business associate if it has the ability to access PHI, even if it does not exercise this ability.[94]

The Rule also defines business associates to include "a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate."[95] Subcontractor, in turn, "means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce[96] of such business associate."[97] HHS explains that the function, activity, or service delegated to the subcontractor is one the business associate agreed to perform for a covered entity or another business associate.[98]

Determining if a subcontractor is acting on behalf of a business associate is the same analysis that applies to whether a business associate is acting on behalf of a covered entity.[99] For example, if a business associate third party administrator hires a company to perform document and media shredding and disposal of PHI, this shredding company would be directly responsible for complying with applicable HIPAA Security and Privacy Rules.[100] Similarly, a subcontractor

---

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] 45 C.F.R. § 160.103.
[96] "Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." *Id.*
[97] *Id.*
[98] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5573.
[99] *Id.* at 5572.
[100] *Id.* at 5573. But if a business associate hires a subcontractor to shred documents that do not contain PHI, then the subcontractor is not a business associate. *See id.* at 5574.

hired to support a business associate with personal health record functions is a business associate and thus required to comply with HIPAA's breach notification rule.[101]

This subcontractor revision aims to prevent covered entities and business associates from avoiding liability for HIPAA privacy and security violations by subcontracting functions.[102] "[D]ownstream entities that work at the direction of or on behalf of a business associate and handle protected health information would also be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary business associate, and likewise would incur liability for acts of noncompliance."[103] Thus, just as CEs must obtain satisfactory assurances from their BAs,

> business associates must do the same with regard to subcontractors [that satisfy the Omnibus HIPAA Rule's definition], and so on, no matter how far 'down the chain' the information flows. This ensures that individuals' health information remains protected by all parties that create, receive, maintain, or transmit the information in order for a covered entity to perform its healthcare functions.[104]

Carlos Leyva, an internet attorney and frequent contributor to hipaasurvivalguide.com, has flagged the "downstream impact' of this modification" as very significant.[105]

Importantly, covered entities are not required to contract directly with subcontractors to establish a chain of liability.[106] Instead, business associates are responsible for obtaining satisfactory assurances in the form of a written contract or other arrangement that a subcontractor will appropriately safeguard PHI.[107] But HHS intended liability to attach to a subcontractor, even if the business associate failed to enter a business associate contract with the subcontractor, as long as the party is an agent of, or other person acting on behalf of, the business associate, as discussed in Section III.A.3 below.[108]

---

[101] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5572. HHS emphasized that despite extending the definition of business associate to include subcontractors, financial institutions that are performing payment processing activities under Section 1179 of HIPAA continue to be excluded from the definition of business associates. *See id.*

[102] *Id.* at 5572-73.

[103] *Id.* at 5573.

[104] *Id.* at 5574.

[105] Leyva, *supra* note 71.

[106] *See* 45 C.F.R. §§ 164.308(b)(1) and 164.502(e)(e)(i); Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5573.

[107] *See* 45 C.F.R. § 164.308(b)(2); HIPAA Omnibus Final Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5573.

[108] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5572; *see also* Leyva, *supra* note 71 ("A person/entity ("Person") becomes a Business Associate by definition, and NOT because there happens to be a Business Associate contract in place; therefore liability attaches immediately when a Person "creates, receives, maintains, or transmits Protected Health Information on behalf of a Covered Entity.") (emphasis in original).

This expansion of HIPAA's reach makes business associates, including subcontractors who satisfy HIPAA's definition of BAs, directly liable for civil monetary, and in some cases criminal, penalties for violations of applicable HIPAA rules.[109]

3. Agency Liability of Covered Entities and Business Associates

In addition to being liable for their own HIPAA violations, covered entities and business associates also can be liable for civil monetary penalties for their agents' violations.[110] Under the Omnibus HIPAA Rule, a CE or BA "is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity [or business associate] . . . acting within the scope of the agency."[111] Agents of CEs may include a workforce member or business associate, whereas agents of BAs may include a workforce member or a subcontractor.[112] HHS intended this revision "to ensure, where a covered entity or business associate has delegated out an obligation under the HIPAA Rules, that a covered entity or business associate would remain liable for penalties for the failure of its business associate agent to perform the obligation on the covered entity or business associate's behalf," even if a compliant business associate agreement is in place.[113]

In adopting this revision, HHS expressed its view that liability for agency violations would not unduly burden CEs or BAs, finding that liability for agents is customary under the common law.[114] Despite describing agency liability as customary, HHS offered additional guidance on when a BA will be deemed an agent. This fact-specific inquiry considers the terms of the BAA and the totality of the circumstances involved in the relationship between the parties.[115] Importantly, HHS rejected comments suggesting that parties could avoid these fact-intensive inquiries by determining agency in their contracts. Using terms, statements, or labels such as independent contractor to refer to a party in the contract will not control the agency analysis.[116]

---

[109] *See* 45 C.F.R. § 160.402(a); Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5589.
[110] 45 C.F.R. § 160.402(c); Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5580.
[111] 45 C.F.R. § 160.402(c)(1)-(2). HHS omitted from Section 160.402 the prior exception to agency liability "for covered entity liability for the acts of its agent in cases where the agent is a business associate, the relevant contract requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations." Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5580.
[112] 45 C.F.R. § 160.402(c)(1)-(2).
[113] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5580.
[114] *Id.* at 5581.
[115] *Id.*
[116] *Id.*; *see also* Leyva, *supra* note 71 ("Covered Entities and Business Associates are liable for the acts of their Business Associate agents. Comment: the Federal Common Law of Agency is controlling AND Covered Entities and Business Associates need to pay close attention to the amount of control they exercise over a third party with which they have a Business Associate contract. What the parties call each other is not dispositive; exercise of control is key.") (emphasis in original).

Rather, the focus of the agency analysis is whether the covered entity, or business associate, in the context of business associate-subcontractor relationships, has "the right or authority . . . to control the business associate's conduct in the course of performing a service on behalf of the covered entity [or business associate]."[117] An example of the type of control that distinguishes agency from non-agency relationships is when a covered entity or business associate has authority to give interim instructions or directions during the course of the relationship. But agency generally will not exist where a BAA "sets terms and conditions that create contractual obligations between the two parties."[118] As HHS explained, "if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent."[119] Thus, where a covered entity delegates or contracts out performance of a specific HIPAA obligation, whether the business associate is an agent of the CE will "depend on the right or authority to control the business associate's conduct in the performance of the delegated service based on the right of a covered entity to give interim instructions."[120]

HHS also identified several factors to consider in determining the scope of agency: (1) the time, place, and purpose of a business associate's conduct; (2) whether a business associate's agent engaged in a course of conduct subject to a covered entity's control; (3) whether a business associate agent's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and (4) whether or not the covered entity reasonably expected that a business associate agent would engage in the conduct in question.[121]

In rejecting a commentator's suggestion that there would be no agency liability when a BA breaches the BAA, HHS explained that just because a BA deviates from the terms of a BAA does not mean that the BA is operating outside of the scope of agency.[122] As a general rule, a BA agent's conduct is within the scope of agency when it "occurs during the performance of the assigned work or incident to such work, regardless of whether the work was done carelessly, a mistake was made in the performance, or the business associate disregarded a covered entity's specific instruction."[123] But a BA generally acts outside of the scope of agency when its conduct "is solely for its own benefit (or that of a third party)" or the conduct is "not intended to serve any purpose of the covered entity."[124]

---

[117] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5581.
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *See id.*
[122] *Id.* at 5582.
[123] *Id. But cf. id.* at 5587 ("An agent that fails to notify a covered entity or business associate may be acting outside its scope of authority as an agent.")
[124] *Id.*

An important consideration in determining if the BA is an agent is the type of service and skill level required to perform the service.[125] For example, HHS opined that it is unlikely that a business associate hired by a small provider to de-identify PHI would be deemed its agent since it is unlikely the covered entity has the requisite expertise with this particular service to give interim instructions to the BA.[126] A business associate hired to perform services that a covered entity is legally or otherwise prohibited from performing, such as accreditation, is unlikely to be deemed to be an agent of that covered entity.[127] But a covered entity does not need to retain the right or authority to control every aspect of a BA's activities for the BA to be an agent.[128] Further, a BA can be an agent even if the CE does not exercise its right of control as long as there is evidence that it has the authority to do so.[129] HHS further made clear that agency can be found even where CEs and BAs are geographically dispersed, including if they are in different countries.[130]

Carlos Leyva recently noted that although "Business Associates and Covered Entities should clearly recognize that we are definitely 'not in Kansas anymore,'" he does not believe the healthcare industry has fully realized the implications of these changes.[131] As some have observed, agency liability "significantly impacts the relationship of covered entities and their business associates, potentially requiring greater monitoring by the covered entity when the business associate is an agent."[132] CEs and BAs have to wrestle with these fact sensitive issues so they can assess the risks of liability from different relationships. They also need to engage in ongoing risk assessment before and during contractual relationships to monitor compliance by downstream actors. OCR is responsible for enforcing the HIPAA Privacy and Security Rules, and OCR Director Leon Rodriguez recently commented that ""[o]ne of the most consistent findings

[125] *Id.* at 5581.
[126] *Id.*
[127] *Id.* at 5581-82.
[128] *Id.* at 5582.
[129] *Id.*
[130] *Id.*
[131] Leyva, *supra* note 71; *see generally* Proskauer, *HHS Issues HIPAA/HITECH Omnibus Final Rule Ushering in Significant Changes to Existing Regulations: Client Alert* (Jan. 29, 2013), http://www.proskauer.com/publications/client-alert/hhs-issues-hipaa-hitech-omnibus-final-rule-ushering-in-significant-changes-to-existing-regulations/ ("Business associates, including Health Information Organizations, E-prescribing Gateways, entities that provide data transmission services for PHI and require routine access to such PHI, and personal health record vendors will have additional work to do as well, including: drafting and adopting policies, procedures and related documents if they do not have them in place already; performing and documenting risk assessments if they have not done so; and reviewing their relationships with subcontractors and entering into business associate agreements with them as necessary.").
[132] Rebecca L. Williams *et al.*, DAVIS WRIGHT TREMAINE LLP, *Advisories: New Omnibus Rule Released: HIPAA Puts on More Weight* (Jan. 23, 2013), http://www.dwt.com/New-Omnibus-Rule-Released-HIPAA-Puts-on-More-Weight-01-23-2013/.

[OCR is seeing] is failure to conduct risk assessments of where protected health information is vulnerable.'"[133]

CEs and BAs have a great deal of work ahead of them.[134] As the Proskauer law firm noted, "[c]overed entities and business associates will have to consider carefully how decisions to delegate responsibility for tasks such as handling breach notification and their retention of authority to provide instructions to their business associates and contractors with respect to certain tasks will affect their exposure to liability."[135] Updating and renegotiating BAAs, for example, is a "massive" undertaking, especially for large health systems that can have as many as 20,000 business associates.[136] On January 25, 2013, HHS published an updated sample business associate agreement that may be of some assistance, although CEs and BAs almost certainly will need to supplement this sample.[137] Negotiations could be more contentious and protracted now that BAs' direct liability gives them more reason to be cautious.[138]

Although the Omnibus HIPAA Rule was effective March 26, 2013, covered entities and business associates have until September 23, 2013 to comply with most of its requirements.[139] Written contracts or other arrangements between CEs and BAs that were entered into before January 25, 2013, complied with the law then in effect, and are not renewed or modified from March 26, 2013 until September 23, 2013 will be deemed compliant with the Omnibus HIPAA

[133] Marianne Kolbasuk McGee, *HIPAA Omnibus Compliance Help on Way HHS Rolling Out Web-based Educational Tools* (Feb. 20, 2013), http://www.healthcareinfosecurity.com/hipaa-omnibus-compliance-help-on-way-a-5524.

[134] *See generally* Leyva, *supra* note 71 ("HHS is saying that compliance with the HIPAA Security Rule was required (to a degree) even before the HITECH Act and the HIPAA Omnibus Rule. Therefore, the new HIPAA Security Rule requirements should just necessitate incremental adjustments. Although that may be true under the 'letter of the law,' as a practical matter nothing could be further from the truth. Prior to the HITECH Act HIPAA was an unenforced paper tiger. Business Associates have a lot of catching up to do, and for that matter, so do most Covered Entities.").

[135] Proskauer, *supra* note 131. The standard for breach notice has changed due to the Omnibus HIPAA Rule. Before, notification was only required if a breach caused a "significant risk of harm" to the data subjects. Deven McGraw, *Final HIPAA Rules a Major Step Forward, But There's More Work To Be Done*, ihealthbeat (Feb, 8, 2013), http://www.ihealthbeat.org/perspectives/2013/final-hipaa-rules-a-major-step-forward-but-theres-more-work-to-be-done.aspx. Now, however, notification is always required unless the discovering entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of a number of listed factors." Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5695.

[136] Kendra Casey Plank, Bloomberg BNA Health IT Law & Industry Report, *Breach, Business Associate Obligations Biggest Provisions in HIPAA Rule, Experts Say* (Jan. 21, 2013), *available at* http://www.morganlewis.com/index.cfm/newsID/c1deaa8b-8191-4cb4-9f52-1e7d61986de2/fuseaction/news.detail.

[137] U.S. Dep't of Health & Human Servcs., *Sample Business Associate Agreement Provisions* (published Jan. 25, 2013), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

[138] Anne Foster *et al.*, BakerHostetler, *Special Edition: Health Law Update: A Baker's Dozen of Significant Changes from the HIPAA/HITECH Rule* (Feb. 28, 2013), http://www.jdsupra.com/legalnews/special-edition-health-law-update-feb-42876/.

[139] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5566.

Rule until the earlier of the date it is renewed or modified on or after September 23, 2013; or September 22, 2014.[140]

4. Increased Penalties and Enforcement

This increased liability for BAs comes as HHS finalizes HITECH's enhanced civil monetary penalties for noncompliance with HIPAA's requirements.[141] Before HITECH, HHS could impose no greater than $100 for each violation, with an annual cap of $25,000 imposed on a given covered entity for identical violations.[142] The Omnibus HIPAA Rule adopted a revised penalty scheme with penalty amounts ranging from $100 to $50,000 per violation up to a maximum aggregate penalty of $1.5 million for violations of an identical provision per calendar year.[143] Thus, if CEs and BAs violate multiple provisions, the maximum aggregate penalty will be $1.5 million per identical violation.[144]

In addition to the threat of increased penalty amounts, OCR has indicated that it is focused on increasing enforcement efforts, no matter the size of the entities.[145] Historically, HIPAA enforcement has been lackluster. But Theodore J. Kobus III from Baker & Hostetler in New York described OCR enforcement efforts as "aggressive" since HITECH.[146] Lynn Sessions with Baker & Hostetler in Houston similarly noted that HHS increasingly has been pursuing resolution agreements and civil penalties against "relatively small providers," who "often are less prepared to comply with HIPAA requirements."[147]

In April 2012, for example, OCR reached a $100,000 settlement with Phoenix Cardiac Surgery, P.C. ("PCS"), a small cardiology practice. [148] PCS allegedly violated HIPAA by, among other things, failing to enter BAAs with cloud service providers that stored and had access to electronic PHI and failing to establish adequate policies and safeguards to protect PHI.[149] OCR Director Leon Rodriguez recently indicated that enforcement under the Omnibus HIPAA Rule "will become tougher" and will include enforcement resulting from breach investigations and random audits.[150] Reportedly, from September 2009 through December 2012,

---

[140] *See* 45 C.F.R. § 164.532(e).
[141] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5566.
[142] *Id.*. at 5582.
[143] 45 C.F.R. § 160.404; Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5577, 5583.
[144] *See, e.g.*, Leyva, *supra* note 71 (observing that "there is no theoretical maximum fine per year" because the maximum will depend "on how many different kinds of violations are found").
[145] Kendra Casey Plank, Bloomberg BNA Health IT Law & Industry Report, *Enforcement, Compliance Become Hot Topics for Covered Entities with Final HIPAA Rule* (Jan. 28, 2013); Anna Spencer & Julie Wagner, Bloomberg BNA Health IT Law & Industry Report, *OCR to Covered Entities: Choose Carefully among Cloud Service Providers* (Feb. 18, 2013).
[146] Plank, *Enforcement, Compliance*, *supra* note 145.
[147] *Id.*
[148] Spencer & Wagner, *supra* note 145.
[149] *Id.*
[150] *Cf., e.g.*, National Conference of State Legislatures, Incentivising State False Claims Acts (last updated Mar. 7, 2013), http://www.ncsl.org/issues-research/health/clarifying-requirements-for-a-state-false-claims-a.aspx (last

OCR received 77,200 HIPAA complaints, investigated 27,500 cases, issued 18,600 corrective actions, and collected $14.9 million in fines and resolution settlements.[151] According to Director Rodriguez, OCR is "'looking for patterns of privacy and security breaches,' including violations that seem to be longstanding and have a high risk of causing harm to individuals." [152]

B. HIPAA in the Cloud from a Patient's Perspective

While patients appreciate that their healthcare provider will usually engage in due diligence before selecting a cloud service provider, they nevertheless appreciate (if sometimes on a visceral or intuitive level) the risks involved in cloud computing scenarios. As William Pewen has observed, "Americans' support for the use of their electronic health records (EHR)--*even to facilitate treatment and payment*--is limited; 78 percent supported giving physicians access to their EHR, while only 30 percent favored health plan access."[153] Those numbers may well degenerate as awareness of cloud computing increases. Whenever there is "sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections," there is legitimate concern about additional opportunities for hacks, breaches, or misuses to occur.[154]

While covered entities and cloud service providers seek legal guidance as they work together to safeguard health data, patients have an interest in assuring that their privacy is protected. Privacy concerns of patients have slowed adoption of some digital records.[155] Moreover, where privacy concerns have been ignored (as in the rapid dissemination of pharmacy

---

visited Mar. 15, 2013) (discussing how the Deficit Reduction Act of 2005 included provisions designed to "create incentives for states to enact anti-fraud legislation modeled after the federal False Claims Act").

[151] McGee, *HIPAA Omnibus Compliance*, *supra* note 133.

[152] *Id.*

[153] William Pewen, *Breach Notice: The Struggle for Medical Records Security Continues* ("[P]atients have been outraged to receive solicitations for purchases ranging from drugs to burial plots, while at the same time receiving care which is too often uncoordinated and unsafe. It is no wonder that many Americans take a circumspect view of health IT.").

[154] World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 4, available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (2009).

[155] *See generally* Roger S. Magnusson, *The Changing Legal and Conceptual Shape of Health Care Privacy*, 32 J.L. Med. & Ethics 680, 685 (2004). Patient concerns are not hypothetical; data breaches have been on the rise. *Reported Health Data Breaches Rose by 97% in 2011*, iHEALTHBEAT (Feb. 1, 2012), http://www.ihealthbeat.org/articles/2012/2/1/health-data-breaches-increased-by-97-in-2011-report-finds.aspx; Scott Gibson, *Stolen Medical Records One of the Most Lucrative Forms of ID Theft*, HEALTHCARETECHREVIEW (Dec. 13, 2011), http://healthcaretechreview.com/stolen-medical-records-lucrative/. Over 21 million patients have suffered data security breaches reported to the federal government over the past three years. *See* section 13402(e)(4) of the HITECH Act, at U.S. Department of Health and Human Services, *Health Information Services, Breaches Affecting 500 Patients or More*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Nov. 11, 2012).

dossiers by reputational intermediaries in the early and mid-2000s), they have led to unfair, invasive, and irremediable violations of the privacy of individuals.[156]

The Omnibus HIPAA Rule addressed some of these concerns. For example, by rendering BAs directly liable for compliance with provisions of the Security and Privacy Rules, it clarified what could have been a source of troubling regulatory arbitrage.[157] It applied data security rules to "downstream entities," making cloud service providers of EHR more responsible. BAs are required to obtain assurances that disclosures they make (that are not required by law) will be "confidential." Civil penalties for BAs also provide important incentives for proper behavior.

As rulemaking (and clarifications of rules) continue, predictable criticisms have been launched. Some insist that complexity in their fields can never truly be grasped by regulators or rendered clear to consumers. Others accuse HHS of engaging in stealth industrial policy, picking winners and losers in the healthcare field by effectively outlawing certain business models and promoting others. The question now is how to respect legitimate efforts to innovate, while still protecting vital patient interests in privacy (and understanding how data is being used and shared).

1. Patient Rights of Access to Records and Accountings of Disclosures

If patients are to fully "buy in" to digitization of health records (and the full array of opportunities for use of them), they will need to be able to understand exactly how their digital records exist (and are used) in an increasingly complex virtual landscape. Patients need to engage in "the right to an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested," and to have the information in formats that allow their own trusted interpreters to make sense of it.[158] Before HITECH, the HIPAA Privacy Rule made it very difficult for patients to fully understand the nature and range of health information accumulated about them, especially because disclosures for "treatment, payment and health care operations" did not need to be accounted for.[159] After HITECH, any record kept electronically needs to be in the accounting.[160]

---

[156] *See, e.g.*, Chad Terhune, *They Know What's in Your Medicine Cabinet*, BLOOMBERG BUSINESSWEEK (July 22, 2008), http://www.businessweek.com/magazine/content/08_31/b4094000643943.htm ("Two-thirds of all health insurers are using prescription data--not only to deny coverage to individuals and families but also to charge some customers higher premiums or exclude certain medical conditions from policies, according to agents and others in the industry."); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 162 (2006) ("Without consent, CVS Pharmacy, Inc. (CVS) mined its customer prescription records for the purpose of sending its customers mailings targeted to their specific medical conditions. . . .").

[157] Marianne Kolbasuk McGee, *HIPAA Omnibus Rule Released, Contains Long-Overdue Rule Modifications*, DATA BREACH TODAY (Jan. 17, 2013), http://www.databreachtoday.com/hipaa-omnibus-rule-released-a-5433.

[158] 45 C.F.R. § 164.528, *available at* http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-528.pdf.

[159] *Id.*

Nevertheless, several critical decisions need to be made to assure that this is actually a meaningful right for patients. In its *Notice of Proposed Rulemaking for HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act*, HHS recognized that "use of audit trails and the right to an accounting of disclosures improve the detection of breaches and assists with the identification of weaknesses in privacy and security practices."[161] Audit logs record the activity taking place in an information-sharing network,[162] including "queries made by users, the information accessed, information flows between systems, and date- and time-markers for those activities."[163] If audit logs are immutable and pervasively attributable to entities accessing and using information, they should seriously deter misuse of data.[164] HITECH tries to protect patients from misuse of their health information by requiring the use of "audit trails" to record each instance of access to a record and creating incentives for the use of encryption and other best practices.[165]

---

[160] Before HITECH, 45 C.F.R. § 164.528 restricted the right to an accounting of disclosures by exempting disclosures that were "to carry out treatment, payment and health care operations." 45 C.F.R. § 164.528(a)(1)(i). HITECH removed that exception. 42 U.S.C. § 17935 (2010) ("In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information. . . . the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information.").

[161] HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31427 (proposed May 31, 2011) (to be codified at 45 C.F.R. 164), *available at* https://www.federalregister.gov/articles/2011/05/31/2011-13297/hipaa-privacy-rule-accounting-of-disclosures-under-the-health-information-technology-for-economic#p-34 [hereinafter HIPAA Privacy Rule Notice of Proposed Rulemaking]. *See also* 45 C.F.R. § 170.302 (2011) ("Record actions--record actions related to electronic health information in accordance with the standard specified in § 170.210(b) . . . [and] Generate audit log [by] [e]nabl[ing] a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210(b)."); Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 75 Fed. Reg. 44591 (July 28, 2010) (to be codified at 45 C.F.R. pt. 170) (requiring that Certified EHR technology have the following capabilities "to, at a minimum, support eligible professionals' and eligible hospitals' efforts to achieve what had been proposed for meaningful use Stage 1 under the Medicare and Medicaid EHR Incentive Programs proposed rule."); 45 C.F.R. § 170.210 (2011) (explaining "[t]he date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed or deleted; and an indication of which action(s) occurred and by whom must also be recorded.").

[162] *Criminal Intelligence Systems Operating Policies*, 28 C.F.R. § 23 (2012).

[163] MARKLE TASK FORCE ON NAT'L SEC. IN THE INFO. AGE, MARKLE FOUND., IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY 1 (2006). The Markle Foundation has worked on several important reports on deploying cutting edge information technology in agencies, including HHS. *Id.* at 4.

[164] For a discussion of the importance of immutable audit logs, *see* Citron & Pasquale, *supra* note 38, at 1473 (explaining that "immutable audit logs . . . [promote] data integrity and relevance. . . . [by] watermark[ing data] with its provenance, assuring attributions and verifiability of observations (much as citations help assure the validity of an assertion in an academic work)[and promoting] tethering and full attribution of data to allow corrections to propagate through the system") (internal citations omitted).

[165] Sandra Nunn, *Managing Audit Trails*, 80 J. AM. HEALTH INFO. 44, 44 (2009) (Audit trails are "records with retention requirements."); John W. Hill *et al.*, *A Proposed NHIN Architecture*, 48 AM. BUS. L. J. 503, 517 ("HITECH expanded the reach of HIPAA's Privacy Rule. Patients must now be notified when their PHI is disclosed or used without their authorization. HITECH closed the loophole for business associates, established

Some industry comments on the HITECH rulemaking have vigorously opposed aggressive implementation of consumer rights.[166] Nevertheless, HHS has confirmed the importance of maintaining patients' access to their records. Covered entities must provide individuals "with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format."[167] It also promoted individuals' rights to determine how their records had been used by guaranteeing an accounting of disclosures.[168] In any twelve-month period, the first accounting requested by an individual from a covered entity must be provided for free, within 60 days of the request (with some narrow exceptions).[169]

2. Encryption, De-Identification, and Best Practices in an Era of Breaches

Part II above described some potential cutting edge applications of cloud computing to solve tough problems in pharmacovigilance and treatment customization. It suggested the growing convergence of research and treatment functions in data-rich environments.[170] Two of

---

patients' right to access and control of their PHI (including obtaining an audit trail showing all electronic disclosures), and prohibited companies from selling PHI without authorization."). The audit trail is a *sine qua non* for technological due process. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305-1306 (2008) (exploring the due process implications of automated system determinations and arguing that technological due process requires the inclusion of audit trails into automated systems). Nevertheless, even this mechanism of protection must be carefully implemented so that the audit process itself does not create its own potential for breaches. *See, e.g.*, Dom Nicastro, *HIPAA Auditor Involved in Own Data Breach*, HEALTHLEADERS MEDIA (Aug. 8, 2011), at http://www.healthleadersmedia.com/page-1/PHY-269480/HIPAA-Auditor-Involved-in-Own-Data-Breach (firm hired to conduct audits lost an unencrypted flash drive with 4,500 patient records).

[166] McDermott, Will, & Emery, OCR'S PROPOSED REVISIONS TO ACCOUNTING FOR DISCLOSURES STANDARD PRODUCES STRONG OPPOSITION FROM MANY COVERED ENTITIES, 1-2 (2011), *available at* http://www.mwe.com/info/news/wp1011b.pdf; Jennifer L. Edlind, HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011), Aug. 1, 2011, at 1 (responding to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as University Hospital Privacy Officer); Larry Davis, Attention: HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011), July 21, 2011, at 3 (responding to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as St. Bernards Healthcare Corporate Compliance Officer).

[167] 45 C.F.R. § 164.524(c)(2).

[168] *See id.* § 164.528. Such accountings must include "(i) The date of the disclosure; (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person; (iii) A brief description of the protected health information disclosed; and (iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§164.502(a)(2)(ii) or 164.512, if any." *Id.* § 164.528(b)(2).

[169] *Id.* § 164.528(c)(2) ("The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee."). Patients may also direct a CE to transmit a copy of the record to a designee, and there are limits on the fee, which cannot be more than the labor cost involved, and images and other linked data are to be included. *Id.*

[170] Susan Wolf has done groundbreaking work on the growing importance of treatment issues in research settings, and vice versa, in the context of "incidental findings" during research. Susan M. Wolf, *Incidental Findings in*

the most important issues affecting health technology policy are transparency and access. Regulators must decide whether to permit innovators to control data flows in order to give them incentives, and where such control must end in order to respect broader social concerns about privacy. Individuals are justly concerned that data or specimens related to them can be used in ways that compromise future opportunities. Research data may be even more sensitive than entries about a patient's existing conditions and complaints, since it can include direct and incidental findings whose implications have not been fully considered and explored by the patient.[171]

These concerns are reflected in health privacy law; the question now is whether HIPAA and cognate state laws can promote optimal standards for data collection, use, analysis, and encryption. Entities covered by HIPAA are restricted in their uses of health information in many analytic settings.[172] The Federal Policy for the Protection of Human Subjects (the "Common Rule"), the FDA framework of human-subject protections, and HIPAA and related regulations create many obligations.[173] Breach notification laws encourage encryption.[174]

One way to reassure patients that their data will not be misused is to reduce or encrypt the linkage between data and its source.[175] Various legal regimes have created a complex set of terminologies for indicating how well-linked given data is to its source.[176] Evans's account of the "networked" nature of pharmacogenomic discovery would help health IT policymakers grasp the potential of information flows, and how unharmonized legal requirements can impede

---

Neuroscience Research: A Fundamental Challenge to the Structure of Bioethics and Health Law (Oxford Handbook of Neuroethics, Judy Illes, Barbara Sahakian, eds., Oxford University Press, 2011).

[171] *See, e.g.*, Susan M. Wolf *et. al.*, *Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations*, 36 J.L. MED. & ETHICS 219, 241 (2008) (noting that an incidental finding may reveal sensitive data the person may not want shared).

[172] 45 C.F.R. § 164.502(b)(1).

[173] CARL COLEMAN *ET AL*., THE ETHICS AND REGULATION OF RESEARCH WITH HUMAN SUBJECTS (2005).

[174] 42 U.S.C. § 17932 (2010) ("A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information…in the case of a breach . . . [must] notify each individual whose unsecured protected health information has been or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosure as a result of such breach."). Via breach notification rules, HITECH encourages, but does not require, encryption, by reducing penalties for the loss of encrypted data. Harley Geiger, *HHS Should Require the Encryption of Portable Devices to Curb Health Data Breaches*, CENTER FOR DEMOCRACY & TECHNOLOGY (March 16, 2011), https://www.cdt.org/blogs/harley-geiger/hhs-should-require-encryption-portable-devices-curb-health-data-breaches. Encryption is an addressable, not a required, specification under the Security Rule; however, a covered entity must comply with certain requirements in declining to implement an addressable specification. *See* 45 C.F.R. §§ 164.306(d), 164.312(a)(2), (e)(2)(ii).

[175] Geiger, *supra* note 174.

[176] *See* Joseph Conn, *Data Encryption Just One Option Under Security Law*, MODERNHEALTHCARE.COM, (May 12, 2009, 11:00 AM), http://www.modernhealthcare.com/article/20090512/NEWS/305129979 (explaining some of the different levels of encryption in HIPAA, such as de-identified records compared to records with limited data sets). Encryption can be an important defense against improper access. Brian T. Horowitz, *Health Care IT: Securing Health Care Information: 10 Ways to Defend Against Data Breaches*, EWEEK.COM (Aug. 14, 2012), http://www.eweek.com/c/a/Health-Care-IT/Securing-Health-Care-Information-10-Ways-to-Defend-Against-Data-Breaches-762368/?kc=rss.

innovation.[177] Limits on access and reuse reflect valid concerns: as endless stories of breaches and new data uses proliferate, data subjects need more robust assurances about controlled data dissemination.[178] As databases proliferate, the risk of re-identification of de-identified data through the use of information from multiple publicly-available sources increases, so that fewer data points are necessary to personally identify the subject of the data. Whatever rules govern the emerging infrastructure of health data surveillance and sharing, they will need to be complemented by monitoring that seeks to detect and deter inappropriate uses of information.[179] Part IV below proposes some methods of making that monitoring more effective, such as the funding of technologists (such as the technologists funded by the FTC to help that agency develop better mobile privacy policies) and the deployment of contingency-funded contractors (such as the Recovery Audit Contractors (RACs) already deployed by CMS to detect and deter fraud and abuse) —and perhaps even, in an era of big data, the types of de-identified data that may eventually be re-identified.[180]

3. Marketing, Sale, and the Vagaries of Consent

The Omnibus HIPAA Rule has helped clarify the obligations of CEs who want to engage in sale, marketing, or research uses of protected health information.[181] For marketing, a CE needs to obtain a patient's authorization if it receives financial remuneration in exchange for communicating about a health-related product or service.[182] Before the communication can be made, the authorization must include the disclosure that the covered entity or business associate is receiving financial remuneration from a third party for making the communication. There do appear to be important exceptions, though. For example, communications about a drug or

---

[177] Barbara Evans, *Ethical and Privacy Issues in Pharmacogenomic Research*, *in* PHARMACOGENOMICS: APPLICATIONS TO PATIENT CARE 325 (Howard L. McLeod *et al.* eds., 2d ed. 2009).

[178] U.S. DEP'T. OF HEALTH & HUMAN SERVS. OFFICE FOR CIVIL RIGHTS, ANNUAL REPORT TO CONGRESS ON BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION 1, 9-10 (2009-10), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf.

[179] *See generally* Evans, *supra* note 177, at 313-38 (discussing the concerns and solutions regarding data flow).

[180] For recent analyses of the re-identification issue, *see* Felix Wu, *Privacy and Utility in Data Sets*, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031808 (Aug. 15, 2012); OCR, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[181] 45 C.F.R. § 164.502(a)(5)(ii)(B)(1) covers the "sale of PHI," which is a disclosure of PHI when the covered entity receives direct or indirect "remuneration from or on behalf of the recipient of the PHI in exchange for the PHI." The Omnibus HIPAA Rule addressed marketing, research, fundraising, and sale of protected health information.

[182] Financial remuneration is defined as "direct or indirect payment from or on behalf of a third party whose product or service is being described." 45 C.F.R. § 164.501. It appears that nonfinancial or in-kind consideration for such communication is not covered by the marketing rule. *See* Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5596 (confirming "that the term 'financial remuneration' does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service"); *id.* at 5597 (noting "that non-financial or in-kind remuneration may be received by the covered entity or its business associate and it would not implicate the new marketing restrictions").

biologic presently prescribed for a patient can be marketed if the payment is "reasonable." For sale of PHI, there is a prohibition, but there are multiple exceptions to that prohibition.[183]

One key question raised here is how the consent and authorization for the use or disclosure of PHI for marketing and sales purposes are to be arranged.[184] A scope of authorization for subsidized communications can be broader than for merely a "single product or service or the products or services of one third party."[185] The preamble to the Omnibus HIPAA Rule notes that the new authorization rules "provide covered entities with a more uniform system for treating all remunerated communications."[186] Furthermore, "where an individual signs an authorization to receive such communications, the covered entity may use and disclose the individual's protected health information for the purposes of making such communications unless or until the individual revokes the authorization pursuant to § 164.508(a)(5)."[187] Such statements suggest an intent to streamline authorization requests, and models of consent that are more blanket than specific.

On the other hand, Marla Durben Hirsch has argued that "use of 'free' EHRs may violate" the Omnibus HIPAA Rule because of the complexity of consent required to assure genuine acceptance and understanding of the business and treatment relationships they imply. Having observed that "[p]hysicians using cloud-based electronic health records should expect to see more pop-up and other types of advertisements from pharmaceutical and medical device manufacturers,"[188] Hirsch cautions that they may require onerously specific consent.[189] An

---

[183] These include exceptions for the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence purposes if the recipient of the PHI is or will become a Covered Entity following the sale, transfer or merger, and for research purposes. Posinelli Shughart, PC, *Uses and Disclosures of PHI under the Final Rule: Changes Related to Marketing, Research, Fundraising and the Sale of Protected Health Information and Other Significant Changes* (Feb. 2013), *available at* http://www.jdsupra.com/legalnews/uses-and-disclosures-of-phi-under-the-fi-55749/.

[184] 45 C.F.R. § 164.508(a)(3). Note that HHS's generosity toward research uses of health information may lead to some regulatory arbitrage, as entities might recharacterize information gathering as research. 45 C.F.R. §164.508(b)(3)(iii) allows for compound authorizations for research, reversing an earlier policy that required study-specific authorizations. Rachel Grunberger, *HITECH Update #4: HHS Relaxes HIPAA Requirements for Research Authorizations*, COVINGTON & BURLING LLP, INSIDE PRIVACY (Jan. 20, 2013), http://www.insideprivacy.com/health-privacy/hitech-update-4-hhs-relaxes-hipaa-requirements-for-research-authorizations/.

[185] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5566, 5596.

[186] *Id*.

[187] *Id*.

[188] Marla Durben Hirsch, *EHRs the Latest Advertising Billboard for Manufacturers* (Jan. 23, 2013), http://www.fierceemr.com/story/ehrs-latest-advertising-billboard-manufacturers/2013-01-23.

[189] Marla Durben Hirsch, *Use of 'Free' EHRs May Violate New HIPAA Rule*, http://www.fierceemr.com/story/use-free-ehrs-may-violate-new-hipaa-megarule/2013-01-29 ("[HIPAA now] requires providers to obtain patient authorizations 'for all treatment and healthcare operations communications where the covered entity receives financial remuneration for making the communications for a third party whose product or service is being marketed.' . . . The megarule doesn't specifically address pop up ads in EHRs. But the purpose of the ads is to market their products to physicians with the hope that they will prescribe, promote or sell them to patients. That sounds just like the marketing that the megarule is addressing. If the physician then 'communicates' the product or service in the ad without having patient authorization to do so, the physician is in violation of HIPAA.").

insightful commentator observes that entirely ad-based EHR business models may not run afoul of marketing restrictions, but could be violating rules on sales of data if "the free EHR is provided to the CE 'primarily' in exchange for the PHI to be entered into the EHR."[190] The faint distinctions between some uses of PHI for marketing and sales purposes (and potential regulatory arbitrage via mere "access" to data) merit further guidance.

There is a tension between guidance cautioning that authorization be clear and prominent, and cost-containment pressures that will demand streamlining of authorization procedures. Perhaps the ideal solution will involve more granular and technically sophisticated consent procedures, made possible by advances in computing.[191]

Such efforts will take place in the shadow of a growing First Amendment jurisprudence protecting data flows. There is already a vast and growing literature on the use of observational data to promote medical research.[192] All involved understand undue restriction of information flows may impede innovation and undermine public health.[193] But the commercial use of data to market drugs and other interventions has not been adequately addressed by academics or governmental entities. And even as they do move on this front, the Supreme Court's decision in *Sorrell v. IMS Health Inc.* has hemmed in positive action somewhat by protecting certain sales of information (albeit largely de-identified) as protected by the First Amendment. That decision

---

[190] David Harlow, commenting at http://www.fierceemr.com/story/use-free-ehrs-may-violate-new-hipaa-megarule/2013-01-29 ("It appears to me that the marketing rule would be implicated only if there were a direct or indirect payment of money . . . . In-kind remuneration (e.g., provision of a free EHR) is excluded from the definition. [But] [t]he free EHR may implicate other sections of the rule . . . The limitation on sale of PHI . . . includes direct and indirect remuneration [whereas the limitation on marketing focuses on financial remuneration]. The commentary to the rule says that 'a sale of protected health information occurs when the covered entity primarily is being compensated to supply data it maintains in its role as a covered entity (or business associate). Thus, such disclosures require the individual's authorization unless they otherwise fall within an exception at § 164.502(a)(5)(ii)(B)(2).' 78 Fed. Reg 5606. Those exceptions are, essentially: (i) for public health purposes, (ii) for research, so long as payment is limited to the sending CE's costs, (iii) for treatment and payment, (iv) in connection with a sale or merger of the CE, (v) to or by a BA where the CE is just paying for the BA's services, (vi) to a patient who requests access to his or her own PHI, (vii) as required by law or (viii) as otherwise permitted under HIPAA where the remuneration covers costs only. None of these exceptions seems to apply.").

[191] P. Mork, *et al.*, *Architectures and Processes for Nationwide Patient-Centric Consent Management* (2011); Center for Transforming Health/MITRE Corp., *Meaningful Choice: Enabling Patients to Selectively Manage Access to Their Health Records* (2011) ("MITRE's research allows the patient to express their desired level of granular control; it is then up to the record holder (such as the hospital) to request the current preferences and then use them to package the records for the information exchange."); Arnon Rosenthal, Digital Policies for Patient Consents: The Thorny (and General) Technical Challenges, MITRE Corp. (2011) ("Our project is architecting and prototyping key elements of a system to elicit and manage consents. All of a patient's consent rules are to be managed in one place, editable over the web, and accessible by authorized record holders.").

[192] Inst. of Med., BEYOND THE HIPAA PRIVACY RULE 141 (2009) ("observational studies play in increasingly critical role" in research).

[193] Clayton Christensen, THE INNOVATOR'S PRESCRIPTION 14 (2007) (integrated information systems may be able to condense some medical research into a matter of weeks or months, rather than the years that are customary now).

struck down a Vermont law limiting data flows, despite documented concerns about the interaction between, say, doctors and pharmacies in the brave new world of health informatics.[194]

4. Are Non-Covered Entities Creating Medical Reputations?

Assume, for now, that all the issues raised above are adequately addressed by regulators and stakeholders. Individuals would still be right to worry that their *medical reputations*—if not their medical records—are being created in processes which they can barely control or understand. As Nicolas Terry has explained, judgments about individuals' health status do not need to be based on medical records:

> The health care sector and its stakeholders constitute an area considerably larger than the HIPAA-regulated zone. As a result, some traditional health information circulates in what may be termed a HIPAA-free zone. Further, the very concept of health sector specific regulation is flawed because health related or medically inflected data frequently circulates outside of the traditionally recognized health care sector. In both cases agreed-upon health privacy exceptionalism is jeopardized.[195]

In an era of Big Data, companies do not even need to consult the "health care sector" to impute various medical conditions or disabilities to data subjects. Consider, for instance, Charles Duhigg's reporting on data mining by Target: the company prides itself on knowing whether customers are pregnant.[196] ProPublica has documented data brokers' interest in health-inflected data:

> Data companies can capture information about your "interests" in certain health conditions based on what you buy — or what you search for online. Datalogix has lists of people classified as "allergy sufferers" and "dieters." Acxiom sells data on whether an individual has an "online search propensity" for a certain "ailment or prescription."[197]

According to FTC Commissioner Julie Brill, "One firm, LeadsPlease.com, reportedly sells the names, mailing addresses, and medication lists of people with diseases like cancer or clinical

---

[194] *CVS Privacy Practices Need Investigation Despite FTC Order, Pharmacist Group Says*, 18 Health L. Rep. 397 (BNA) (March 2009).

[195] Nicolas Terry, *Protecting Patient Privacy in the Age of Big Data* (Sept. 27, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153269.

[196] Charles Duhigg, *How Companies Learn Your Secrets*, THE N.Y. TIMES MAGAZINE (Feb. 16, 2012), *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[197] Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA, Mar. 7, 2013, http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

depression. Another data broker, ALC Data, reportedly offers lists of consumers, their credit scores, and their specific ailments."[198]

It is clear that healthcare companies are also developing an interest in cognate data.[199] Consider all the sources that could collect such data:

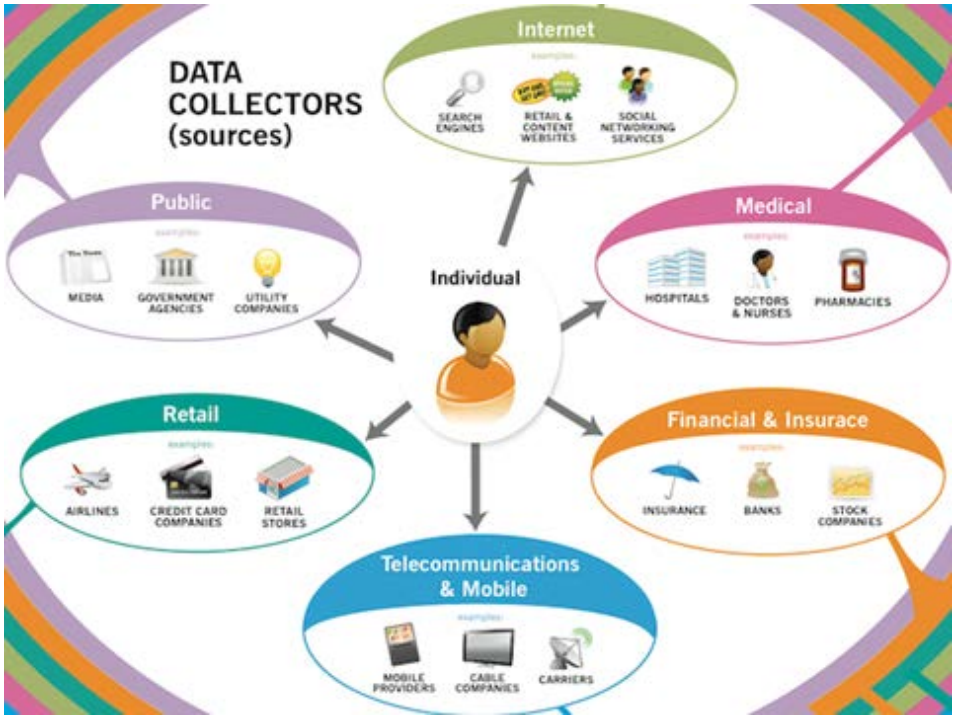

Image Credit: Federal Trade Commission.

And how far data brokers could go to combine and recombine those sources:

[198] Julie Brill, *Reclaim Your Name*, Keynote Address at Computers, Freedom, and Privacy Conference, June 26, 2013, at http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

[199] *Id.* ("One health insurance company recently bought data on more than three million people's consumer purchases in order to flag health-related actions, like purchasing plus-sized clothing, the Wall Street Journal reported. (The company bought purchasing information for current plan members, not as part of screening people for potential coverage.)").

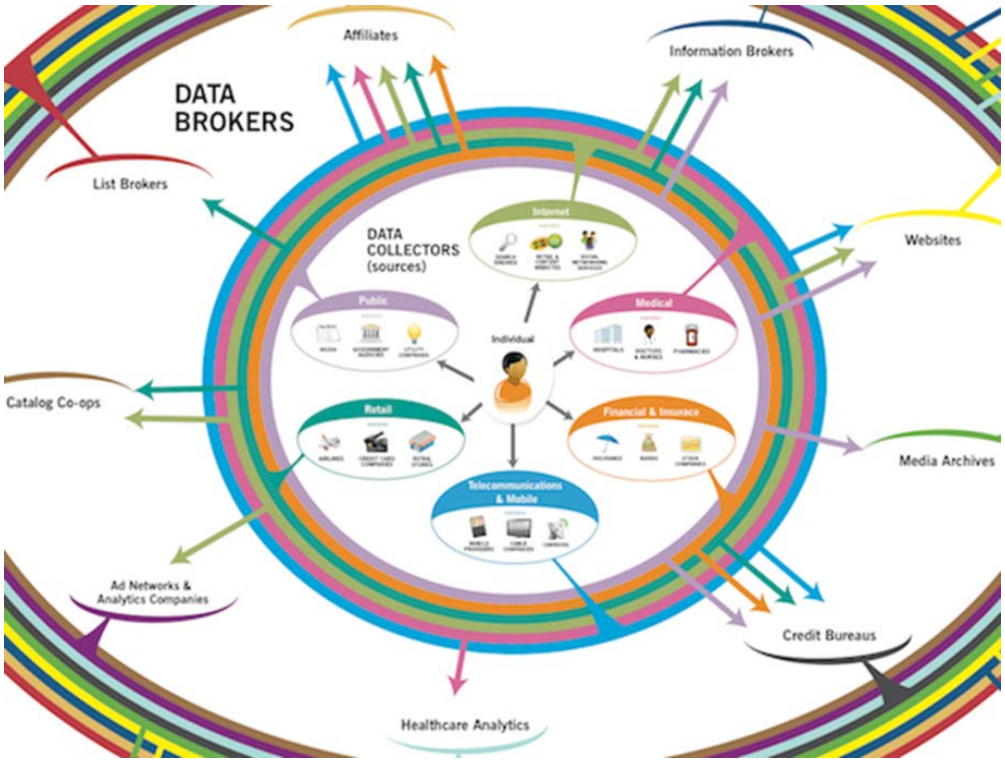

Image Credit: Federal Trade Commission.

Social networks have also intensified the surveillance of health-inflected data. But these platform providers enjoy a largely deregulated online environment. As social networks organized around personal health records like PatientsLikeMe provide novel and powerful opportunities to address health issues and to form communities, they also open the door to frightening and manipulative uses of data by firms and governments, employers, and ranking intermediaries.[200]

Social network profiles are sometimes less accessible than search engine results, thanks to passwords and privacy settings. But many users never take steps to keep their profile private, and data miners have already logged details of profiles. Facebook can suddenly reset defaults, causing what James Grimmelmann calls "privacy lurches" to unexpectedly expose aspects of profiles that users once thought were only visible to themselves and friends. Many users fail to change the default settings, effectively making that part of their life online an "open book."

[200] A company called Acxiom has 1,600 pieces of information about 98% of United States adults, gathered from thousands of sources. ELI PARISER, THE FILTER BUBBLE 3 (2011). At least some of them are health-indicative or health-predictive. Such information will only be more valuable to employers as self-insured health plans become more common. DAN SOLOVE, THE FUTURE OF REPUTATION (2009); Natasha Singer, *You for Sale: Mapping the Consumer Genome*, THE N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all.

Moreover, lacking "visceral notice" of the accessibility of their profiles, many users explicitly or implicitly assume that only their friends are seeing it (since they are usually the only group able to comment on postings). Very few take the basic privacy step of logging out and then trying to access their own account via another, "dummy" account, to see the picture of themselves that they are broadcasting to the world at large.

What Daniel J. Solove has called the "digital person" has real consequences for the data subject it is connected to, however unaware the latter may be of the former. According to a 2009 survey, 35% of employers have decided not to hire someone on the basis of content on the applicant's social media site.[201] Of those who did so, 44% found the candidate's mention of alcohol or drug use a "no-go" — and who is to know what types of inferences about health status they may have derived from such information.[202] There are also legitimate worries about discriminatory uses of information either not covered by extant privacy or anti-discrimination laws or undetectable by workers.[203]

Efforts to assure the fairness and accuracy of such reputation-affecting information have not caught up to technological advances in producing it. For example, an investigating office may tailor its software to assure that the most damaging information available about a person (from its perspective) comes up first in whatever databases it queries.[204] The applicant would need to use the same personalizing software to be fully aware of all the negative information such a search was generating. Yet trade secrecy and contracts will likely prevent him from ever accessing an exact replica of the programs used by the educators, employers, landlords, bankers, and others making vital decisions about his future. Some digital scarlet letter could be floating in the ether, prominent to those with certain filtering programs, and virtually invisible to others.

The cost of information storage has consistently declined over time, and recent developments suggest even more dramatic advances toward "total recall" by computerized networks.[205] As privacy expert Helen Nissenbaum has observed, "anything about an individual

---

[201] CareerBuilders, *Forty-Five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds* (Aug. 19, 2009), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=8412d5b32ef54ce6854a035cf3a59d12-303995843-x3-6. Sites included not only personal ones, like Facebook, but also LinkedIn.

[202] Another study found that as many as 50% of employers and 77% of job recruiters who have concerns about an applicant's alcohol or drug abuse, violence, or other similar problems will use the Internet to search potential applicants. Richard A. Paul & Lisa Hird Chung, *Brave New Cyberworld: The Employer's Legal Guide to the Interactive Internet*, 24 LAB. LAW. 109, 116 (2008-2009).

[203] Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KAN. J.L. & PUB. POL'Y 409, 422 (2010) (raising the possibility of a growing use of "complex scoring algorithms based on EHRs to determine which individuals are likely to be high-risk and high-cost workers").

[204] For fuller explanation of these technologies, *see* Frank Pasquale, *Reputation Regulation*, in THE OFFENSIVE INTERNET 111 (Martha Nussbaum & Saul Levmore, eds., 2010).

[205] Victor Mayer-Schonberger, DELETE (2009).

that can be rendered in digital form can be stored over indefinitely long periods and be readily retrieved."[206] Joseph Turow's book, *The Daily You*, describes in great detail the kinds of profiles that can result from the endless search for data.[207] Social networks can both generate and use such data to create secret profiles. Those profiles, in turn, may be of interest to far more than advertisers. Police and other officials need little more than a subpoena to review such files.[208] Data brokers are keen to monetize their information trove.

Health-inflected information from entities not covered as either CEs or BAs under HIPAA can be a critical source of correlations, profiles, and attributions. Companies are not shy about using and distributing the information; for example, PatientsLikeMe.com states "you should expect that every piece of information you submit (even if it is not currently displayed) may be shared with our partners and any member of PatientsLikeMe."[209] Users were later shocked to find that "Nielsen Co., [a] media-research firm . . . was 'scraping,' or copying, every single message off PatientsLikeMe's private online forums."[210] Had the virtual break-in not been detected, health attributes connected to usernames (which, in turn, often can be linked to real identities) could have spread into numerous databases.

For those in the individual insurance market, the risk of runaway health data has already been realized. Patients who purchased antidepressants were later denied insurance repeatedly, thanks to a dossier sold to insurers. Consider, for instance, the plight of Walter and Paula Shelton, a Louisiana couple who sought insurance while in their fifties.[211] Paula had taken an antidepressant as a sleep aid, and occasionally used a blood pressure medication to relieve some swelling in her ankles. Humana, a large insurer based in Kentucky, refused to insure the couple based on that prescription history. They were not able to find insurance from other carriers, either.[212] No one had explained to them that a few prescriptions could render them uninsurable.

---

[206] Helen Nissenbaum, PRIVACY IN CONTEXT 36 (2008); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 129 (2004).

[207] Joseph Turow, THE DAILY YOU (2011) (describing online internet advertising markets for data).

[208] Chris Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (Summer 2004).

[209] PatientsLikeMe FAQ, http://www.patientslikeme.com/help/faq/Corporate ("Except for the restricted personal information you entered when registering for the site, you should expect that every piece of information you submit (even if it is not currently displayed) may be shared with our partners and any member of PatientsLikeMe, including other patients.").

[210] Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, THE WALL STREET JOURNAL (Oct. 11, 2010, 9:30 p.m. ET), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html.

[211] Terhune, *supra* note 156 ("Two-thirds of all health insurers are using prescription data--not only to deny coverage to individuals and families but also to charge some customers higher premiums or exclude certain medical conditions from policies, according to agents and others in the industry.").

[212] Uninsured people like the Sheltons can count on some help from the Affordable Care Act, the landmark legislation passed in 2010. That law will require insurers to guarantee issue of policies. They can still charge people in their 50s three times as much as they charge those in their 20s, but those with a prescription history will not have to worry about flat rejections. PPACA sec. 1201(4), § 2702(a)–(b)(1), 42 U.S.C.A. § 300gg-1(a)–(b)(1) (West Supp. 1A 2010) (requiring acceptance of all applicants, but allowing limitation to certain "open or special

Indeed, the model for blackballing them may still have been a gleam in an entrepreneur's eye when Mrs. Shelton obtained her drugs. It became a big business: prescription-reporting service Intelliscript claimed in 2008 that clients using it reported "financial returns of 5:1, 10:1, even 20:1."

According to *BusinessWeek*'s Chad Terhune, who first reported on the Sheltons, use of prescription data has been widespread in the individual insurance market.[213] Insurers tailored policies to exclude pre-existing conditions, or to charge some members more. Companies like MedPoint and Intelliscript gathered millions of records from pharmacies, avoiding privacy restrictions on hospital and physician records.[214] They then sold them on to insurers eager to gain a competitive advantage by avoiding the sick. Since 1% of patients account for over one fifth of healthcare costs, and 5% account for nearly half of costs, an insurer who can "cherry pick" the healthy and "lemon drop" the sick will be far more profitable than those who take all comers.[215] Even though PPACA's guaranteed issue provisions and exchanges will help deter such underwriting practices, it is by no means clear that health reform can address all the varied ways in which insurers can try to shift high-risk individuals to undesirable plans, or self-insured employers can adopt pretextual tactics to drive them away as employees.

The FTC is supposed to deter "unfair and deceptive" trade practices, particularly those that can harm consumer reputations. The FTC determined that MedPoint and Intelliscript had violated the law by keeping their systems secret from consumers. But the agency imposed no penalties, and its judgment against them barely put a dent in their business practices. The FTC merely required that the prescription data brokers tell consumers if their file caused a denial of coverage or other adverse action. There is no privacy here, just a chance at ensuring accuracy: all the consumer can do in response is review the record and try to correct it if it is wrong.[216]

---

enrollment" periods); PPACA sec. 1201, § 2701(a)(1)(A), 42 U.S.C.A. § 300gg(a)(1)(A) (permitting 3 to 1 age-based pricing differentials). They will, however, want to think about how data brokers' other forms of categorization may inform other, subtler forms of risk selection by employers and insurers.

[213] Terhune, *supra* note 156.

[214] Intelliscript Complaint, http://www.ftc.gov/os/caselist/0623189/080212complaint.pdf. Less harmful uses of the information may also be troubling to consumers, or may end up going beyond their original purposes. See, for instance, concerns raised in Weld v. CVS Pharmacy (pharmacy sold names and contact information of customers to allow a direct marketer to target customers with specific medical conditions).

[215] Statistics are from the Agency for HealthCare Research and Quality, or AHRQ.

[216] Agreement Containing Consent Order (Milliman/Intelliscript), *available at* http://www.ftc.gov/os/caselist/0623189/2070917agree0623189.pdf; Decision and Order (Milliman/Intelliscript), http://www.ftc.gov/os/caselist/0623189/080212do.pdf; Analysis of Proposed Consent Order to Aid Public Comment, http://www.ftc.gov/os/caselist/0623189/2070917analysis0623189.pdf; Notice in Federal Register, http://www.ftc.gov/os/fedreg/2007/september/070928milliman.pdf; Intelliscript Complaint, http://www.ftc.gov/os/caselist/0623189/080212complaint.pdf; Medpoint Agreement Containing Consent Order, http://www.ftc.gov/os/caselist/0623190/070917agree0623190.pdf.

Meanwhile, data brokers quietly continue gathering information, and making predictions based on it.[217] MedPoint and Intelliscript developed methods of estimating the likely cost of claims of an insured person, expressed as a numerical score. That opinion could be very valuable to lenders, employers, and just about any other entity with a stake in a person's future. But the companies are under no obligation to disclose how it is computed. It is numbers like these, and concomitant risk assessments and denials of opportunity that will matter to the 21st century health data subject just as much as opportunities to track and understand health data flows.

For about half of American workers, their employers bear some direct financial risk should they become ill.[218] Whatever their ethical commitments, data-driven managers will be forced by market demands to try to avoid the productivity drag of a sick or otherwise impaired workforce, unless very strong laws and enforcement penalties deter such behavior. Sharona Hoffman has predicted the growing use of "complex scoring algorithms based on electronic health records to determine which individuals are likely to be high-risk and high-cost workers."[219] These methods are already used in life insurance.[220] Moreover, companies can skip covered health records altogether and use other medically inflected data to predict an employee's overall vitality or productivity. For example, a wide waist, or multiple visits to the Coca Cola websites, could reflect a predisposition to diabetes. While anti-discrimination laws militate against decisions based on such data, it is increasingly difficult for those affected to understand (let alone prove) how health-inflected data affected decision-making about them.

This is in part because the amount of data gathered by third and fourth party entities is immense; the inferences they enable are even more staggering. Data miners need not ask a person directly about clothing sizes; they might merely keep track of whether he visits a "big &

---

[217] Sarah Ludington, *supra* note 156, at 162. There are also legitimate worries about discriminatory uses of information either not covered by extant privacy or anti-discrimination laws, or undetectable by workers. Hoffman, *Employing E-Health*, *supra* note 203, 422 (raising the possibility of a growing use of "complex scoring algorithms based on EHRs to determine which individuals are likely to be high-risk and high-cost workers.").

[218] As Ann Marie Marciarille observes, "an estimated 59% of private sector workers with health coverage are enrolled in self-insured plans (up from 41% in 1998)." Marciarille, *Self-Insurance Among Small Employers Under the ACA*, Missouri State of Mind, at http://delong.typepad.com/annmariemarciarille/2013/02/self-insurance-by-small-employers-under-the-aca.html, Feb. 18, 2013. Self-insured status has become popular for many reasons; for example, the self-insured employer can more easily avoid state insurance regulation because of ERISA preemption. Furrow *et al.*, HEALTH LAW (Rev. 6th Ed., 2008). Though many of these companies buy stop-loss insurance to mitigate their own risks, even if they are very well-insured in that respect, productivity losses due to illness (and particularly chronic illness) are well-documented.

[219] Hoffman, *Employing E-Health*, *supra* note 156, at 422.

[220] Frank Pasquale, *Online Health Data in Employers' and Insurers' Predictive Analytics*, CONCURRING OPINIONS, Nov. 19, 2010, http://www.concurringopinions.com/archives/2010/11/online-health-data-in-employers-and-insurers-predictive-analytics.html ("Did you know that buying generics instead of brands could hurt your credit? Or that a subscription to *Hang Gliding Monthly* could scare off life insurers? Or that certain employers' access to electronic health records could lead them to classify you as "high-risk" or "high-cost"?").

tall" clothing store, on- or offline.[221] So many online activities have some implications about a person's health status that access to medical records is not necessary to construct a medical reputation.[222] Harvest enough data about the food consumers buy, how often they go to the gym, the size of their clothing, their educational attainment and interests, and "big data" mavens will be happy to predict their likely health outcomes.

After the FTC's intervention, consumers should be able to locate and correct errant pharmacy record files now. But consumer protection agencies have nowhere near the staff they would need to monitor all companies trafficking in reputational data. Unattributed data sources are used to make critical judgments about individuals.[223]

IV. Recommendations

A. Increasing Business Associate Compliance: Mandatory Business Associate Agreement Terms, Education, and Increased Enforcement

Although the Omnibus HIPAA Rule gives teeth to HIPAA by extending liability down the chain, many cloud service providers seem unwilling or unable to accept the implications of HHS's enforcement authority. This issue should be a priority for regulators, particularly as they implement audits for CEs and BAs,[224] and consider expanding the program.[225]

A chorus of legal advisories agrees that the Omnibus HIPAA Rule reaches many cloud service providers. David Holtzman of OCR's Health Information Privacy Division, for example, has warned CEs, "'If you use a cloud service, it should be your business associate. If they refuse

---

[221] *See* Duhigg, *supra* note 196 ("Almost every major retailer, from grocery chains to investment banks to the U.S. Postal Service, has a "predictive analytics" department devoted to understanding not just consumers' shopping habits but also their personal habits, so as to more efficiently market to them.").

[222] Just as life insurers dig into subscription records to find out if an applicant subscribes to *Hang Gliding Monthly* or *Cigar Aficionado*, employers are going to want to know more intimate details of employees' lives, especially as the cost of data and its analysis declines.

[223] Frank Pasquale, THE BLACK BOX SOCIETY: TECHNOLOGIES OF REPUTATION, SEARCH, AND FINANCE (under contract with Harvard University Press; forthcoming, 2014).

[224] Audit authority is described at 42 U.S.C. § 17940 (2009) ("The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements"). To monitor covered entities to assure they are complying by HIPAA requirements, OCR launched an audit program in November 2011 as part of its health information privacy and security compliance program.

[225] Business associates were "immune from audit selection during the 2012 pilot phase, but this is expected to change should OCR expand the program in 2013, as HITECH explicitly subjects business associates to the HIPAA audits as well." Richard B. Wagner, *Early Results from New HIPAA Audit Pilot Reveal Emphasis on Policy Documentation and Business Associate Agreements*, ABA HEALTH eSOURCE, May, 2012, *available at* http://www.americanbar.org/newsletter/publications/aba_health_esource_home/aba_health_law_esource_0512_wagner.html.

to sign a business associate agreement, don't use the cloud service."[226] Advice abounds as to what BAAs with cloud service providers should include to minimize risks of HIPAA liability and ensure HIPAA compliance, such as elements to permit a risk assessment and risk management process.[227]

Yet some of the most powerful cloud service providers refuse to execute BAAs with CEs or BAs. Amazon, for example, reportedly has "taken the position that it is not required to sign BAAs with companies that run HIPAA applications and/or permanently store PHI on [Amazon Web Services]."[228] Art Gross has represented that cloud service providers Google, Yahoo, and AOL are not willing to sign a BAA with a CE.[229] There are reports that many cloud service

[226] Spencer & Wagner, *supra* note 145; *see also* Art Gross, *HIPAA Omnibus and Microsoft Office 365* (Feb. 16, 2013), http://www.hipaasecurenow.com/index.php/hipaa-omnibus-and-microsoft-office-365/ ("If the CE is using Cloud Providers such as Google, Yahoo or AOL and they are sending PHI, then the Cloud Provider would be considered a HIPAA Business Associate. As a Business Associate, each of the Cloud Providers would be required to sign a HIPAA Business Associate Agreement (BAA) with the CE."); Bianchi *et al.*, *supra* note 57 ("OCR has made it clear that cloud vendors are business associates, even if they do not access PHI. This analysis is important as cloud-based solutions become more widespread in the health care industry."); *Attorney: HIPAA Rules Change Game for Cloud Companies*, HEALTH DATA MANAGEMENT (March 21, 2013), http://www.healthdatamanagement.com/issues/21_3/Attorney-HIPAA-Rules-Change-Game-for-Cloud-Companies-45749-1.html ("Many cloud companies have taken the view that they are not business associates under HIPAA, but some of them now will be . . . . [A] company that maintains data is a BA even if it doesn't access the data. I think that will have implications for the cloud industry.") (quoting Robert Belfort, partner in the health care practice at law firm Manatt, Phelps & Phillips).

[227] *See, e.g.*, Spencer & Wagner, *supra* note 145 (itemizing what, at minimum, a HIPAA-compliant BAA between a CE and cloud computing entity should include "to obtain[] the operational and cost efficiencies of cloud computing, but, to help avoid the risk of a costly HIPAA violation"); Alex Ruoff, BNA Health IT Law & Industry Report, *Data Security Should Be High Priority For Cloud Storage Users, White Paper Says* (Jan. 7, 2013) (identifying elements of a proper risk assessment and risk management process what should be addressed when entering a BAA with a cloud vendor to mitigate liability, as outlined in a white paper by Foley & Lardner LLP); Alex Ruoff, BNA Health IT Law & Industry Report, *OCR Could Include Cloud Provision In Forthcoming Omnibus HIPAA Rule* (Jan. 7, 2013) (describing call for guidance from Deborah Peel, founder of Patient Privacy Rights, "that highlights the lessons learned from the Phoenix Cardiac Surgery case while making clear that HIPAA does not prevent providers from moving to the cloud," including "request for technical safeguards for cloud computing solutions, such as risk assessments of and auditing controls for cloud-based health information technologies; security standards that establish the use and disclosure of individually identifiable information stored on clouds; and requirements for cloud solution providers and covered entities to enter into a business associate agreement outlining the terms of use for health information managed by the cloud provider"); Reece Hirsch, BNA Health IT Law & Industry Report, *What Every General Counsel Should Know About Privacy and Security: 10 Trends for 2013* (Feb. 25, 2013) (summarizing opinion 05/2012, guidance on cloud computing from the European Union Article 29 Working Group, advising "cloud customers to maximize oversight of cloud arrangements, recommending that cloud customers conduct a comprehensive data protection risk assessment before selecting a cloud provider . . . [and identifying] 14 specific issues that cloud customers should address in cloud service agreements").

[228] rudi2001, Amazon Web Services Discussion Forums, *HIPAA BAA Agreement, Omnibus Rules New As of Jan 2013* (Feb. 6, 2013), https://forums.aws.amazon.com/thread.jspa?messageID=428426.

[229] Gross, *supra* note 226; *see also* Leyva, *supra* note 71 (noting that even though Google would be a business associate if a CE or BA uses a tool like Google Apps to store PHI, it is unlikely a company like Google would enter into the contract now required by the Omnibus HIPAA Rule).

providers do not believe that they are bound by HIPAA.[230] Others may feel free to ignore HIPAA's commands because enforcement seems unlikely.[231]

When cloud service providers do enter contracts with CEs or BAs, they often use their disproportionate bargaining power to insist that their customers "enter into standard, non-negotiable agreements," particularly with "low value contracts and community cloud contracts."[232] One attorney who provides legal advice to a Fortune 100 company said that cloud service providers refuse to negotiate the terms of a BAA. At best they might offer to share the results of a third party audit. But such audits do not excuse the CE or BA from complying with HIPAA's written contract requirement.[233]

It is possible that the liability provisions in the Omnibus HIPAA Rule will convince resistant cloud service providers to rethink their position on BAAs since they bear direct and potential agency liability for subcontractor BAs under the Rule.[234] For example, after radio silence for three weeks, Amazon on February 27, 2013 finally responded to a customer's web forum inquiry about whether it was reconsidering its refusal to sign BAAs, in light of the Omnibus HIPAA Rule, responding that Amazon is "in the process of considering the impact of

[230] *See, e.g.*, Belfort *et al.*, *supra* note 69 (noting that HHS's interpretation that vendors maintaining PHI are BAs even when they do not require routine access to PHI appears "to impose HIPAA requirements on certain cloud computing companies and other data storage vendors that previously took the position they were not business associates"); Patrick Ouellette, *HIPAA Omnibus Responsibility Focus Shift: Legal Q&A* (Jan. 22, 2013), http://healthitsecurity.com/2013/01/22/hipaa-omnibus-responsibility-focus-shift-legal-qa/ ("Every subcontractor involved is going to have HIPAA Security Rule obligations and some of them may not even know it."); Plank, *Enforcement, Compliance*, *supra* note 145 ("But some attorneys have worried that subcontractors, who do work involving protected health information, will not realize they are now covered."); Steve Swann, Anitian Blog, *Analysis of the HIPAA Omnibus Rule* (Feb. 12, 2013), http://blog.anitian.com/?p=348 ("This means a lot of companies who do not think HIPAA applies to them, are now required to be HIPAA compliant.").

[231] Of course, as discussed below, not all cloud providers refuse to execute BAAs. Some understand and are willing to comply with HIPAA's requirements, including the requirement to sign a BAA. Melissa Markey observes that these cloud providers, which typically qualify for federal government contracts, tend to be more expensive, but they are "much cheaper than a breach response." Notes from Melissa Markey, Esq. (on file with authors).

[232] Classen, *supra* note 7, at 21.

[233] U.S. Department of Health & Human Services, Health Information Privacy: FAQ (created Dec. 19, 2002; last updated Mar. 14, 2006), http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/237.html ("Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule? Answer: No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at 45 CFR 164.504(e)"); *see also* David Kidd, *What Does It Take to Be HIPAA-Compliant in the Cloud?*, THE DATA CENTER JOURNAL (Feb. 25, 2013), http://www.datacenterjournal.com/it/hipaacompliant-cloud/ ("Many technology companies are announcing the availability of their HIPAA-compliant cloud solutions, and it is important for health-care companies to understand what such a solution entrails [sic]. Employing these solutions does not mean the customer is no longer responsible for meeting specific HIPAA requirements for their applications, data and IT infrastructure. In fact, some HIPAA requirements will always be the sole responsibility of the customer, not the cloud provider.").

[234] *See* Proskauer, *supra* note 131; Plank, *Enforcement, Compliance*, *supra* note 145.

[the Omnibus] rule to AWS."[235] One commenter noted that "[t]his is the single show-stopping item that is preventing my company from moving all our infrastructure to AWS."[236]

While Amazon is considering its position, it has been reported that Microsoft will sign a BAA with a CE that uses the Microsoft Office 365 platform, "a cloud solution that provides email, instant messaging, calendaring, file and data storage, etc."[237] Perhaps this is evidence that the market is reacting to the liability risks made plain by the Omnibus HIPAA Rule. If Microsoft starts signing BAAs, this is sure to put pressure on the market.[238] Another commenter on Amazon's Web Service discussion board posted that he was pursuing alternatives with a competitor who would enter a BAA with it because it has "a responsibility to remain compliant."[239] Another posted a link to Azure, whom it claimed was issuing BAAs. [240] These reports suggest that perhaps some of the negotiation imbalance may be starting to self-correct.

HHS should consider how it can help this evolution progress. Recognizing that cloud service providers often have a bargaining advantage vis-à-vis CEs or BAs, HHS could require that BAAs contain certain terms that some cloud service providers to date have resisted but that will enable CEs and BAs to evaluate whether cloud vendors are complying with HIPAA. For example, HHS could consider requiring BAAs to include certain security provisions, such as requiring cloud vendors to provide an audit certification that complies with the Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC), Type II, or an equivalent audit;[241] a summary of the vendor's security plan; a summary of the disaster response and continuity of operations plan; an executive summary of a risk assessment performed at least annually and potentially whenever there are significant changes to the computing environment and/or there are new threats or vulnerabilities identified; and access for the security officer of the CE or BA to speak to the security officer of the cloud vendor.[242] HHS also could consider when it may be appropriate to require cloud vendors to grant access to its data center so the CE or upstream BA may examine the vendor's physical security. Although it may go too far to require cloud vendors to permit CEs or upstream BAs to conduct remote scans of the cloud's system, another option is to require the cloud vendor to agree to share a high level

[235] rudi2001, Amazon Web Services Discussion Forums, *supra* note 228; AWS is Amazon's could computing service.
[236] *Id.*
[237] Gross, *supra* note 226.
[238] *C.f. id.* ("Microsoft has built a very affordable, HIPAA compliant cloud service and is clearly aiming at CEs of all sizes. It will be interesting to see how Google, Yahoo and AOL respond. How long Microsoft enjoys the only HIPAA compliant cloud service niche is still left to be seen.").
[239] rudi2001, Amazon Web Services Discussion Forums, *supra* note 228.
[240] *Id.*
[241] For more information about SSAE 16 SOC 2, Type II audits, *see* Markey & Marchak, *supra* note 7, at 25-26. A clean SSAE 16 SOC 2, Type II audit provides a useful indication that the vendor takes seriously its security responsibilities.
[242] *See id.* at 23, 33; Notes from Melissa Markey, Esq. (on file with authors); Notes from Telephone Interview of Melissa Markey, Esq. on May 17, 2013 (on file with authors).

summary of the results of a penetration scan performed by a mutually agreeable, qualified, and authorized pen tester, which would yield similar information regarding the security of the cloud vendor.[243]

HHS also could consider requiring a term in the BAA to apportion liability for HIPAA violations in accordance with each party's responsibility. Several advisories have recommended that parties negotiate indemnification terms,[244] given the exposure to direct and agency liability contemplated by the Omnibus HIPAA Rule. Some vendors maintain that these terms no longer are appropriate because they are directly liable to HHS. But as Melissa Markey, Esq. and Margaret Marchak, Esq. have pointed out, direct liability to HHS does not necessarily mean the CE will not be liable for a breach.[245] If the cloud provider caused the breach, the CE may want "to require the business associate to protect the covered entity from costs and losses due to the failure of the business associate to comply with the agreement."[246] Despite the continued importance of indemnification clauses to cloud contracting, however, some CEs may lack sufficient bargaining power to extract (or may not know to ask for) such a clause from a cloud service provider. A requirement in the BAA for the parties to apportion liability between the parties based on fault arguably would give each party an incentive to comply with HIPAA to avoid liability. Such a clause, however, would not protect the parties from enforcement by HHS because HITECH and the Omnibus HIPAA Rule establish the liability of CEs and BAs.[247]

HHS also can look for ways to educate the CEs and cloud service providers of HIPAA's reach, requirements, and penalties in the hope of increasing compliance. As Stephen Wu, a partner at Cooke Kubrick and Wu LLP, has noted, "If you don't know you're a business associate . . . you might not be taking all the steps you need to comply.'"[248] To this end, HHS' Office of Civil Rights is designing online educational resources to help healthcare organizations and BAs

---

[243] *See* Notes from Melissa Markey, Esq. (on file with authors); Notes from Telephone Interview of Melissa Markey, Esq. on May 17, 2013 (on file with authors); Markey & Marchak, *supra* note 7, at 22-24.

[244] *See, e.g.*, Proskauer, *supra* note 131 (recommending that "both covered entities and business associates should now consider seeking indemnification in their business associate agreements"); Anne Foster *et al.*, *supra* note 138 ("Covered entities are encouraged to shore up their business associate agreements to include indemnification language and consider cyber liability insurance requirements when contracting with business associates.").

[245] Markey & Marchak, *supra* note 7, at 4.

[246] *Id.* Ms. Markey also generally seeks to carve out HIPAA compliance from any limitations of liability in cloud contracts, such as disclaimers of consequential and/or punitive damages. *See* Notes from Telephone Interview of Melissa Markey, Esq. on May 17, 2013 (on file with authors); Notes from Melissa Markey, Esq. (on file with authors).

[247] *See, e.g.*, Spencer & Wagner, *supra* note 145 ("Although the parties can sign agreements and decide which entities will be financially responsible for certain activities, 'you cannot avoid the federal government. Now that business associates are liable under statute, you can't have a contract that says business associates are not liable for anything,' [Joy] Pritts[, chief privacy officer at the HHS Office of the National Coordinator for Health IT,] said. If the federal government 'decides the business associate was the one responsible, they still have the ability to enforce against the business associate,' Pritts said."); Anne Foster *et al.*, *supra* note 138 ("Business associates cannot avoid regulatory liability by refusing to sign a business associate agreement or limiting liability in those agreements.").

[248] Marianne Kolbasuk McGee, *HIPAA Omnibus: The Liability Chain: Expert Explains Compliance* Flow (Feb. 13, 2013), http://www.healthcareinfosecurity.com/interviews/hipaa-omnibus-liability-chain-i-1787.

comply with the Omnibus HIPAA Rule, which OCR intends to release on its web site around March 26, 2013, when the Rule is effective.[249] These resources will include: a breach risk assessment tool to help CEs and BAs assess if notification is required; guidance to help CEs comply with the minimum necessary standard when dealing with BAs and others; compliance tools focused on helping smaller healthcare entities; modified HIPAA training for state attorneys general that CEs may use; and consumer materials, such as YouTube videos and multilingual fact sheets that explain patient rights and other aspects of the Rule.[250] HHS should expand these planned educational efforts by developing educational materials targeted to cloud service providers to help them understand their responsibilities and liability exposure under HIPAA.

HHS also should work to empower CEs and upstream BAs with information about cloud provider liability and resources available to help them evaluate potential vendors from a security standpoint. According to Melissa Markey, CEs do not always appreciate that they have bargaining power and options such that they can walk away from cloud vendors who refuse to execute BAAs or provide any information about their security practices.[251] Ms. Markey and Ms. Marchak reject vendors' defense that they must keep their processes confidential to maintain security, retorting that, "security by obscurity is not a good policy."[252] While some details of the security operations must remain confidential, they believe the security officers from the customer and vendor can share much information without jeopardizing security to "allow the customer to evaluate whether security is reasonable."[253] Education of all parties is critical to have meaningful negotiations.

CMS's deployment of integrity contractors to address problems of errors in payments and claims may provide one model of education toward compliance, if Congress is willing to authorize and provide initial investment in more calibrated interventions to assure compliance. CMS has pioneered innovative deployments of private sector contractors in social welfare programs. It has used "fiscal intermediaries (FIs), carriers, and durable medical equipment regional carriers (DMERCs) to process Part A, Part B, and durable medical equipment (DME) claims for reimbursement" for decades, and Quality Improvement Organizations (QIOs) to assess the value and effectiveness of care offered.[254] The agency has also employed a wide array of contractors to detect and deter improper payments, sometimes funding the contractors with a

[249] *See* McGee, *HIPAA Omnibus Compliance*, *supra* note 133.
[250] *See id.*
[251] *See* Notes from Telephone Interview of Melissa Markey ,Esq. on May 17, 2013 (on file with authors).
[252] Markey & Marchak, *supra* note 7, at 24.
[253] *Id.*
[254] Sara Kay Wheeler *et al.*, *Meet the Fraud Busters: Program Safeguard Contractors and Zone Program Integrity Contractors*, 4 J. HEALTH & LIFE SCI. L. 1 (2011) (citing 42 C.F.R. §§ 421.100 (FIs), 421.200 (carriers), 421.210 (DMERCs), and describing the functions of each)); *see also* CENTERS FOR MEDICARE AND MEDICAID SERVICES, MEDICARE PROGRAM INTEGRITY MANUAL § 1.3.6 (last updated Nov. 20, 2009); 42 C.F.R. § 421.304 (describing the function of Medicare Integrity Program Contractors).

percentage of the improper claims detected.[255] Perhaps HIPAA fines could be deployed in a similar way, to provide a sustainable ecosystem of self-funding to expert entities capable of monitoring a rapidly changing technical landscape.

CMS is committed to "developing new methods and technologies to stay ahead of criminals and identify their patterns of behavior early" and "data analysis to identify cases of suspected fraud, waste and abuse."[256] The Medicare Program Integrity Manual governs Medicare fraud-detection contractors, along with applicable Statements of Work.[257] According to the Manual, comprehensive error rate testing ("CERT") contractors "establish[] error rates and estimates of improper payments."[258] The Recovery Audit Contractors ("RACs") "detect and correct improper payments in the Medicare FFS [fee for service] program and provide information to CMS, [affiliated contractors] ACs and [medicare administrative contractors] MACs."[259] Once these surveillance entities produce data, Medicare Administrative Contractors ["MACs"] can identify program vulnerabilities and develop approaches to respond to wayward providers.[260] Their medical reviews do not have to culminate in charges or prosecutions; rather, "prepayment edits" and provider education are preferred in many situations.[261] These contractors are emerging as sophisticated analysts of data. They engage not only in reactive but

[255] Timothy Martin, *Revenue-Cycle Management and Reimbursement: The Impact of Health Law and Health Reform on Providers*, 4 J. HEALTH & LIFE SCI. L. 159 (2011) (discussing the creation and authorization of contractors and the methods utilized in analyzing claims); *see also* Mark E. Reagan & Mark A. Johnson, *Taming the Medicaid Beast: The Federal Government's Ambitious Attempt to Combat Medicaid Fraud, Waste, and Abuse*, 3 J. HEALTH & LIFE SCI. L. 1 (2010) (explaining "the role and duties of Medicaid Integrity Contractors").

[256] Anatomy of a Fraud Bust: From Investigation to Conviction: Hearing before the S. Comm. on Finance, 112th Cong. (2012) (testimony of Peter Budetti), available at http://www.hhs.gov/asl/testify/2012/04/t20120424a.html.

[257] Centers for Medicare and Medicaid Services, MEDICARE PROGRAM INTEGRITY MANUAL, *supra* note 254, § 1.1 ("Medicare administrative contractors (MACs), comprehensive error rate testing (CERT) contractors, recovery audit contractors (RACs), program safeguard contractor (PSCs) and zone program integrity contractors (ZPICs) shall follow the PIM [Program Integrity Manual] as required by their applicable Statement of Work (SOW).").

[258] *Id* § 1.3.1. ("error rates produced by the CERT program" are used to "identify where to target [] improper payment prevention efforts"). A Fraud Prevention System (FPS) runs "predictive algorithms and other sophisticated analytics nationwide against all Medicare fee-for-service claims . . . prior to payment." *Assessing Medicare and Medicaid Program Integrity: Hearing before the Subcomm. on Gov't Org., Efficiency, & Fin. Mgmt. of the H. Comm. on Oversight & Gov't Reform*, 112th Cong. (2012) (testimony of Peter Budetti), *available at* http://www.hhs.gov/asl/testify/2012/06/t20120607a.html.

[259] CENTERS FOR MEDICARE AND MEDICAID SERVICES, MEDICARE PROGRAM INTEGRITY MANUAL, *supra* note 254, § 1.3.1(C). "[I]t is difficult to prevent all improper payments, considering that more than 1 billion claims are processed each year. *Id.* To address this issue, CMS uses specialized programs to detect and correct improper payments and "provide information to CMS, ACs and MACs that could help protect the Medicare Trust Funds by preventing future improper payments." *Id.*

[260] *Id.* at § 1.3.1.B (Medicare contractors "primarily use error rates produced by the CERT program and vulnerabilities identified through the RAC program to identify where to target their improper payment prevention efforts.").

[261] Medical Appeals Council reviews are designed to spot errors. The Medicare Program Integrity Manual advises contractors that "most errors do not represent fraud. Most errors are not acts that were committed knowingly, willfully, and intentionally." *Id.* § 1.3.9 ("Providers may conduct self-audits to identify coverage and coding errors" using the Office of Inspector General (OIG) Compliance Program Guidelines, which are available at http://www.oig.hhs.gov/compliance/compliance-guidance/index.asp).

proactive efforts to identify problems, combing records for outliers. They can access a wide array of information sources.[262]

Truly assuring the privacy and security of data in the cloud may require intense and fine-grained surveillance. Just as David Ticoll and Don Tapscott predicted in 2003 that "radical transparency" would shake up the business world,[263] CMS's myriad contractors are motivating healthcare providers to modernize their practices.[264] Surveillance "serves as a means, made possible by increasingly effective technologies of recording and preservation, to allow the replaying of the past in the future."[265] Moreover, monitoring and assessment critically involve "assertions of power over what can be seen/recorded/reduced."[266] The mere threat of intense assessment of interventions can increase productivity.[267] Work can be performed more efficiently as it is recorded and studied.[268] New forms of regulation depend on rapid accumulation of data, and auditors should not shy away from benchmarking ideals for continuous quality improvement at cloud service providers.[269]

It may be possible to attribute some of cloud vendors' deafness to HIPAA's requirements to the relatively low number of enforcement actions brought against CEs and BAs. Many penalty actions originate from CEs that self-reported breaches while those who flout the regulatory system remain untouched. This creates a regrettable disincentive for compliance. HHS should exercise its power to conduct audits over cloud service providers to root out noncompliance and hopefully encourage a culture of compliance. Given resource constraints

---

[262] Wheeler *et al.*, *supra* note 254, at 23. ZPICs can access referrals from MACs, QIOs, states' Medicaid fraud control units, state licensing boards, and U.S. Attorney offices; OIG reports; beneficiary complaints; fraud alerts; national claims data from the Health Care Customer Information System; and National Claims Data from CMS Data Center's Part B Analytics. *Id.* Complaints can be filed by virtually any person with "direct and independent information of the fraud," including compliance officers, employees (both current and former), technologists, auditors, accountants, consultants, and salespersons. *Id.*

[263] David Ticoll & Don Tapscott, THE NAKED CORPORATION: HOW THE AGE OF TRANSPARENCY WILL REVOLUTIONIZE BUSINESS 5 (2003) (describing openness as a business imperative).

[264] The Recovery Audit Contractor Program was created by the Medicare Modernization Act of 2003 to recover Medicare overpayments under fee-for-service Medicare Plans. In 2006, the Tax Relief and Health Care Act of 2006 made the program permanent, and required implementation in all states by 2010. During the demonstration program that ran from 2005 to 2008, the RAC program had identified approximately $992.7 million of improper overpayments for CMS. As the authority, functions, and objectives of contractors differ, providers are advised to "develop unique plans for communicating and interacting with each contractor to minimize the risk of sanctions for alleged noncompliance." Wheeler *et al.*, *supra* note 254, at 7.

[265] Larry Catá Backer, *Global Panopticism: States, Corporations and the Governance Effects of Monitoring Regimes*, 15 IND. J. GLOBAL LEGAL STUD. 101, 110 (2008).

[266] *Id.* at 111.

[267] *Id.* at 112.

[268] *Id.*

[269] Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 670 (2012).

that might limit efforts to increase Federal HIPAA enforcement, HHS also could study whether the States could be better incentivized to assist with HIPAA enforcement.[270]

B. Study Assessing Feasibility of Limited Safe Harbor for Covered Entities Engaged in Best Practices

It seems like sound policy to encourage upstream HIPAA entities to provide guidance and supervision to downstream entities. There are several reasons, however, that CEs or BAs contracting with cloud service providers might not exercise this supervisory role.

For one, as discussed in Section IV.A.1. above, cloud service providers enjoy strong bargaining power and thus sometimes demand that CEs and BAs sign form contracts. It is unlikely cloud service providers will volunteer to be controlled and directed during their performance under the BAA, opting instead for independence and flexibility. HHS could address the bargaining power disparity and encourage downstream supervision by requiring BAAs to include terms that preserve a monitoring role for CEs and BAs.

Even without the bargaining imbalance, a CE or BA may be reluctant to reserve the right or authority to control a downstream BA's conduct[271] for fear of being held liable for the agent's violations even though the CE or BA lacks any real ability to control the agent's behavior. HHS expressed its understanding in the preamble to the Omnibus HIPAA Rule that a BA could still be acting within the scope of agency if it deviated from the terms of the BAA by, for example, acting carelessly, making a mistake, or disregarding the CE or upstream BA's specific instruction.[272] Thus, it appears that although agency liability requires the principal to have the authority to control the BA's conduct by, for example, being able to give instructions during the course of the agent's performance of the service, agency liability does not necessarily lapse when the agent does not heed the principal's instructions. A CE or BA may not want to retain the appearance of control yet risk that it will be liable for a sloppy or perhaps even rogue agent's violations. It would be helpful for HHS to expand on its discussion in the preamble to the Omnibus HIPAA Rule as to when a CE or upstream BA would remain liable for the violations of an agent that disregards the principal's instructions or otherwise violates the BAA.

Moreover, given the technical complexities of cloud computing, it would be valuable for HHS to focus more attention on regulating cloud providers more directly. The nascent auditing of BAs discussed elsewhere in this paper may provide one model. HHS also ought to clarify to

---

[270] Unfortunately, despite some notable action against an Accretive breach in Minnesota, other states have not been that active in utilizing newfound authority under HITECH. Kimberley Leonard, *State Attorneys General Not Leaping to Embrace HIPAA Enforcement*, THE CENTER FOR PUBLIC INTEGRITY, http://www.publicintegrity.org/2011/09/20/6666/state-attorneys-general-not-leaping-embrace-hipaa-enforcement.

[271] Final Omnibus HIPAA Rule Preamble, *supra* note 51, 78 Fed. Reg. at 5581.

[272] *See id.* at 5582. *But cf. id.* at 5587 ("An agent that fails to notify a covered entity or business associate may be acting outside its scope of authority as an agent.")

what extent agency liability applies in the cloud computing context. The preamble emphasizes that agency liability is a fact sensitive inquiry that depends on the type of service and skill level required to perform the service.[273] HHS expressed its doubt, for example, that a small provider would have sufficient expertise to supervise and direct a company hired to de-identify PHI.[274] It is unclear how this analysis applies in the cloud computing context. It is possible that at least some cloud computing services require expertise CEs and upstream BAs lack such that the cloud service provider is not the agent of the CE or BA. But this analysis depends on the particular service the cloud service provider is performing as well as the skill set and expertise of the CE or upstream BA. In addition, since a CE or BA does not need to retain the right or authority to control every aspect of a downstream BA's activities to create agency liability,[275] perhaps HHS will take the position that, despite cloud expertise, CEs and BAs can and should supervise downstream cloud BAs at least with respect to risk management and HIPAA compliance. CEs and BAs would benefit from additional guidance from HHS regarding whether cloud service providers are or can be agents of CEs or upstream BAs despite potential gaps in technical sophistication.

To the extent agency liability applies to cloud service provider relationships, HHS could study the feasibility of creating a limited safe harbor for CEs and upstream BAs who engage in guidance and vetting of downstream BAs. Recognizing that HHS recently omitted from the Omnibus HIPAA Rule a previous exception to agency liability for CEs,[276] this limited safe harbor could not be an end run around agency liability. Rather, a limited safe harbor would need to go beyond the elements of the liability exception HHS rejected. For example, in addition to complying with the pertinent BAA and HIPAA requirements and not being aware of a pattern or practice of the BA violating the contract, CEs and upstream BAs would need to actively engage in evaluating, educating, monitoring, and providing feedback to downstream BAs with the goal of raising awareness of and sensitivity to the need to protect PHI. A number of the security provisions itemized in Section IV.A above could facilitate the vetting and monitoring HHS wants to encourage, such as requiring an SSAE 16 SOC, Type II audit and access to the cloud vendor's security officer for technical level discussions about its security practices.[277] To encourage due

[273] *Id.* at 5581.
[274] *Id.*
[275] *Id.* at 5582.
[276] *Id.* at 5580; James Swann, *supra* note 63.
[277] *See* Markey & Marchak, *supra* note 7, at 23, 33. Markey & Marchak offer a useful list of questions to consider asking as part of the due diligence required to assess a cloud vendor's approach to security:

- What security measures are in place to protect the data center against unauthorized physical intrusion?
- Who would be permitted to access my data and under what circumstances?
- What are your procedures for terminating access to data or systems upon termination of an employee, or upon change of job duties?
- What are the processes to ensure that default passwords are changed and/or other access controls are implemented?

diligence and vigilance, HHS could distinguish supervising from exercising control. Thus, guidance could clarify that being more aware of how a cloud vendor approaches security and confirming that it has a clean audit before engaging in business with that vendor, for example, as distinguished from retaining control to direct vendor actions on a day-to-day basis, will not create agency liability.

Alternatively, in determining how to exercise its discretion both to bring enforcement actions and to set penalties, HHS could issue guidance clarifying that it will take into consideration the relative bargaining power of the parties and the extent to which CEs or upstream BAs took steps to assess risks and take appropriate steps to preserve PHI. For example, HHS could affirm the value of CEs and upstream BAs vetting potential vendors prior to contracting to evaluate their qualifications and compliance with HIPAA; using a BAA that includes all terms required by HHS; actively monitoring the agent's performance; providing appropriate and ongoing training and instruction to cloud service providers; and responding to signals of possible violations.[278]

- What procedures exist to ensure configurations are properly set?
- What does your testing/patch process include?
- What is your encryption policy?
- How do you secure transmissions outside your network?
- Where will the data be stored? In the United States or other countries?
- Does the cloud provider:
    - Have cyber-insurance?
    - Have an audit certification of their information security program in compliance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 or 3, or equivalent audit (e.g. ISO 27001/2)?
    - Conduct (at a minimum) quarterly vulnerability scans and annual network penetration tests?
    - Use security monitoring and event log management to ensure the collection and secure storage of audit trails?
    - Review event logs periodically for anomalies?
    - Document changes following industry standard practices for configuration management and change control?
    - Employ redundant hardware components, load-balanced Internet connections with multiple service providers, and functioning firewalls?
    - Implement backup options and encrypt any removable or portable backup media?
    - Conduct business continuity and disaster recovery exercises on a regular, planned basis?

Markey & Marchak, *supra* note 7, at 22-24.

[278] *Cf. generally* Dep't of Just. & U.S. Sec. & Exchange Comm'n, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, 57-62 (Nov. 14, 2012), http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf (itemizing ten hallmarks of effective compliance programs that DOJ and SEC take into consideration in deciding whether to take enforcement action against a company and what penalty to impose: commitment from senior management and clearly articulated policy against corruption; code of conduct and compliance policies and procedures; oversight,

C. Increasing Patient Empowerment: From Transparency to Intelligibility to Accountability

Expanding access to personal information is part of a larger movement to hold corporate actors accountable in an era of rapidly declining data storage costs. Asked about privacy practices, Google's former CEO Eric Schmidt once said, "[W]e like to get right up to the creepy line, but not cross it."[279] But it would probably be more accurate to say that he and other corporate leaders don't want to be *caught* crossing the creepy line. Law and technology provide a rich variety of tactics to avoid that possibility. Accountings of disclosures should provide a persistent record of data use that should deter at least some privacy violations.[280]

Many aspects of the Omnibus HIPAA Rule are aimed at assuring that patients are able to understand (and control some) aspects of the data kept about them by CEs and BAs. While the Rule makes several steps in the right direction, it does not reflect a full appreciation of the levels of complexity in data flows occasioned by technological advance. Standards and best practices still need to be adopted by the larger cloud computing community to assure optimal realization of these rights. For example, how well can records interact with visualizations like Collusion or The Data Map?[281] Fuller interoperability and more open API's will be necessary in order to empower consumers to fully understand how data flows, and how those flows influence their opportunities.

Nor did Congress adequately appreciate, in HITECH, the degree to which big data companies' use of health-inflected data could eventually render HIPAA irrelevant by fueling the creation of medical reputations unmoored from covered medical records. In order to address these 21st century challenges to health privacy, policymakers should take two steps: rendering

---

autonomy, and resources; risk assessment; training and continuing advice; incentives and disciplinary measures; third party due diligence and payments; confidential reporting and internal investigation; continuous improvement: periodic testing and review; mergers and acquisitions: pre-acquisition due diligence and post-acquisition integration).

[279] Derek Thompson, *Google's CEO: 'The Laws Are Written by Lobbyists,'* ATLANTIC ONLINE (Oct. 1, 2010, 11:58 AM), http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/.

[280] *See* HIPAA Privacy Rule Notice of Proposed Rulemaking, *supra* note 161 (pointing out that audit trails "discourage inappropriate behavior").

[281] Gary Kovacs has promoted Collusion as an app to track app data sharing; Latanya Sweeney has focused "The Data Map" on health issues. Latanya Sweeney, *The Data Map, available at* http://thedatamap.org/intro.html ("When you visit a doctor, you expect some organizations to receive information about your visit (*e.g.*, your medical insurance company and your pharmacy), but you might be surprised and not even recognize many of the other entities who may also receive identifiable information about your visit (*e.g.*, a data mining company, your employer, your state government). If you then suffer an economic harm or discrimination as a result of the hidden sharing, you would not know the information was used against you, and if the information was incorrect, you could offer no correction. If a data breach occurs, you would not know your information was stolen because you would have no reason to believe your information was being held by the breached company, yet you could be the victim of identity theft or medical identity theft as a result.").

existing data about information practices more intelligible to consumers, and presenting in plain terms to Congress the types of privacy challenges enabled by the deployment of big data.

Over a decade ago, Bill Sage complained that both supporters and critics of information-based regulation in healthcare "have overlooked serious operational issues and misunderstood some of the best uses of information."[282] Sage argued that disclosure must be "properly designed and implemented" to improve outcomes, and he worried that the disclosure movement of the 1990's was ill-equipped to provide actionable information to patients and providers.[283] Sage's concerns appear especially relevant in the realm of health privacy, where the proliferation of entities with some interest in and access to health records is far outpacing the ability of conventional notices and written descriptions to convey information to patients.

As HHS continues clarifying the implications of the Omnibus HIPAA Rule, it should focus on moving from *transparency* to *intelligibility* in health data. Rather than merely opening up presently maintained information, policymakers need to focus on promoting the types of standards and analysis that can make that data actionable. This will require careful collaboration between regulators, technical experts, and data visualization and design experts who have studied optimal communication strategies.

The President's Council of Advisors on Science and Technology ("PCAST") warned in 2010 against health information technology adoption uninspired by a vision for data use and sharing that would allow healthcare to enjoy the quality and efficiency gains characteristic of information industries.[284] It is now time to take the next step and consider how high technology approaches could also promote privacy in healthcare. In this respect, the Federal Trade Commission, often seen as the lead privacy regulator in the U.S. (and an entity with some role in health privacy, given its statutory authority to regulate personal health records), offers both lessons and a cautionary tale.

Realizing how quickly the world of online data collection is moving, the FTC has taken important steps to monitor evolving business practices. The agency appointed Ed Felten as "Chief Technologist," and has also employed highly regarded privacy experts like Paul Ohm and Christopher Soghoian. Soghoian and Felten have extensive experience in computer science; Ohm combines computer science training with legal expertise. Each of these individuals has done a great deal to help the agency apply expertise to current problems in privacy. Moreover, the agency's report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, was a model of sensitive appreciation of stakeholder concerns, leading to guidance on some best practices for digital companies.

---

[282] William M. Sage, *Regulating Through Information: Disclosure Laws and American Health Care*, 99 COLUM. L. REV. 1701, 1710 (1999).
[283] *Id.*
[284] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 28, at 14.

This perceptive, well-written report grappled with fundamental issues in the law of fair data practices and consumer protection. Where the law was plainly inadequate, the report said so. For example, it supported "legislation that would provide consumers with access to information held by data brokers," an increasingly important priority in a pervasively scored society.[285] The FTC's December 2012 subpoena of leading data brokers indicates an interest in illuminating some of the darker corners of data collection, analysis, sharing, and use. The FTC's commitment to technical personnel and cutting edge reports is something of a model for other agencies tasked with protecting privacy in an era of rapid change.

Nevertheless, there are also faults in the FTC's approach. Peter Maass's investigative report for ProPublica called the agency hopelessly outmatched in terms of staffing, vis-à-vis the extraordinary proliferation of data-driven business models it is ostensibly policing.[286] Echoing the 1968 *Nader Report* on the FTC, Maass described the near-heroic (but ultimately doomed) efforts of a chronically underfunded entity to keep up with privacy threats in the new economy. Sadly, top officials at the agency were more defensive than supportive of Maass's characterization of the impossible task Congress had set for them, given the resources allocated to it. Where its technical capacity is clearly lacking, it should say so. And it should not be afraid to ask Congress for the resources it needs to detect lawbreaking. This might include a self-funding agency model, like the Patent and Trademark Office, the Consumer Financial Protection Bureau, or the FDIC.[287] Or it could ask for authorization to hire contractors to discover wrongdoing, paying them on a contingency basis. All of these approaches should be considered by agencies tasked with protecting health privacy, lest their mission shrink to fit whatever inadequate resources happen to be allocated to them in any particular budget cycle.

V. Conclusion

There are multiple uses (and misuses) of health information compiled about patients, insureds, research subjects, physicians, hospitals, and populations. Privacy law has focused on

[285] Applying the Fair Credit Reporting Act, the FTC itself required firms that "score" the health status of individuals based on their pharmacy records to disclose these records to scored individuals.

[286] Peter Maass, *Your FTC Privacy Watchdogs: Low-tech, Defensive, Toothless*, ProPublica/Wired Joint Publication (June 28, 2012), *available at* http://www.wired.com/threatlevel/2012/06/ftc-fail/all/ ("The mismatch between FTC aspirations and abilities is exemplified by its Mobile Technology Unit, created earlier this year to oversee the exploding mobile phone sector. The six-person unit consists of a paralegal, a program specialist, two attorneys, a technologist and its director, Patricia Poss. For the FTC, the unit represents an important allocation of resources to protect the privacy rights of more than 100 million smartphone owners in America. For Silicon Valley, a six-person team is barely a garage startup. Earlier this year, the unit issued a highly publicized report on mobile apps for kids; its conclusion was reflected in the subtitle, 'Current Privacy Disclosures Are Disappointing.' It was a thin report, however. Rather than actually checking the personal data accessed by the report's sampling of 400 apps, the [17 page] report just looked at whether the apps disclose, on the sites where they are sold, the types of personal data that would be accessed and what the data would be used for.").

[287] For a description of the self-funding model, see Juliana Gruenwald, *SEC Chief Backs Self-Funding*, GOV'T EXEC., Mar. 17, 2010, http://www.govexec.com/oversight/2010/03/sec-chief-backs-self-funding/31076/.

assuring the confidentiality, security, and accuracy of health information. The post-HITECH landscape will increasingly balance these concerns with the goals of innovation, access, and cost-control.

A new body of law—health information law—is becoming a distinctive field. Just as intellectual property (IP) law adapted property law principles to new economic phenomena, and privacy law extended tort and contract law principles into the intangible realm of reputation, now health information law is emerging to combine IP, privacy, and administrative principles in the high-stakes healthcare context.

Advanced information technology has raised a number of new questions. Beyond HIPAA and HITECH regulation, consumer protection law plays an important role in these fields. Patients are opting to personalize their health records with the help of cloud computing firms; what law governs this digital migration? There is increasing concern about the role of "incidental findings" in medical research; how will regulators and professional groups address them? When employers demand access to employee health records, in what ways can they use them to profile the employee? Should law limit the development of "medical reputations" about individuals, even if they are not based on protected health records? What are the proper tradeoffs between data privacy, security, portability, integrity, and accuracy?

The networked health IT of cloud computing will raise all these questions and more as it attempts to bring the productivity gains characteristic of information industries to healthcare. But its systems need to be designed to protect the integrity and security of protected health information.

The laws governing the management of healthcare information are extremely complex. Some of this complexity is necessary to the subject matter. However, it should not obscure the larger goals of health information law. This white paper has recommended some steps forward to assure that the interests of patients are front and center as health data collection enters a new and qualitatively different era of promise and peril. Both covered entities and their cloud service providers should be held to high standards by technologies of compliance as precise and persistent as the practices they aim to monitor and improve. If medical reputations are being created with data outside the bounds of present HIPAA and HITECH regulation, HHS needs to study these processes and acknowledge the limits of present models of privacy protection. Finally, regulation needs to assure that responsibility for protecting the privacy and security of data rests with the correct entity, be it a covered entity or business associate. The Omnibus HIPAA Rule released in January 2013 is a major step forward for health privacy, but more work remains to be done to assure a regulatory framework up to the challenges generated for privacy and security generated by cloud computing technologies.