Saint Louis University Journal of Health Law & Policy

Volume 8
Issue 2 *Overcoming Barriers to Effective Legislative and Regulatory Changes in Health Care*

Article 8

2015

HITECH Act: Building an Infrastructure for Health Information Organizations and a New Health Care Delivery System

Kalle Deyette
kdeyette@slu.edu

HITECH ACT: BUILDING AN INFRASTRUCTURE FOR HEALTH INFORMATION ORGANIZATIONS AND A NEW HEALTH CARE DELIVERY SYSTEM

TABLE OF CONTENTS

I. INTRODUCTION

The United States (U.S.) spends trillions of dollars on health care every year.[1] Nearly thirty percent of that spending is on wasteful medical treatment.[2] Approximately 44,000 to 98,000 deaths occur each year in hospitals as a result of preventable medical errors,[3] and an additional 770,000 people are injured because of adverse drug events.[4] Faced with rising medical costs, high medical errors, and inefficient use of medical resources, the U.S. has debated the use of health information technology (health IT) for a decade.[5] Many envision health IT as a way to reduce costs, improve quality and safety of care, and increase data availability for the improvement and development of public health and clinical research,[6] visualizing it as the backbone of a new health care delivery system.[7] Additionally, health IT is viewed as a method to accomplish integration, both horizontally and vertically, which stands at the heart of many of the initiatives of the Affordable Care Act (ACA), such as Accountable Care Organizations (ACOs).

1. *National Health Expenditure Data: Historical*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html (last modified Jan. 7, 2014).

2. NICOLE CAFARELLA LALLEMAND, HEALTH AFFAIRS POLICY BRIEF: REDUCING WASTE IN HEALTH CARE 2 (2012), *available at* http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_82.pdf. *See* Elliot S. Fisher et al., *The Implications of Regional Variations in Medicare Spending, Part 1: The Content, Quality and Accessibility of Care*, 138 ANNALS INT. MED. 273, 273 (2003); *see also* Elliot S. Fisher et al., *The Implications of Regional Variations in Medicare Spending, Part 2: Health Outcomes and Satisfaction with Care*, 138 ANNALS INT. MED. 288, 297-98 (2003).

3. INST. OF MED., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 26 (Linda T. Kohn et al. eds., 1999).

4. AGENCY FOR HEALTHCARE RESEARCH & QUALITY, No. 01-0020, RESEARCH IN ACTION: REDUCING AND PREVENTING ADVERSE DRUG EVENTS TO DECREASE HOSPITAL COSTS 1 (2001), *available at* http://archive.ahrq.gov/research/findings/factsheets/errors-safety/aderia/ade.html

5. On April 24, 2004 George W. Bush established the Office of the National coordinator for Health Information Technology (ONC) to "develop, maintain, and direct the implementation of a strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors that will reduce medical errors, improve quality, and produce greater value for health care expenditures." Exec. Order No. 13335, 69 Fed. Reg. 24059, 24059 (April 30, 2004). The Senate developed the Wired for Health Care Quality Act and in 2008, the House worked on the Protecting Records, Optimizing Treatment, and Easing Communication through Healthcare Technology Act and the Health-e Information Technology Act. *See* Pete Stark, *Congressional Intent for the HITECH Act*, 16 AM. J. MANAGED CARE SP 24, SP 25 (2010).

6. Stark, *supra* note 5, at SP 24, SP 26.

7. *See* Michael R. Solomon, *Regional Health Information Organizations: A Vehicle for Transforming Health Care Delivery?*, 31 J. MED. SYS. 35, 35 (2007).

With health IT as the backbone of the health care delivery system, information is at providers' fingertips, allowing them to deliver better patient-centered care. For example, a patient from Saint Louis, Missouri could appear unconscious at an emergency room (ER) in the Bootheel of the state and the treating physician could instantly gain access to her medical records through the *Missouri Health Connection*—Missouri's health information organization (HIO). The physician could see, for example, that the patient had a metal plate inserted in her head when she was thirty years old and is currently being treated for diabetes. Additionally, her medical record would list all of her medications and past laboratory tests. After reviewing the record, the physician would then know the proper medications to prescribe to avoid adverse drug interactions. As a result of health IT, this ER physician would no longer be treating the patient blindly, running every test imaginable to get a snap shot of the patient's medical status. The physician, equipped with an accurate, detailed medical history, would be able to customize each patient's medical treatment specifically to him or her. Additionally, the patient's treating physicians back in Saint Louis would be alerted that their patient was admitted and could then follow up with the patient upon their return to Saint Louis. Further, the Saint Louis physicians would have immediate access to all treatments done in the Bootheel by other providers and, therefore, would not need to go through the hassle of contacting the hospital in the Bootheel, requesting the patient's file, waiting for the hospital to process the request, tracking down the patient's file, photo copying it and, finally, faxing the file over. The file, including laboratory results, could immediately be pulled up on the computer.

Two health IT-innovations make this patient's experience possible: electronic health records (EHRs) and health information exchanges (HIEs). The EHR is a digital version of a patient's full medical history completed by all providers and staff members from multiple health organizations.[8] The HIE is "[t]he electronic movement of health-related information among organizations."[9] In addition to these definitions, formal organizations that

8. *What is an Electronic Medical Record (EMR)?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/electronic-medical-records-emr (last visited Jan. 3, 2014). It should be noted that there is a difference between Electronic Medical Records (EMRs) and EHR. EMR is a digital version of a patient's medical chart from one medical practice that contains the patients' medical history from that medical practice. *Id*. The HITECH Act provides funding and incentives for the implementation of EHRs. American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 300jj-32, 300jj-34, 300jj-35 (2012).

9. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEP'T HEALTH & HUMAN SERVS., DEFINING KEY HEALTH INFORMATION TECHNOLOGY TERMS 22 (2008) [hereinafter DEFINING KEY HIT TERMS]. While HIE refers to the electronic exchange of health-related information among organizations, an HIE that conforms to nationally recognized standards, may exchange information with only a single organization. *Id.* at 24. The key is that

"oversee and govern the exchange of health-related information among organizations according to nationally recognized standards" are called HIOs.[10] Thus, the EHR is the complete medical record, the HIE is the process by which the records are shared, and HIOs are the organizations governing the HIE. Together they create an infrastructure that integrates the different providers by giving them access to timely, accurate, and complete information. This information allows providers to make better-informed decisions regarding treatment and to avoid duplicative tests.[11] Taken together, EHRs and HIOs have the potential to reduce costs, facilitate coordination, and improve the quality, safety, and service of care.

Historically, several barriers have prevented the widespread use of these technologies. First, the cost of implementation was substantial.[12] Second, providers questioned the security of the technology, worrying the organization could not adequately protect the confidentiality of personal health information.[13] Third, little information existed to assist providers in choosing the appropriate technology and integrating it into their practices.[14]

To address these barriers, on February 17, 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act.[15] The HITECH Act attempts to make health IT the backbone of the health care delivery system. It builds an infrastructure for the development and implementation of health IT in four ways. First, the HITECH Act establishes congressional support for the National Coordinator for Health Information Technology (ONC), whose goal is to develop a strategic plan and to develop policies to standardize health IT.[16] Second, the Act establishes a two billion dollar fund to start and strengthen programs that support providers' adaptation and development of health IT and data exchange.[17] Third, the HITECH Act creates incentives for providers who meaningfully use health IT—specifically certified by the ONC—through additional Medicare and Medicaid payments.[18]

---

the HIE meets the nationally recognized standards so it has the ability to exchange information with disparate entities.

10. *Id.*

11. *See* Solomon, *supra* note 7, at 39.

12. *See* Marsha Gold et al., *Obtaining Providers' Buy-in' and Establishing Effective Means of Information Exchange Will Be Critical to HITECH's Success*, 31 HEALTH AFF. 514, 515-16 (2012).

13. *Id.* at 517-18.

14. *Id.* at 517.

15. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited Jan. 2, 2014). The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009. *Id*.

16. American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 300jj-11 (2012).

17. 42 U.S.C. § 300jj-31 (2012). *See also* Stark, *supra* note 5, at SP 26.

18. 42 U.S.C. § 1395w-4(o) (2012); 42 U.S.C. § 1396b(a) (2012).

Fourth, recognizing that the success of implementing health IT depends on the belief of both providers and patients that their personal health information is secured, protected, and used properly,[19] the HITECH Act strengthens the way in which the Health Insurance Portability and Accountability Act (HIPAA) can provide better protection of individually identifiable health information.[20]

This paper examines the HITECH Act's impact on the formation of HIOs and the adoption of health IT. The first section of the paper defines HIOs, the benefits they add to the delivery system, and the barriers to their formation, outlining the need for governmental assistance. The second section of the paper, divided into two parts, analyzes the HITECH Act's two major interventions: the modifications to HIPAA, as well as federal grants. The first part argues that the new HIPAA modifications create a legislative framework that builds trust in HIOs and increases stakeholders' support and willingness to participate in them, because the law now defines the parties' obligations to each other and creates a structure, or a checklist, around which HIOs form. The second part describes various funding opportunities available to stakeholders to develop and implement HIOs and other health IT necessary for the success of HIOs, such as EHRs. This part of the paper argues that while these funding opportunities created by the HITECH Act address the historical barriers to HIOs, the HITECH Act's ambitious timeline and scope ultimately create new barriers for the development of HIOs. The final section of the paper analyzes the HITECH Act's impact on the implementation of HIOs, including the need for policy modifications and future government support if the health industry is to fully capitalize on the government's investment in health IT.

Ultimately, health IT will become the backbone of the health industry, but it will not be under the HITECH Act's timelines or original vision. The HITECH Act simultaneously calls for the creation of new technology, policies, and implementation for an industry that historically evolves at a snail's pace. The HITECH Act was overly ambitious, and it left the industry to develop and implement a new system in just a few years, or else lose substantial money. Furthermore, the Act underestimated the time it would take to develop and implement the technology,[21] as health IT evolves much faster than any federal Agency can produce guidelines. The result is that the industry, going forward, will be in a state of frenzy and frustration. As the industry tries to build a newer infrastructure around the amorphous vision forced upon them by scholars and government officials, smaller regulations and laws will need to be enacted to fill the gaping holes.

19. *See infra* Part II.B.1.

20. *See infra* Part III.A.

21. ROB CUNNINGHAM, NAT'L HEALTH POLICY FORUM, ISSUE BRIEF NO. 834, STIMULUS BILL IMPLEMENTATION: EXPANDING MEANINGFUL USE OF HEALTH IT 1, 5 (2009), *available at* http://www.nhpf.org/library/issue-briefs/IB834_StimulusIT_08-25-09.pdf.

II. HEALTH INFORMATION ORGANIZATIONS (HIOS)

There is no single definition of an HIO, nor is there one standard function of an HIO.[22] HIOs come in a variety of forms and perform various functions, such as electronic prescribing (e-prescribing) and automatic laboratory recording.[23] Therefore, no precise definition can cover the spectrum of different types of organizations.[24] However, generally speaking, an HIO is a formal "organization that oversees and governs the exchange of electronic health-related information between different, disparate organizations within the health care industry according to national standards."[25] Ideally, the HIO facilitates the exchange of health-related information between all stakeholders, including providers, hospitals, pharmacies, clinics, insurance companies, and potentially, the patient.[26] Currently, information is coming and going in pieces, creating a fractional, disarrayed system where information is unavailable, incomplete, and/or untimely. The idea is to move away from this fragmented system and to create a new centralized system where information can converge and be systemically disseminated throughout the health care industry.[27] The centralized system is the HIE and the organization that runs the HIE is the HIO. Below is a depiction of the flow of information under the current system and a depiction of the flow of information facilitated by an HIO.

22. *See* U.S. DEP'T HEALTH & HUMAN SERVS., PRIVACY AND SECURITY FRAMEWORK: INTRODUCTION 1 (2008) [hereinafter FRAMEWORK INTRODUCTION].

23. HEALTHCARE INFO. & MGMT. SYS. SOC'Y, INTEGRATING THE HIE INTO THE EHR WORKFLOW 3-7 (2011).

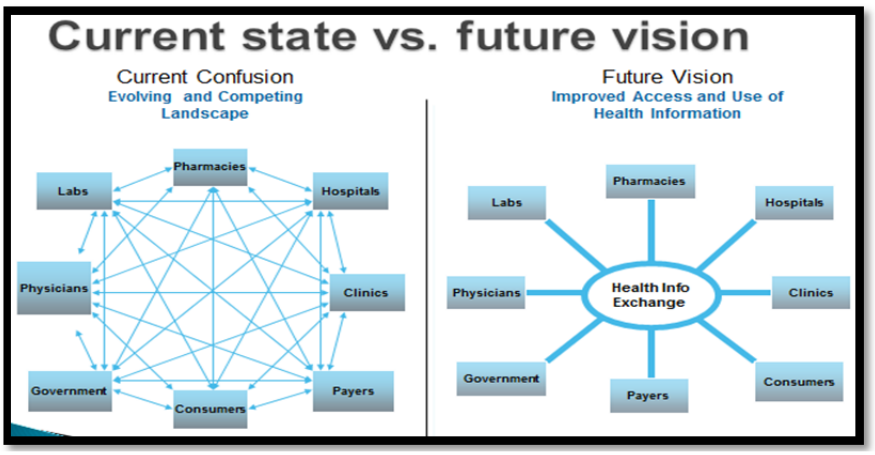
24. *See* FRAMEWORK INTRODUCTION, *supra* note 22, at 1; *see also* DEFINING KEY HIT TERMS, *supra* note 9, at 23.

25. DEFINING KEY HIT TERMS, *supra* note 9, at 24.

26. *See* JULIE J. MCGOWAN ET AL., WESTAT, STRENGTHENING HEALTH INFORMATION EXCHANGE: FINAL REPORT HIE UNINTENDED CONSEQUENCES WORK GROUP 1 (2012).

27. *See infra* Figure 1.

Figure 1[28]



A. Benefits of HIOs

Creating a centralized system has the potential to revolutionize the health care delivery system by (1) improving quality, (2) reducing costs, and (3) advancing both clinical and public health research.[29] First and foremost, it would improve the quality of care by giving providers access to a person's medical information at the point-of-service. Having the information at the point-of-service will improve patient safety because providers will immediately have knowledge of any allergies and medication and thus, be able to avoid adverse events.[30] Additionally, having access to complete and updated information will improve quality of care by assisting with chronic disease management.[31] Chronic diseases, like diabetes, often need continuous treatments and involve collaboration between multiple specialties in order to be effective.[32] An HIO will allow the different specialties to communicate in real-time to develop a single, integrated treatment plan and help monitor patient compliance. This will keep patients healthier and out of the hospital.[33] Moreover, this could improve the quality of care by improving the patient's

28. Ron Levy, Executive-in-Residence, Dep't of Health Management & Pol'y, Saint Louis Univ. Sch. of Pub. Health, Lecture to Health Care Organization class on Missouri Statewide Health Information Organization 6 (Nov. 6, 2012).

29. MCGOWAN ET AL., *supra* note 26, at 8-11.

30. *Id.* at 8-9.

31. *Id.* at 9.

32. *See generally* C.B. Giorda et al., *Comparison of Direct Costs of Type 2 Diabetes Care: Difference Care Models with Different Outcomes*, 24 NUTRITION, METABOLISM & CARDIOVASCULAR DISEASES 717, 717-18, 723 (2014).

33. Nir Menachemi & Taleah H. Collum, *Benefits and Drawbacks of Electronic Health Record Systems*, 4 RISK MANAGEMENT & HEALTHCARE POLICY, 47, 49 (2011) [hereinafter *EHR Benefits and Drawbacks*].

experience. Imagine the improvement in a patient's experience if they no longer needed to go through the hassle of repeatedly filling out pages of documents detailing their medical history, or having to remember to bring in a plastic bag filled with their medications.

Secondly, the HIO, through the facilitation of data, reduces medical costs by helping providers practice more effectively. Specifically, by exchanging health data, providers have access to the results of previous tests and past courses of therapy, which reduces duplicative tests, redundant data, and ultimately, medical costs.[34] One study predicts that EHRs could "save approximately $44 billion per year in reduced medication, radiology, laboratory and [adverse drug event]-related expenses per year."[35] Further, an HIE can reduce the cost of readmissions and possibly reduce over-utilization by assisting the health care industry in providing a continuum of care.[36] This is particularly important to hospitals, as the ACA penalizes hospitals with high readmission rates.[37] Moreover, HIEs can reduce administrative costs associated with medical transcription and filing claims.[38] Currently, providers must spend significant time and money on administrative tasks such as transcribing physician notes, pulling charts, filing papers, and processing laboratory orders and results.[39] The use of an HIO would greatly reduce or eliminate this expense because the exchange of data would bring the charts to the physicians' finger tips, notes would be automatically entered as they are taken, and laboratory orders and results would be automatically routed and stored.[40] Furthermore, the use of an HIO to facilitate HIEs would increase providers'

34. *Id.* at 49-50.

35. Scott Barlow et al., *The Economic Effect of Implementing an EMR in Outpatient Clinical Setting*, 18 J. HEALTHCARE INFO. MGMT. 14-52 (2004), *reprinted in* 18 J. HEALTHCARE INFO. MGMT. 1, 6 (2004), *available at* http://www.himssehra.org/docs/caseStudies/Allscripts_JHIM_Central%20Utah%20Clinic%20Case%20Study.pdf.

36. *See* Sean M. Murphy & Darin Neven, *Cost-Effective: Emergency Department Care Coordination with a Regional Hospital Information System*, 47 J. EMERGENCY MED. 223, 224-225, 227 (2014) (concluding that care coordination with the use of an HIO reduced the number of visits to the emergency room and the resources utilized per visit); *see also* Mary Mosquera, *UnitedHealthcare Sees Lower ER Use with Data Exchange*, HEALTHCAREIT NEWS (Sep. 29, 2011), http://www.healthcareitnews.com/news/unitedhealthcare-sees-lower-er-use-data-exchange.

37. *See Selected Medicare Hospital Quality Provisions Under the ACA*, ASS'N AM. MED. COLLS., https://www.aamc.org/advocacy/medicare/153882/selected_medicare_hospital_quality_provisions_under_the_aca.html (last visited Feb. 23, 2014).

38. *See* Barlow et al., *supra* note 35, at 3-4.

39. Angela Ferneding, *Regional Health Information Organizations: Lower Health Care Costs, Fewer Iatrogenic Illnesses, and Improved Care – What Are We Waiting For?*, 22 J. L. & HEALTH 163, 173 (2009).

40. *Id.*

accounts-receivable and cash-on-hand by improving the efficacy and accuracy of claims processing.[41]

Thirdly, HIOs will facilitate clinical and public health research. HIOs can aggregate large sums of data, which researchers can use to detect emerging public health concerns and determine the needs of a community.[42] Population health data is becoming increasingly more important for organizations, especially for non-profit hospitals that must conduct community health needs assessments every three years, as a result of the ACA's emphasis on evidence-based medicine.[43] Furthermore, data available through HIOs can also support initiatives focusing on comparative-effectiveness research and patient-centered outcomes research.[44] For example, Indiana is using an HIE to compare the relative effectiveness of different medications for behavioral symptoms of Alzheimer's disease.[45] This represents just one way in which data aggregated by an HIO can be used to advance clinical medicine.

B. Barriers to HIOs

HIOs and HIEs are not new ideas—states, communities, and organizations have been trying to implement them for years.[46] Early pilots faced barriers, including: (1) cost of implementation, (2) technical constraints through product availability and product integration, and (3) stakeholder support and buy-in.[47] HIOs developing today continue to struggle in overcoming these same barriers.[48] Many of these barriers are associated with the implementation of EHRs because without the implementation and systematic use of EHRs throughout the health care industry and in all aspects of patient care, HIOs will not be successful—they are only as effective as the information shared with them.

41. *Id.* at 173. *See also EHR Benefits and Drawbacks*, *supra* note 33, at 50.

42. *See* MCGOWAN ET AL., *supra* note 26, at 10.

43. *See* Greg D. Randolph & John H. Morrow, *The Potential Impact of the Affordable Care Act on Population Health in North Carolina*, 74 N.C. MED. J. 330, 330-32 (2013).

44. *See* MCGOWAN ET AL., *supra* note 26, at 11.

45. *Id*.

46. PRASHILA DULLABH ET AL., NORC, UNIV. OF CHICAGO, THE EVOLUTION OF THE STATE HEALTH INFORMATION EXCHANGE COOPERATIVE AGREEMENT PROGRAMS: STATE PLANS TO ENABLE ROBUST HIE 1-2 (Aug. 2011), *available at* http://www.healthit.gov/sites/default/files/pdf/state-health-info-exchange-program-evolution.pdf. *See also* Solomon, *supra* note 7, at 36-38.

47. *See* Gold et al., *supra* note 12, at 515-18.

48. *See generally* Julia Alder-Milstein et al., *Operational Health Information Exchanged Show Substantial Growth, but Long-Term Funding Remains a Concern*, 32 HEALTH AFF. 1486 (2013).

1. Participants' Trust and Buy-In

Because HIOs simply govern the exchange of electronic health-related information among participants, HIOs cannot exist without participants' trust and buy-in.[49] HIOs need participants to exchange data and in order for them to be willing to do so, they need to trust that the data will remain private and secure. Participants need to trust that their relationship with their patient (or customer) will remain unaffected and that the HIO can adequately protect the confidentiality and integrity of the information being exchanged. A breach of a patient's (or customer's) personal health information could harm patients (or customers) and destroy the trust between them and participants. Further, breaches increase participants' risk of liability. Under HIPAA and other state laws, covered entities and business associates are required to implement reasonable precautions to protect personal health information.[50] Thus, the industry has a financial incentive to take extra precaution when exchanging data. Moreover, as participants, providers fear that moving towards an electronic era will depersonalize medicine and jeopardize their relationships with patients.[51] This is particularly worrisome because a provider's practice depends on strong relationships with their patients.

In addition to the participants, the patient whose information is ultimately being exchanged needs to trust that the HIO is secured and private, in order to consent to the exchange of their information. HIPAA's Privacy Rule requires notice and patient authorization for providers to use personal health information for any purposes, other than purposes that are medically necessary, such as the submission of claims data to the patient's insurance company for payment.[52] Therefore, in accordance with HIPAA's Privacy Rule, most HIOs currently under development require that a patient whose provider is a participant in the HIO, be given notice that his or her data will be exchanged through the HIO, and further, the patient must be given the opportunity to opt-out of the exchange.[53] Under this system, referred to as an "opt-out system," a patient's information will be exchanged through the HIO unless he or she takes

49. *See* Gold et al., *supra* note 12, at 517-18.

50. *See infra* notes 129-131 and accompanying text.

51. *See generally* Elizabeth A. Kitsis & Robert H. Shmerling, *Ethics Forum: Electronic Health Records Raise Concerns About Physician-Patient Relationship*, THE RHEUMATOLOGIST (Oct. 2014), http://www.the-rheumatologist.org/details/article/6808071/Ethics_Forum_Electronic_Health_Records_Raise_Concerns_about_Physician-Patient_Re.html; *see also* ACR Subcommittee on Health Info. Tech., *Electronic Health Records Present Communication Challenges for Physicians*, THE RHEUMATOLOGIST (Oct. 2014), http://www.the-rheumatologist.org/details/article/6807881/Electronic_Health_Records_Present_Communication_Challenges_for_Physicians.html.

52. *See* 45 C.F.R. § 164.520 (2014).

53. *Id.*

affirmative action to exclude their data from the exchange.[54] Alternatively, a few HIOs have adopted an "opt-in system," where patients must be notified and then must give affirmative, written authorization before their information may be exchanged.[55] Both systems require patient knowledge and consent and in order to gain patient consent, the patient must trust the HIO and believe in its value.

In addition to trust, participants need to believe that the benefits outweigh the costs. This means that they need to believe the HIO will add significant value to health organizations—either to their bottom-line, or to improved quality of care—ultimately outweighing the implementation costs, the sharp learning curves, and potential liability risks. Currently, providers are hesitant to take on the additional risk without assurance of the value in HIOs.[56] Particularly, the inclusion of all patients and participants presents a potential limitation on the value of an HIO. Value can only be derived if most patients are willing to participate and all providers (physicians, pharmacists, therapists) are contributing information.

2. Affordability

Implementing an HIO involves substantial upfront costs, both direct and indirect.[57] Before an HIO can be established, the health industry needs to implement the necessary infrastructure. To establish this infrastructure, every provider, provider group, hospital, clinic, pharmacy, and so forth, needs to implement its own EHR system. Only after such entities have an EHR system can HIOs facilitate the communication between them. Implementing the infrastructure, however, is extremely expensive. For example, the federal government estimates the cost of installing an EHR system ranges from $15,000 to $70,000 per provider.[58] Besides the direct costs of implementing an EHR system, organizations suffer from indirect costs caused by a decrease in

54. *See generally The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Individual Choice*, U.S. DEP'T HEALTH & HUMAN SERVS. 2-5, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf (last visited Apr. 28, 2015).

55. *See* BELLA ZAGHI, ECONNECT POLICY ADVISORY GROUP, "TO OPT IN OR NOT? THAT IS THE QUESTION": EVALUATING THE OPT IN CONSENT OPTION WITH THE CALIFORNIA HEALTH EXCHANGE, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY 2-3 (2011), *available at* http://www.himss.org/files/HIMSSorg/content/files/Line%2011%20-%20HIE%20Case%20Study%20Opt%20in%20Vs%20Opt%20Out%20Consent%20Options.pdf.

56. *See generally* Alder-Milstein et al., *supra* note 48, at 1491.

57. *See* Gold et al., *supra* note 12, at 515.

58. *How Much Is This Going to Cost Me?*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/faqs/how-much-going-cost-me (last visited Feb. 23, 2014). Additionally, Michigan estimates that to set up an EHR system in a physician's office, on average, will cost $33,000 in upfront costs and an additional $4,000 per year. *Id.*

productivity while providers learn and adapt to the new system.[59] One study estimates a provider's productivity decreases by twenty percent in the first month after implementing the EHR system.[60] Moreover, in addition to the learning curve, physicians complain they spend more time inputting data into the EHR system than they do with patients.[61] As a result, they see fewer patients, causing a decrease in revenue.[62] Since costs are substantial and all upfront, many providers cannot afford to establish an EHR system, meaning there are fewer organizations that can connect with an HIO.

In addition to the substantial cost of implementing EHR systems, long-term financial sustainability remains a challenge for HIOs. One HIO estimated its operating costs at approximately $230,000 per month.[63] Currently, many HIOs plan to charge participants prescription and transaction fees for using the services of an HIO.[64] Thus, for an HIO to remain sustainable, there must be enough participants and organizations willing and able to pay such fees. So far, HIOs have faced hesitation from organizations, particularly providers.[65]

3. Technical Concerns: Product Availability and Practice Integration

While the philosophy behind HIOs is sound, many technical barriers still exist. For one, EHR implementation is not widespread, especially within small practices.[66] As a result, there needs to be ONC-approved EHR software that is

59. *See* Gold et al., *supra* note 12, at 515. The costs include hardware, such as servers, computers, and printers; EHR software; implementation assistance, such as an IT contractor and an attorney; workforce training; and network fees and maintenance, such as making sure it continuously meets developing national standards. *See* Neil S. Fleming et al., *The Financial and Nonfinancial Costs of Implementing Electronic Health Records In Primary Care Practices*, 30 HEALTH AFF. 481, 485-87 (2011).

60. Nir Menachemi & Robert G. Brooks, *Reviewing the Benefits and Costs of Electronic Health Records and Associated Patient Safety Technologies*, 30 J. MED. SYS. 159, 162 (2006). *See also* Alex Ruoff, *Health Center Control Networks, Safety Net Providers Struggling with EHR Costs*, HEALTH IT L. & INDUSTRY REP. (BNA), Feb 3, 2014, at 8-9 (finding that one health center reported a loss of $900,000 in revenues due to decreases in productivity).

61. *See* Ben Guarino, *Seeking Satisfaction with EHRs*, ANESTHESIOLOGY NEWS (June 2014), http://www.anesthesiologynews.com/ViewArticle.aspx?d=Technology&d_id=8&i=June+2014&i_id=1068&a_id=27572.

62. *EHR Benefits and Drawbacks*, *supra* note 33, at 52.

63. Ben Fischer, *D.C. Health Information Exchange Future in Doubt After Shutdown*, WASH. BUS. J. (Nov. 4, 2011), http://www.bizjournals.com/washington/print-edition/2011/11/04/dc-health-information-exchange.html?page=all.

64. *See* Alex Ruoff, *Public HIE Executives, ONC Refute Claims of Diminishing Health Data Exchange Market*, 6 HEALTH IT L. & INDUSTRY REP. (BNA), Feb. 3, 2014, at 4 [hereinafter *ONC Refute Claims*].

65. *See* Alder-Milstein, et al., *supra* note 48, at 1491 (finding that fewer than a quarter of HIOs could cover its operational cost from revenue collected by participants).

66. Gold et al., *supra* note 12, at 516.

trusted by providers and that meets their needs.[67] Historically, EHR designers focused on the needs of large provider systems and did not address the needs of small, office-based practices.[68] In fact, some of the larger EHR systems, such as EPIC, will not license to small community hospitals, claiming these hospitals may not have the resources to run the system properly.[69] This leaves smaller hospitals with the option of contracting with larger hospitals to sublicense and facilitate its EHR system. Other small to medium practices implemented expensive EHRs that did not perform critical functions of their practice,[70] such as clinical management, and did not address their patients' diverse needs, such as mental health issues. Historically, there has been an overall lack of knowledge, choice, and product variation in EHR systems, which has left providers with expensive systems that are resource-intensive, and may or may not fulfill the actual objectives of EHRs.

The HITECH Act attempts to address this by issuing certification standards to assist providers in choosing appropriate systems.[71] However, few EHR designers are seeking certification.[72] This becomes problematic because it decreases the supply and increases hesitation from providers, who fear that with evolving health technology, they could be implementing an expensive system that will become useless before they ever see a return on their investment.[73] Particularly, providers fear that EHR designers will not update the technology to meet the next stage in Meaningful Use (MU) requirements.[74] This would cause providers to fall out of MU-compliance, resulting in the forfeiture of substantial federal payments and risk of possible payment reductions.[75] This fear may prevent providers from implementing the infrastructure needed to participate in an HIO.

Additionally, once participants implement an EHR system, then integrating the technology into providers' daily practice becomes a barrier.[76] Individuals must be trained and actually utilize the EHR system for the system to work. This takes time and results in decreased revenue, which is often met with

67. *Id.*

68. *Id.*

69. *See* Helen Gregg, *10 Things to Know About Epic*, BECKER'S HOSPITAL REV. (April 17, 2014), http://www.beckershospitalreview.com/lists/10-things-to-know-about-epic.html.

70. *See generally* MARK W. FRIEDBERG ET AL., RAND CORP., FACTORS AFFECTING PHYSICIANS PROFESSIONAL SATISFACTION AND THEIR IMPLICATIONS FOR PATIENT CARE, HEALTH SYSTEMS, AND HEALTH POLICY 38 (2013).

71. Gold et al., *supra* note 12 at 517.

72. Alex Ruoff, *CCHIT Announces End to Certification Program, Says Market No Longer Profitable*, 6 HEALTH IT L. & INDUSTRY REP. (BNA), Feb. 3, 2014, at 6-7.

73. *See* Gold et. al, *supra* note 12, at 517.

74. *See generally* Blair Butterfield, *What Physicians Want in an EHR*, 83 J. AM. HEALTH INFO. MGMT. ASS'N 44 *passim* (2012).

75. *See infra* Part III, B.3.

76. Gold et al., *supra* note 12, at 517.

frustration and resistance,[77] reducing participants' willingness to adopt the necessary infrastructure to support an HIE. Furthermore, studies show that among providers who have implemented an EHR system, many are not using all the functions of the system.[78] For HIOs to succeed, providers need to utilize the full capacity of their EHR system because HIOs can only facilitate an HIE with information from the participants' EHR system. Therefore, it is critical that all information is within the system so that the HIO can fulfill its purpose and provide participants with complete, accurate, and timely information. This cannot happen if HIOs do not have access to all the information. Moreover, the value of HIOs decreases if some information remains in paper form, because the patient file would be incomplete and the system would remain fragmented. Thus, providers could not trust the completeness or accuracy of the information provided to them through the exchange.

III. FEDERAL INTERVENTIONS

Recognizing the barriers prohibiting the implementation of HIOs, the federal government attempts to assist the development of HIOs in two primary ways. First, the federal government hopes to increase trust in HIOs by strengthening HIPAA's Privacy and Security Rules. Second, to reduce the initial implementation costs and provide technical assistance, the federal government is providing financial assistance and incentives for the development and implementation of HIEs and health IT.

A. HIPAA: New Privacy and Security Regulations

1. Introduction to HIPAA

HIPAA, enacted in 1996, was codified under various sections of the U.S. Code.[79] It addresses numerous aspects of health care including health insurance coverage,[80] insurance reform,[81] health care fraud,[82] health care information,[83] and taxation.[84]

HIPAA's most well-known provisions are the Administrative Simplification provisions, which center on the governance of Protected Health Information (PHI).[85] These provisions establish national standards for the use

77. *See supra* notes 59-60.

78. *See infra* notes 237-241 and accompanying text.

79. MELANIE D. BRAGG, HIPPA FOR THE GENERAL PRACTITIONER 3 (2009).

80. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936, tit. I (1996).

81. Health Insurance Portability and Accountability Act of 1996 tit. IV.

82. Health Insurance Portability and Accountability Act of 1996 tit. II.

83. *Id.*

84. Health Insurance Portability and Accountability Act of 1996 tit. III.

85. MARGRET AMATAYKUL, HANDBOOK FOR HIPAA-HITECH SECURITY 18 (2013).

of electronic health information.[86] The goal of the Administrative Simplification provisions is to improve the efficiency and effectiveness of the health care system by encouraging the use of health IT.[87] The Act intended to accomplish this goal by reducing the administrative burden associated with manually processing enrollment, eligibility, and payment.[88] The Administrative Simplification provisions consist of four governing rules that focus on: (1) transactions and code standards, (2) identifier standards, (3) privacy standards, and (4) security standards.[89] In addition to the Administrative Simplification provisions, HIPAA includes an enforcement section giving the Office of Civil Rights (OCR) the authority to investigate and impose civil penalties for failing to comply with the Administrative Simplification provisions.[90] Other commentary addresses the first two rules. This paper addresses the last two rules and the enforcement provisions, both of which were modified by the HITECH Act and propose possible implications for HIOs.

2. Overview and Scope of HIPAA

HIPAA is limited in scope with regards to the type of information the rules protect and to whom the rules apply. HIPAA protects PHI,[91] which is defined as individual identifiable health information "transmitted by electronic media, maintained in electronic media, and/or transmitted or maintained in any other form or medium."[92] This includes information transmitted orally and on paper.[93] Individual identifiable health information is health information collected from an individual that is created, held, or received by a covered entity, and "relates to the past, present or future physical or mental health or condition of an individual; [to] the provision of health care to an individual; or [to] the past, present, or future payment from the provision of health care to an individual."[94] The information must either identify the individual or there must

86. *Id.*

87. *Id.*

88. JUNE M. SULLIVAN, HIPPA: A PRACTICAL GUIDE TO THE PRIVACY AND SECURITY OF HEALTH DATA xiii (2004).

89. BRAGG, *supra* note 79, at 11.

90. AMATAYAKUL, *supra* note 85, at 12-13.

91. SULLIVAN, *supra* note 88, at 5.

92. 45 C.F.R § 160.103 (2013). PHI excludes individual identifiable health information in educational records covered by the Family Education Rights and Privacy Act, other records covered by 20 U.S.C. 1232g(a)(4)(B)(iv), records held by a covered entity in its role as employer, and individually identifiable health information regarding a person who has been deceased for more than fifty years. *Id*.

93. OFFICE OF CIVIL RIGHTS, U.S. DEP'T HEALTH & HUMAN SERVS., SUMMARY OF HIPPA PRIVACY RULE: HIPAA COMPLIANCE ASSISTANCE 3 (2003) [hereinafter HIPAA COMPLIANCE ASSISTANCE].

94. 45 C.F.R § 160.103 (2014).

be a reasonable belief that the information could identify the individual.[95] Individual identifiers include, but are not limited to, name, address, date of birth, and social security number.[96] Therefore, HIPAA does not regulate information that cannot be traced back to a particular person, nor does it protect health information shared outside the health care system, such as information exchanged between relatives in a social setting.[97] HIPAA also provides further protection for electronic Protected Health Information (e-PHI), which is PHI transmitted by electronic media or maintained in electronic media.[98] Providing additional protection for e-PHI promotes the legislation's purpose of encouraging and facilitating the use of health IT.

Before the HITECH Act, HIPAA only applied to covered entities, meaning that if an organization was not a covered entity it was not within the scope of the law and thus, did not need to follow HIPAA requirements.[99] Covered entities include health plans, health care clearinghouses, and health care providers who transmit any health-related information electronically, to perform a transaction covered by HIPAA's Administrative Simplification provisions.[100] Therefore, if a provider only performs transactions through paper formats, the provider is not subject to HIPAA.[101] However, if the provider transmits any PHI electronically, in accordance with HIPAA's Administrative Simplification rules, then the provider is classified as a covered entity and any PHI, even PHI conveyed verbally or kept in paper form, is protected by HIPAA.

95. *Id.*

96. *See* SULLIVAN, *supra* note 88, at 5.

97. *Id*.

98. John Christiansen, *Scope and Applicability of the Security Rule, in* A Guide to HIPAA Security and the Law 14-15 (Stephen S. Wu ed., 2007).

99. *See* SULLIVAN, *supra* note 88, at 3. Under the old rule, HIPAA applied only to covered entities, but it required covered entities who shared information with business associates to enter a BAA, which required the business associate to give covered entities reassurance that they would properly protect PHI. Business associates were then contractually responsible for certain HIPAA provisions. HIPAA COMPLIANCE ASSISTANCE, *supra* note 93, at 2. The HITECH Act now imposes direct obligations on business associates for certain privacy and security provisions. *Key Laws and Regulations: Changes Relevant to the Markle Common Framework*, Markle, http://www.markle.org/health/markle-common-framework/connecting-professionals/key-laws-and-regulations#I (last visited Nov. 2, 2014) [hereinafter *Markle Framework*].

100. HIPAA COMPLIANCE ASSISTANCE, *supra* note 93, at 2. A provider transmits health-related information electronically to perform a transaction covered by HIPAA when: 1) they share health information electronically in support of financial or administrative responsibilities, including submitting health claims, authorizing referrals, or confirming status of enrollment or eligibility and 2) they transmit the health information according to the standard electronic format required by the Administrative Simplification Compliance Act. SULLIVAN, *supra* note 88, at 3.

101. SULLIVAN, *supra* note 88, at 4.

In addition to covered entities, certain HIPAA provisions apply to a second category of entities called business associates. A business associate is an entity who regularly creates, receives, maintains, or transmits PHI on behalf of a covered entity in order to accomplish or help accomplish a function or activity regulated under HIPAA.[102] Such activities include claims processing, data analysis, utilization review, patient safety activities, billing, and practice management.[103] Examples of business associates include lawyers, actuaries, accountants, consultants, administrators, financial advisors, and accreditors who are not a part of the covered entity's workforce.[104]

The category of business associates existed prior to the HITECH Act, but the Act expanded the definition of business associates to include "health information organization[s], E-prescribing Gateway[s], [and] other person that provides data transmission services with respect to protected health information to a covered entity and [who] requires access on a routine basis to such protected health information."[105] This expansion makes it clear that HIOs are business associates and are subject to HIPAA and its new enforcement mechanisms.

In addition to expanding the definition of business associates, the HITECH Act makes business associates directly liable for impermissible usage or disclosure of PHI and subjects them to OCR-oversight.[106] Prior to the HITECH Act, business associates were only responsible for complying with their business associate agreement (BAA)—a contract between the business associate and the covered entity.[107] Therefore, business associates were only liable to covered entities for a contract breach and were not subject to OCR-oversight. Put another way, prior to the HITECH Act, the Agency could not go after business associates—now it can. Additionally, business associates must now assist with investigations conducted by the OCR to ensure compliance and are also subject to civil and possible criminal penalties for non-compliance.[108]

3. Privacy Rule and Business Associates

The HIPAA Privacy Rule governs the circumstances under which covered entities may use or disclose PHI and defines an individual's right to access,

102. 45 C.F.R. § 160.103 (2013).

103. *Business Associate*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last visited Nov. 2, 2014).

104. *Id.*

105. 45 C.F.R. § 160.103 (2014).

106. *See infra* Part III, A.7.

107. Megan Bradshaw & Benjamin K. Hoover, *Not So Hip?: The Expanded Burdens on and Consequences to Law Firms as Business Associates Under HITECH Modifications to HIPAA*, 13 RICH. J.L. & PUB. INT. 313, 320 (2010) [hereinafter *Not So Hip*].

108. *See infra* Part III, A.7.

amend, and control their PHI.[109] The Rule gives consumers the right to control the inappropriate use of their health information, while at the same time permitting health information to be shared for a legitimate purpose.[110] The Rule balances an individual's interest in keeping their health information private and confidential, with the needs of health care professionals and others to efficiently share information and thus, improve productivity, patient safety, and quality of care.[111]

Traditionally, the Privacy Rule applied to covered entities and protected PHI.[112] The Rule outlines permissible usages and disclosures of PHI, for which covered entities do not need prior consent, although they do need to inform patients their information may be used for these purposes.[113] Additionally, the Privacy Rule outlines the requirements for authorizing usages and disclosures, for which covered entities must seek prior consent.[114] The Rule also limits both permissible and authorized usages and disclosures to the extent necessary to carry out the request and no more.[115] For instance, if a cardiologist requests a copy of a patient's latest echocardiogram from another provider, the other provider may only send the latest echocardiogram and may not send the patient's entire medical record, unless the provider can justify why the cardiologist reasonably needed the entire record to treat the patient's heart condition. Moreover, the Privacy Rule establishes flexible and scalable guidelines for covered entities to ensure compliance.[116] Specifically, the Rule requires covered entities to develop, implement, and maintain reasonable and appropriate administrative, physical, and technical safeguards.[117] The guidelines related to these safeguards are sometimes referred to as the "mini" Security Rule.[118]

Under the HITECH Act, the Privacy Rule applies to business associates to the extent defined by their BAA.[119] This means that business associates are

109. SULLIVAN, *supra* note 88, at 2.

110. BRAGG, *supra* note 79, at 18.

111. HIPAA COMPLIANCE ASSISTANCE, *supra* note 93, at 1.

112. SULLIVAN, *supra* note 88, at 69.

113. HIPAA COMPLIANCE ASSISTANCE, *supra* note 93, at 8.

114. *Id.* at 9.

115. *Id.* at 10.

116. *Id.* at 1.

117. *See* Francoise Gilbert, *HIPAA Privacy and Security*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 10-12 (Stephen S. Wu ed., 2007).

118. *See* Steven Fleisher, *Background and History of HIPAA*, *in* A GUIDE TO HIPAA SECURITY AND THE LAW 7 (Stephen S. Wu ed., 2007).

119. *Not So Hip*, *supra* note 107, at 321. Failing to enter into a BAA does not release the organization or person who maintains, transmits, creates, or receives PHI from responsibilities under the Privacy Rule. The rule requires that a BAA be in writing and failing to enter one is a violation by the business associate in and of itself. *See generally* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information

required to comply with certain aspects of the Privacy Rule.[120] Specifically, where the covered entity delegates responsibilities to a business associate, the business associate must perform its responsibility in a way that provides at least as much privacy protection as the covered entity would have needed to provide under the Privacy Rule, if it had performed the responsibility itself.[121] This means that the Privacy Rule applies to business associates to the extent it is performing tasks regulated under the Privacy Rule. Therefore, the provisions a business associate is obligated to follow depend on the scope of the business associate's responsibilities as they relate to the creation, reception, maintenance, or transmission of PHI.

A BAA, in part, allows covered entities to contract with another organization or person to perform specific functions more efficiently, while providing protection for the downstream use of PHI.[122] However, the BAA must include several implementation specifications. First, it must be in writing and give "satisfactory assurance that the business associate will appropriately safeguard" PHI.[123] Second, the contract must specify both the permitted and required usage and disclosure of PHI.[124] This establishes how and for what purpose the business associate may use or disclose PHI. The contract may place restrictions on the business associate's usage of PHI beyond what the Privacy Rule places on the covered entity's usage of PHI, but the contract may not expand a business associate's usage of PHI.[125] Third, the BAA must require business associates to assist with any investigation conducted by the Secretary of the Department of Health and Human Services (HHS) to determine compliance, by ensuring all internal practice policies, books, and records relating to the usage and disclosure of PHI are available to the Secretary.[126] Additionally, under the BAA, business associates must comply with the Security Rule and report any non-compliance, whether intentional or accidental, under either the Privacy Rule or Security Rule, to the covered entity.[127] Lastly, as with all contracts, the BAA may be terminated if the business associate materially breaches the contract, at which time all PHI must be returned or destroyed.[128]

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, 5570-72 (Jan. 25, 2013). [hereinafter HIPAA Modification Final Rule].

120. HIPAA Modification Final Rule, *supra* note 119, at 5573.

121. 45 C.F.R. § 164.504(e)(2)(i) (2014); 45 C.F.R. § 164.504(e)(2)(ii)(E-H).

122. *See* HIPAA Modification Final Rule, *supra* note 119, at 5573.

123. 45 C.F.R. § 164.504(e)(l)(iii); 45 C.F.R. § 164.502(e) (2014).

124. 45 C.F.R. § 164.504(e)(2)(i)(A)-(B).

125. *Id.*

126. 45 C.F.R. § 164.504(e)(2)(ii)(I).

127. *See* 45 C.F.R. § 164.504(e)(2)(ii)(B)-(C).

128. 45 C.F.R. § 164.504(e)(2)(ii)(J)-(e)(2)(iii).

The BAA is essential because it defines a contractual relationship between the covered entity and business associate by setting clear expectations and limitations for both parties.[129] The contractual relationship gives the covered entity control over the business associate by specifically stating what type of information the business associate will be privileged to access, how the information is to be used, and what measures should be implemented to protect the information.[130] This control reassures the covered entities that they will maintain compliance with HIPAA, even if they delegate some responsibility to business associates.

4. Privacy Rule and Business Associates' Impact on HIOs

Because the HITECT Act includes HIOs under the definition of a business associate, under the Privacy Rule, HIOs must enter into BAAs with entities that wish to utilize the services of the HIO. The reassurance of control through the BAA is crucial for HIOs because they cannot develop without the buy-in and support of providers and other covered entities.[131] If covered entities believe that HIOs cannot satisfactorily secure the integrity and confidentiality of PHI, or that participation will increase the covered entities' liability, then they will not participate in the system. Therefore, this assurance that the HIO will comply with the relevant Privacy Rule provisions, as defined by the contract, is the first necessary step in convincing covered entities that participation in the HIO is safe.

Covered entities receive additional assurance because the BAA states that the business associate will comply with any compliance investigation conducted by the Secretary of HHS.[132] Thus, the BAA gives the Secretary the ability to directly monitor HIOs' compliance. This additional mechanism should further reduce apprehension of entering into BAAs with HIOs because it gives covered entities another opportunity to ensure compliance. Therefore, trust between HIOs and participating parties' covered entities is built and supported through its contractual relationship, defined by the BAA.

BAAs are also essential because they build trust between the HIO and the person whose information is being shared, by ensuring all users who legitimately have access to PHI will implement the necessary security measures, as required under the BAA. Trust between patients and HIOs is necessary in order to attain patients' consent to share their information within

129. *See generally* HIPAA Modification Final Rule, *supra* note 119, at 5599.

130. *See generally Business Associate Contracts*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last modified Apr. 3, 2003) (describing what needs to be in a business associates agreement); *see also* FRAMEWORK INTRODUCTION, *supra* note 22, at 3.

131. *See supra* Part II.B.1.

132. *See* 45 C.F.R. § 164.504(e)(2)(ii)(I).

the HIO system. This trust can be developed through confidence in the competency and reliability of the HIO.[133] The BAA attempts to build this confidence by reducing areas of possible vulnerability. The HITECH Act recognizes that security breaches can occur anywhere along the flow of information and thus, the Act tries to protect information by requiring everyone, including business associates and subcontractors, provide assurance that they will protect and secure all PHI.[134]

Recent events regarding the security of debit cards illustrate the importance of addressing the entire stream in which information flows. For example, in the winter of 2013-2014, hundreds of people had their debit card information stolen after hackers installed malware inside the software of a retailer's clearinghouse.[135] While banks and securities have long received pressure to implement top-of-the-line security measures, little attention has focused on security measures for third parties who use the information.[136] The new requirements related to business associates under the Act attempt to correct the third party oversight observed in financial security through the BAA. Because security measures are required along the flow of information, people will have more confidence in HIOs and will be more willing to consent, ultimately facilitating the flow of their information across the health system.

However, others argue that BAAs are detrimental because they increase costs.[137] HHS predicts that changes in the new requirements for BAAs could cost business associates collectively between $21 million and $42 million.[138] These costs are primarily associated with entities who are already business associates under their contract with covered entities and who need to modify their existing policies in order to comply with the new requirements.[139] However, HIOs are unlikely to experience any additional costs because they are primarily in the developmental stage and regardless of the new requirement, by the very nature of HIOs, they would need to engage with

133. *See* Deven McGraw et al., *Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange*, 28 HEALTH AFF. 416, 417 (2009).

134. *See generally* HIPAA Modification Final Rule, *supra* note 119, at 5572-74. The BAA mandates that all organizations who contract with third parties to create, receive, maintain, or transmit PHI seek adequate assurance from the organization they are contracting with that they implement adequate security measures. Additionally, organizations may be liable for any breaches by contractual parties under federal common law of agency. *Id.*

135. *See* Cheyenne Hopkins & Todd Shields, *Target Card Breaches Open New Front in Old Battle With Bankers*, BLOOMBERG NEWS (Jan. 31, 2014), http://www.bloomberg.com/news/2014-01-31/target-card-breaches-open-new-front-in-old-battle-with-bankers.html.

136. *See id.*

137. *See generally* Jonathan P. Tomes, *The Law of Unintended (Financial) Consequences: The Expansion of HIPAA Business Associate Liability*, 39 J. HEALTH CARE FIN., Summer 2013, at 28-35.

138. HIPAA Modification Final Rule, *supra* note 119, at 5567.

139. *See id.*

covered entities to define the scope of their relationship and develop existing policies and procedures. Therefore, the costs associated with entering into a BAA are inherent in the creation of HIOs, and furthermore, template BAAs are available online for assistance.[140] Moreover, while every party must agree to the BAA, the HIOs do not need to have a separate BAA with each covered entity.[141] Rather, the HIO can create a standard BAA to which all participating parties agree.[142] Having the ability to enter into a single BAA will reduce costs and, therefore, make the BAA requirement more financially possible.

5. Security Rule

Infrastructure is essential when it comes to ensuring the confidentiality and integrity of e-PHI. The HIPAA Security Rule creates this basic infrastructure by establishing standards, as well as mechanisms to achieve those standards.[143] The Rule only protects e-PHI, meaning it does not cover PHI maintained in paper format or verbal communication.[144] Significantly, therefore, it is narrower in scope than the Privacy Rule, which protects all forms of PHI.[145] However, like the Privacy Rule, the Security Rule traditionally applied solely to covered entities.[146] The HITECH Act, as it did with the Privacy Rule, expands the applicability of the Security Rule to include business associates.[147] Therefore, business associates now must adopt the basic infrastructure built by the Security Rule.

The Security Rule creates an infrastructure by breaking down its goals into different components and then breaking those components down into narrower issues. The Rule recognizes three large, vulnerable areas in which security breaches occur including: (1) the workforce, (2) the physical infrastructure and environment, and (3) technology. Accordingly, the Rule requires organizations to implement three types of safeguards categorized as: (1) administrative,[148]

140. *See, e.g.*, *Business Associates and Health Information Exchanges*, HEALTHCARE INFO. & MGMT. SYS. SOC'Y, http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=1715&navItemNumber=21230 (last visited Jan. 20, 2014).

141. FRAMEWORK INTRODUCTION, *supra* note 22, at 3.

142. *Id.*

143. *See generally* 45 C.F.R. § 164.306(a), (d) (2014).

144. Christiansen, *supra* note 98, at 15-16.

145. *See id*. at 16.

146. *See Summary of HIPAA Security Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited Feb. 12, 2014) [hereinafter *Security Rule Summary*].

147. *Key Laws and Regulation: Changes Relevant to the Markle Common Framework*, MARKLE (Apr. 2012), http://www.markle.org/health/markle-common-framework/connecting-professionals/key-laws-and-regulations#I.

148. 45 C.F.R. § 164.308 (2014). The administrative safeguard focuses on security management and the workforce. In addressing security management, an organization must appoint a security official to be responsible for ensuring proper development and implementation

physical,[149] and technical.[150] These safeguards are further broken down into standards that address specific issues facing each vulnerable area. Some of

of security measures. 45 C.F.R. § 164.308(a)(2). Additionally to meet the standard of "prevent[ing], detect[ing], contain[ing] and correct[ing] security violations", the entity must conduct a risk analysis and implement measures to diminish risks and vulnerabilities identified by the risk analysis. 45 C.F.R.§ 164.308(a)(1). In order to detect or correct security violations in the future, entities must regularly review its systematic activities by conducting review mechanisms, such as audits, or reviewing security violation tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D). Further, organizations must implement procedures to respond and report security incidents. 45 C.F.R. § 164.308(a)(6)(ii). These measures must be able to identify incidents, mitigate the harm caused by the incident, and record all incidents. *Id*. Lastly, all procedures and policies must be continuously reviewed and updated in light of environmental and operational changes. 45 C.F.R. § 164.308(a)(8).

Administrative safeguards addressing the management of the workforce focus on policies and procedures addressing issues around access of e-PHI and awareness of security measures. 45 C.F.R. § 164.308(a)(3-5). Organizations must address who gets access and the scope of their access. *Id*. Additionally, entities must implement a policy addressing modifications to a person's authorized access, including what happens if an employee with access is terminated. 45 C.F.R. § 164.308(a)(3)(ii). Further, policies need to outline sanctions for employees who fail to comply with security policies and procedures. 45 C.F.R. § 164.308(a)(1)(ii)(C). Moreover, entities must provide training and awareness to the entire workforce. 45 C.F.R. § 164.308(a)(5)(i). This includes providing the workforce with security updates and implementing: 1) software to detect and protect against unauthorized software, 2) a login monitoring system, and 3) password management safeguards which creates procedures for creating and changing passwords.

149. 45 C.F.R. § 164.310 (2014). The physical safeguard rule focuses on the security of the facility where the e-PHI is accessed and stored. 45 C.F.R. § 164.310(a). Specifically, entities need to establish and implement policies to safeguard facilities and equipment from environmental and hazardous threats, theft and tampering, and to control persons' access to the facilities. 45 C.F.R. §§ 164.310(a)(2)(i-iii). Additionally, entities may have to maintain records of repairs and or modifications to the physical component of security including hardware, locks, and building. 45 C.F.R. §§ 164.310(a)(2)(iv). Moreover, the rule lays out standards for workstations requiring the entity to implement policies and procedures that outline the task and manner that need to be performed and the specific work environments where e-PHI may be accessed. 45 C.F.R. § 164.310(b), (c). Workstation refers to electronic devices or electronic media. 45 C.F.R. § 164.304 (2014). Lastly, the rule governs the use, re-use, or disposal of devices and electronic media that contain e-PHI. 45 C.F.R. § 164.310(d). The rule specifies the importance of creating policies designed to track the whereabouts of the devices and electronic media that store e-PHI and the persons responsible for it and to store or back up an exact copy of e-PHI before any movement of equipment occurs. 45 C.F.R. § 164.310(d)(2)(i)-(iv).

150. 45 C.F.R. § 164.312 (2014). The technical safeguards focus on the technology itself and its ability to limit access to only those who are authorized, as well as its ability to track the use and activities of the health information system. *Id.* The rule also addresses the need for secure transmission of e-PHI and policies and procedures to ensure that e-PHI is not improperly modified. 45 C.F.R. § 164.312(e). A common implementation specification throughout the standards in the rule was the need for encryption and decryption software. *See, e.g.*, 45 C.F.R. § 164.312(a)(2)(iv). Other implementation specifications included automatic log off and unique identification indicator. 45 C.F.R. § 164.312(a)(2)(iii).

these standards are then further broken down into implementation specifications. These implementation specifications are methods necessary to meet the given standard. The Rule's structure gives organizations a starting point when considering how to best secure e-PHI and lays out the issues organizations need to address, rather than giving bright-line requirements.

The Rule's infrastructure is intentionally flexible and gives organizations a considerable amount of discretion in implementing each requirement. For instance, implementation specifications are either required or addressable.[151] While required provisions are mandatory, meaning that all organizations must implement the specification,[152] addressable implementation specifications are only mandatory where the specification is likely to contribute to the protection of e-PHI and the organization finds the specification reasonable and appropriate.[153] This means that to some extent, the organization has the opportunity to weigh the costs of implementing the specification against its potential benefits.[154] This flexibility is necessary, considering the differences in the types and sizes of entities covered by the Rule. Each organization is different and therefore, has different security concerns. For instance, a hospital employs numerous employees with various types of responsibilities, making it necessary for them to have detailed administrative safeguards to address issues surrounding their large, diverse workforce. While HIOs have far fewer employees than hospitals, they rely heavily on technology, making it crucial to design detailed technical safeguards.[155] The flexibility in the Rule recognizes this diversity and allows organizations to customize safeguards to meet their individual security needs, while still requiring the organizations to consider all possible areas of vulnerability.[156] This flexibility is critical in promoting the Rule's intent of ensuring the confidentiality, integrity, and availability of e-PHI, without over-burdening entities with obligations that would prohibit all-but-the huge health institutions from using e-PHI.[157]

6. Security Rule's Impact on HIOs

The Security Rule's standards and implementation specifications are particularly important for the development of HIOs because they develop a

151. 45 C.F.R. § 164.306(d)(1) (2014).

152. 45 C.F.R. § 164.306(d)(2).

153. 45 C.F.R. § 164.306(d)(3).

154. Factors an organization may consider in determining the reasonableness and appropriateness are: 1) the size and complexity of the entity, 2) the technical infrastructure of the entity's security capabilities, 3) the cost of the security measure, and 4) the probability the measure will reduce potential risks and vulnerabilities to e-PHI. 45 C.F.R. § 164.306(b).

155. *See* U.S. DEP'T HEALTH & HUMAN SERVS., PRIVACY AND SECURITY FRAMEWORK: SAFEGUARDS 1-2 (2008) [hereinafter FRAMEWORK SAFEGUARDS].

156. *See generally* 45 C.F.R. § 164.306.

157. *See* HIPAA Modification Final Rule, *supra* note 119, at 5566, 5589, 5591.

framework for an organization, on how to secure the confidentiality and integrity of e-PHI.[158] This basic infrastructure is particularly important for HIOs because they are in the early stages of development and are currently in the process of trying to develop mechanisms to secure e-PHI. While the Rule only gives broad expectations and leaves substantial discretion to the organization, it does outline the large issues that need to be addressed and creates a checklist of policies and procedures that are needed to create a secure infrastructure.[159] HIOs can, in return, use this checklist to ensure all large security issues are addressed. Certainly, the Rule does not provide HIOs with a comprehensive plan to secure e-PHI, nor does it answer all questions regarding the best security practices. However, it does give HIOs a launching pad on which to implement the policies and procedures needed to secure e-PHI. By breaking down the "security question" into three parts—administrative, physical, and technical—and then further breaking each of those parts into yet smaller questions through standards and specifications, the Rule makes the seemingly impossible task of securing individuals' e-PHI less-daunting. By no means is this a small task, but by providing the building blocks for such a system, the task of building it becomes more manageable, rather than simply trying to accomplish the task from scratch. Furthermore, since the structure and basic issues are laid out, organizations can spend more time on the substance of the policies.

HIOs are indeed using the structure of HIPAA's Security Rule to frame and design their security policies and procedures. The Washington DC HIO, for example, used the Security Rule's framework to create its *District of Columbia Health Exchange Policy and Procedure Manual* (*Manual*).[160] The *Manual* divides the Security Rule into safeguards and then divides those sections into subsections, using the language within the safeguards' standards and implementation specifications.[161] The *Manual* even includes quotes from the HIPAA statute before it describes the policy.[162] Moreover, the *Manual* demonstrates how an HIO can model its structure after the Security Rule.

158. *See supra* notes 129-30 and accompanying text.

159. For example, the Administrative Safeguards address a security management process, security personnel, information access management, workforce training and management, and evaluation. *See Security Rule Summary*, *supra* note 146. The Physical Safeguards address facility access and control and workstation and device security. *Id*. The Technology Safeguards address access controls, audit controls, integrity controls, and transmission security. *Id*.

160. *See, e.g.*, DEP'T OF HEALTH CARE FIN., D.C., DISTRICT OF COLUMBIA HEALTH INFORMATION EXCHANGE POLICY AND PROCEDURE MANUAL: HIPAA PRIVACY & DIRECT PRIVACY POLICIES 3-4 (2012), *available at* http://dhcf.dc.gov/sites/default/files/dc/sites/dhcf/publication/attachments/DC%20HIE%20POL%20%20PRO-FINAL%2011-27-12_0.pdf.

161. *See id.* at 1-2.

162. *See id.* at 34.

7. Enforcement Mechanisms Against Business Associates

The HITECH Act provides more stringent enforcement against violations of the HIPAA Administrative Simplification provisions, including those caused by business associates.[163] Specifically, four mechanisms of enforcement are created under the Act: (1) the OCR may impose civil penalties,[164] (2) the Department of Justice (DOJ) may bring criminal charges,[165] (3) a state's Attorney General may bring a civil claim on behalf of one or more of its residents,[166] and (4) the OCR may conduct audits to determine covered entities' and business associates' compliance.[167] Note that there is no private cause of action created under federal law, meaning that an individual may not bring a HIPAA claim directly. However, state law may create a private right of action.[168]

The OCR may impose civil penalties against business associates.[169] Penalties vary depending on the business associate's level of culpability, determined by the law's four prescribed tiers.[170] The first tier, with penalties ranging from $100 to $50,000 per violation, applies to persons who did not know and could not have reasonably known of the violation.[171] The second tier, with penalties ranging from $1,000 to $50,000 per violation, applies to persons who violated a HIPAA Administrative Simplification provision due to reasonable cause and not willful neglect.[172] The third tier, with penalties ranging from $10,000 to $50,000 per violation, applies to persons who willfully neglected to comply with an Administrative Simplification provision,

163. *See Not so Hip*, *supra* note 107, at 322-24, 334.

164. 42 U.S.C § 1320d-5(a) (2012). *See also How OCR Enforces the HIPAA Privacy & Security Rules*, U.S DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html (lasted visited Feb. 18, 2014) [hereinafter *OCR Enforcement*].

165. 42 U.S.C § 1320d-6 (2012). *See also OCR Enforcement*, *supra* note 164 (stating the OCR may refer the complaint to the DOJ to examine and prosecute criminal provisions of HIPAA).

166. 42 U.S.C § 1320d-5(d).

167. *See HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html (last visited Feb. 18, 2014).

168. *See Not so Hip*, *supra* note 107, at 324. *See generally* 42 U.S.C § 1320d-5(d) (2012).

169. *Not so Hip*, *supra* note 107, at 333-34.

170. *See generally* 45 C.F.R. § 160.402 (2014).

171. 45 C.F.R. § 160.404(b)(2)(i)(A) (2014).

172. 45 C.F.R. § 160.404(b)(2)(ii). Reasonable cause is interpreted to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." 45 C.F.R § 160.401 (2014) (implying that reasonable cause violations occur where there is no conscious intent to violate HIPAA or reckless indifference to the violation).

but corrected the violation within thirty days.[173] Finally, the fourth tier, with a penalty of $50,000 per violation, applies to persons who did not correct willfully neglected violations.[174] Importantly, each penalty is assessed per violation, meaning that if the identical Administrative Simplification provision was violated multiple times (for instance, if a provider improperly disclosed PHI of multiple patients) the total fine could be exponentially greater.[175] However, while fines can be compounded, fines for a single violation are capped at $1.5 million annually.[176] Despite this cap, a person may receive a penalty greater than $1.5 million in a given year if the person violates different Administrative Simplification provisions.[177] For example, in 2011, the OCR issued a $4.3 million dollar fine to Cignet Health of Prince George's County, Maryland for failing to provide forty-one patients with a copy of their medical records and for failing to cooperate with the OCR's investigation of the complaints.[178]

While the OCR may impose large penalties, the OCR prefers to address violations through voluntary compliance, corrective actions, and resolution agreements.[179] In fact, Cignet's fine in 2011 was the first civil penalty the OCR ever issued,[180] demonstrating how the Agency exercises substantial discretion in assessing penalties.[181] The OCR explicitly stated that the "goal of enforcement is to ensure that violations do not reoccur without impeding

173. 45 C.F.R § 160.401. Willful neglect is defined as "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." *Id. See also* 45 C.F.R. § 160.404(b)(2)(iii).

174. 45 C.F.R § 160.404(b)(2)(iv).

175. HIPAA Modification Final Rule, *supra* note 119, at 5584.

176. *See, e.g.*, 45 C.F.R § 160.404(b)(2)(i)(B).

177. HIPAA Modification Final Rule, *supra* note 119, at 5584.

178. Dep't Health & Human Servs. v. Cignet Health, OCR Notice of Final Determination (Feb. 4, 2011), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cygnetpenaltyletter.pdf. *See also* Lena H. Sun, *Clinic Fined $4.3 Million for Failing to Provide Patients' Medical Records*, WASH. POST (Feb. 23, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207094.html.

179. Kendra Casey Plank, *BlueCross BlueShield Company Fined $6.8 Million in Connection With Data Breach*, HEALTH CARE DAILY REP. (BNA), Feb. 20, 2014, at 27-28. *See generally Case Examples and Resolution Agreements*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Nov. 1, 2014) (discussing various HIPAA violations the OCR has resolved).

180. Sun, *supra* note, 178.

181. HIPAA Modification Final Rule, *supra* note 119, at 558. *See* 45 C.F.R. § 160.408 (2013). In determining fines, the OCR may consider the nature and extent of the violation, the nature and extent of the harm caused by the violation, as well as other factors such as size and financial condition of the covered entity or business associate. HIPAA Modification Final Rule, *supra* note 119, at 5583.

access to care."[182] Thus, the OCR wants to ensure organizations follow the law—its goal is not to financially bankrupt organizations.

In addition to penalties imposed by the OCR, the state's Attorney General may bring a state civil claim against a business associate that violates the new law, in order to enjoin them from committing further violations, or to obtain damages on behalf of the state resident.[183] A state's Attorney General may seek a maximum fine of $25,000 for the violation of identical requirements or provisions in a given year.[184] However, if the state is successful, the court may award the state the costs associated with the action and reasonable attorney fees.[185] Moreover, the Secretary of HHS has the authority to intervene in the action, the right to be heard on all matters arising from the action, and the right to file an appeal on any action.[186]

Further, in particular cases where wrongful disclosures of PHI occur, individuals may be criminally charged. An individual, however, must knowingly use, obtain, or disclose PHI in violation of the law in order to be criminally liable.[187] Examples of criminal charges would include submitting fraudulent Medicare claims, or stealing a patient's PHI in order to use it against the patient in a legal proceeding.[188]

Lastly, business associates and covered entities now face periodic audits by the OCR. Audits are random and designed to sample the wide range of types and sizes of organizations.[189] They are designed to determine compliance, identify the best privacy and security practices, and discover risks and vulnerabilities.[190] While the audits may discover violations and could expose organizations to civil penalties, the intent of the audit is to provide technical

182. HIPAA Modification Final Rule, *supra* note 119, at 5585.

183. 42 U.S.C. § 1320d-5(d)(1) (2012).

184. 42 U.S.C. § 1320d-5(d)(2)(B).

185. 42 U.S.C. § 1320d-5(d)(3).

186. 42 U.S.C. § 1320d-5(d)(4).

187. 42 U.S.C. § 1320d-6(a) (2012).

188. *See* May L. Sethi, *United States: Criminal Liability for the Wrongful Use of Health Information HIPAA and More*, NUTTER MCCLENNEN & FISH LLP, http://www.mondaq.com/unitedstates/x/80212/Healthcare/Criminal+Liability+For+The+Wrongful+Use+Of+Health+Information+HIPAA+And+More (last modified May 28, 2009); *see also Not So Hip*, *supra* note 107, at 324-25.

189. *Audit Pilot Program*, U.S. DEP'T HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html (last visited Nov. 2, 2014) [hereinafter *Audit Pilot Program*]. *See* Richard B. Wagner, *Early Results from New HIPAA Audit Pilot Reveal Emphasis on Policy Documentation and Business Associate Agreements*, ABA HEALTH E-SOURCE, http://www.americanbar.org/newsletter/publications/aba_health_esource_home/aba_health_law_esource_0512_wagner.html (last modified May 2012).

190. *Auto Pilot Program*, *supra* note 189.

assistance and determine best practices, so the OCR can further help organizations improve their privacy and security protections.[191]

8. Enforcement Mechanisms' Impact on HIOs

The four enforcement mechanisms act as a double-edged sword for HIOs. On one side, the enforcement mechanisms increase potential liability and, thus, threaten the financial sustainability of the organization. If an HIO were to breach one or more of the requirements or provisions, the HIO would potentially be exposed to millions of dollars in fines from the federal government[192] and thousands of dollars in fines from state government. Considering many HIOs are struggling to even develop a sustainable financial plan,[193] there is little possibility that HIOs could pay such large penalties and remain viable. Rather, the organization would likely go bankrupt. Moreover, one such failure would destroy individuals' confidence and raise fears regarding such organizations, which would threaten the viability of HIOs around the country.

Furthermore, stricter enforcement mechanisms also impose potential reputational and financial risks for individuals who utilize the services of an HIO, which would decrease individuals' willingness to participate in an HIO. Trust is critical in the field of health care and providers fear that any HIPAA violation will create distrust between them and the patient.[194] Additionally, the enforcement mechanisms could increase the financial liability of persons who utilize the services of an HIO. Some providers fear that HIOs will grant them too much access to too much information, which would open them up to further malpractice liability. For example, they fear they could misdiagnose or mistreat a patient because they relied too heavily on untimely, inaccurate, and incomplete data accessed through the HIO.[195]

Moreover, it is uncertain whether people who utilize the services of an HIO will be liable for certain types of breaches within the HIO. While the HITECH Act makes HIOs, as business associates, directly liable for breaches, the regulations also make it explicitly clear that covered entities are liable for acts of their agents.[196] The issues then become whether HIOs are agents of the covered entity and whether the breach was within the scope of that agency.[197]

191. *Id.*

192. *See supra* notes 149-55 and accompanying text.

193. *See supra* Part II, B.2.

194. MCGOWAN ET AL., *supra* note 26, at 24.

195. *Id.* at 23-24; LARRY OZERAN & MARK R. ANDERSON, DO EHRS INCREASE LIABILITY 7-10 (2011), *available at* http://www.acgroup.org/images/2011_White_Paper_-_Do_EHRs_Increase_Liability.pdf.

196. HIPAA Modification Final Rule, *supra* note 119, at 5580.

197. *Id.* at 5581. Whether or not a business associate is an agent depends on the totality of the circumstances. *Id.* In assessing the totality of the circumstances, one should consider the type of

If HIOs are agents and the breach is within the scope of the agency, covered entities may be responsible for the breach and face substantial liability.[198] While this presents a legitimate fear for covered entities, the law also provides protection from unjust penalties by granting the Secretary the authority to waive any civil penalties if found excessive, relative to the violation.[199] Further, the Secretary may choose not to issue penalties where the organization corrects the violation in a reasonable time, given the nature and extent of the violation.[200] Thus, covered entities may protect themselves from liability associated with the potential agency theory by exercising reasonable diligence and making attempts to correct violations as soon as they become aware of them, regardless of whether they caused the breach. Protecting covered entities from potential liability is critical in encouraging stakeholders to participate in the system. However, just the fear of additional liability may create hesitation from stakeholders.[201] Thus, it would benefit HIOs if the OCR would clearly state that covered entities are not principles of the HIO.

On the other side of the sword, the enforcement mechanisms increase the legitimacy of HIOs by holding them accountable for any privacy breaches and thus, increasing providers' and other participants' willingness to enroll in an HIO. While the Privacy Rule sets out permissible, or in many cases impermissible, usages of PHI by HIOs,[202] and the Security Rule sets out the structural plan,[203] the enforcement mechanisms act as the project manager—ensuring both Rules are carried out effectively. The threat of large penalties creates incentives and assurance that parties faithfully carry out the Rules. Patients whose records are available through the HIO can take comfort in the fact that possible recovery for a breach is available, through action taken by their state Attorney General. Similarly, covered entities can take comfort in the fact that HIOs, as business associates, are independently liable for breaches and additional surveillance of HIOs, through audits, exists to ensure

service and skill level required to perform the service. *Id.* Scope of agency is determined by several factors: 1) the time, place and purpose of the agent's conduct; 2) whether the principle had control over the agent's conduct; 3) whether the conduct is commonly performed by agents; and 4) whether the principle reasonably expected the agent would engage in the conduct in question. *Id.* Given the technical and skilled nature of maintaining and transmitting large amounts of data, it is unlikely HIOs would be considered agents. Further, it is unlikely that a breach would be within the scope of agency, especially for small practice groups, because covered entities generally will not have sufficient control over the HIO since they are not directly supervised and do not regularly monitor HIO's conduct, nor do they have the expertise to do so.

198. HIPAA Modification Final Rule, *supra* note 119, at 5582.

199. 45 C.F.R. § 160.412 (2014); HIPAA Modification Final Rule, *supra* note 119, at 5585-86.

200. 45 C.F.R. § 160.410 (2014).

201. MCGOWAN ET AL., *supra* note 26, at 23-24.

202. *See supra* notes 91-97 and accompanying text.

203. *See supra* notes 129-30 and accompanying text.

compliance. Thus, adding such teeth to the Act enables effectiveness by allowing stakeholders to trust that the HIO will protect the confidentiality and integrity of individuals' PHI.

The enforcement mechanisms recognize the need for a balance between both sides of the sword and attempt to find an appropriate balance. However, it is still uncertain whether the Act has found the perfect balance and clearer guidelines are needed to determine the true risk of liability for both HIOs and covered entities. The Act sets out potentially strict penalties, but balances this by giving the Secretary great discretion in imposing penalties. History shows that the Agency prefers to work with organizations on correcting issues rather than beating organizations with a stick.[204] Further, the OCR is continuing its commitment to work with organizations to protect PHI through its audit program.[205] However, the OCR has recently become increasingly stricter and it remains uncertain just how strict it will become.[206] Similarly, under the new enforcement mechanisms, a state Attorney General may file claims, but it also remains uncertain how aggressive the Attorney Generals will be.[207] Granted, the law does balance this by granting the Secretary authority to intervene in any proceeding.[208] Furthermore, with the availability of the federal common law theory of agency, it is uncertain who may be liable—the covered entity, business associate, or both.[209] However, given this gentle balance in the enforcement mechanisms and uncertainty on how the OCR and state Attorney Generals will utilize them, the mechanisms could either act as a strong deterrent to HIOs, or strengthen the infrastructure built by the other HIPAA Rules.

B. Financial Support and Incentives

In addition to building an infrastructure to support the use of health IT by strengthening the HIPAA Administrative Simplification provisions, the federal government recognizes the need to assist the health industry in implementing and adapting to health IT. The most commonly cited barrier to the implementation of HIOs is the substantial cost.[210] Recognizing this, the HITECH Act originally designated $300 million to support regional or sub-national efforts to implement an HIE.[211] While the Act appropriated $300

204. *See supra* notes 157-60 and accompanying text.

205. *See supra* notes 167-169 and accompanying text.

206. *See generally* Krystyna Monticello, *Enforcement of HIPAA*, LEGAL HEALTH INFO. EXCHANGE, http://www.legalhie.com/enforcement-of-hipa/ (last visited Nov. 2, 2014).

207. *See supra* notes 161-164 and accompanying text.

208. *See supra* note 164.

209. *See supra* notes 196-98 and accompanying text.

210. *See infra* Part II, B.2.

211. American Recovery and Reinvestment Act of 2009, 42 U.S.C. § 300jj-11 (2012).

million, the ONC has increased available funding opportunities and provided additional financial assistance for other health IT-related infrastructures.[212] The four largest sources of funding include (1) the State HIE Cooperative Agreement Program, (2) the Regional Extension Center (REC) grants, (3) the Medicare and Medicaid EHR Incentive Programs, and (4) the Administration of the Medicaid EHR Incentive Programs. Other funding opportunities exist for eligible communities, to support further innovation and increase possibilities for HIE.[213] The availability of such large grant money has drawn the attention of every state and as of 2011, all fifty states and six territories have received some federal money to support the implementation of HIE.[214]

1. State Health Information Exchange Cooperative Agreement Program

The State HIE Cooperative Agreement Program is a grant offered to each state[215] or eligible state designated entity.[216] The purpose of the grant is to hasten the implementation of HIE by reducing the initial investment.[217] A state

212. *See* OFFICE NAT'L COORDINATOR FOR HEALTH INFO. TECH., GET THE FACTS ABOUT STATE HEALTH INFORMATION 1 (2011), *available at* http://www.healthit.gov/sites/default/files/get-the-facts-about-state-hie-program-2.pdf.

213. ONC offered an additional grant on January 27, 2011 called HIE Challenged Grant Program. *State Health Information Exchange Cooperative Agreement Program*, HEALTHIT.ORG (Jan. 27, 2011), http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange [hereinafter *State Cooperative Agreement*]. The grant awarded a total of $16 million in additional funding to states to develop new innovations to enable their HIO's infrastructure to be scaled to support a nationwide HIE. *Id.* As of Jan. 2013, ten states have received a HIE Challenge Grant Program ranging between $1-2 million. *Health Information Exchange Challenge Grant Program*, HEALTHIT.ORG, http://www.healthit.gov/providers-professionals/healthinformation-exchange-challenge-grant-program (last visited Jan. 4, 2014). Other grants are available through the Centers for Disease Control and Prevention (CDC) and HHS. New York, for instance, has received a $20 million grant to improve public health situational surveillance and a $4.7 million contract from HHS "to support the Nationwide Health Information Network (NHIN) Trial Implementations Project". N.Y. STATE DEP'T OF HEALTH, NEW YORK EHEALTH COLLABORATIVE (NYEC): STATE HIE COOPERATIVE AGREEMENT PROGRAM STRATEGIC PLAN 6 (2009), *available at* http://dss.mo.gov/hie/resources/workgroup2009/newyork.pdf (last visited Jan. 4, 2014) [hereinafter NY EHEALTH COLLABORATIVE].

214. *See State Cooperative Agreement*, *supra* note 213.

215. The definition of state includes eligible U.S. territories. Eligible territories include: Washington DC, American Samoa, Guam, Puerto Rico, Virgin Islands, and the Northern Mariana Islands. *Id.*

216. OFFICE OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEP'T HEALTH & HUMAN SERVS., AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, TITLE XIII – HEALTH INFORMATION TECHNOLOGY, SUBTITLE B – INCENTIVES FOR THE USE OF HEALTH INFORMATION TECHNOLOGY, SECTION 3013, STATE GRANTS TO PROMOTE HEALTH INFORMATION TECHNOLOGY: STATE HEALTH INFORMATION EXCHANGE COOPERATIVE AGREEMENT PROGRAM FUNDING OPPORTUNITY ANNOUNCEMENT 5 (2009) [hereinafter GRANT PROGRAM ANNOUNCEMENT].

217. *See id.* at 23.

may receive anywhere from $4 million to $40 million dollars between 2010 and 2015.[218] In total, as of January 27, 2011, the ONC has awarded $547,703,438 in State HIE Cooperative Agreements to all fifty states and six territories.[219] The grant is not expected to cover the entire cost of implementing the program. As the name implies, the implementation of HIE is supposed to be a cooperative effort between federal, state, and private entities. Since 2011, the ONC may not provide any grant money to states that do not contribute non-federal money.[220] In 2011, for every non-federal dollar, the federal government provided ten dollars[221] and in 2012, for every non-federal dollar, the federal government provided seven dollars.[222] In 2013, and in each subsequent fiscal year, for every non-federal dollar, the federal government will provide three dollars.[223]

The State HIE Cooperative Agreement Program provides the largest source of federal funding for the implementation of HIEs, offering millions of dollars. Missouri, for example, was awarded $13,765,040.[224] While accepting this money comes with strings,[225] these strings have not caused states to hesitate. Perhaps this is because the state's obligations under the program are ultimately necessary to implement an HIO in any regard. For instance, recipients of the grant must engage stakeholders.[226] This, however, is necessary for the success of any HIO policy. At first glance, one may have believed the matching requirement imposed by the federal government would cause apprehension from states, especially considering approximately half of them refused to expand Medicaid under the ACA.[227] However, this has not been the case. The

218. *See id.* at 22.

219. *State Cooperative Agreement*, *supra* note 213.

220. American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 300jj-33 (2012).

221. 42 U.S.C. § 300jj-33(i)(1)(A).

222. 42 U.S.C. § 300jj-33(i)(1)(B).

223. 42 U.S.C. § 300jj-33(i)(1)(C).

224. *See State Cooperative Agreement*, *supra* note 213.

225. Recipients of the grant are expected to: a) ensure that the technical services necessary for the implementation of HIE are available across the state, b) remove interoperability issues and other barriers to ensure laboratories, hospitals, clinical offices, health plans and others may be able to exchange information, c) engage stakeholders in order to build trust and support of the HIE, d) guarantee an effective governance and accountability model is implemented, e) coordinate with Medicaid and state public health programs to monitor the Medicaid Meaningful Use Incentives, and f) develop and update privacy and security requirements. GRANT PROGRAM ANNOUNCEMENT, *supra* note 216, at 8-9.

226. *Id.*

227. At the end of 2013, twenty-six states planned on expanding Medicaid in 2014, while twenty-two States did not plan on expanding Medicaid. *Status of State Action on the Medicaid Expansion Decision*, KAISER FAM. FOUND. (Dec. 11, 2013), http://kff.org/health-reform/state-indicator/state-activity-around-expanding-medicaid-under-theaffordable-care-act/.

matching requirement has not been a barrier.[228] Perhaps this is because states are not required to directly contribute and are only required to contribute non-federal money,[229] meaning that money may come from other stakeholders. Missouri, for instance, is considering charging an initial connectivity fee, which is a reoccurring fee for sustaining connectivity and adjudicating insurance claims.[230] New York plans on supporting its HIE through its state reimbursement reform.[231] Ensuring non-federal money was a wise decision because without placing a heavy financial burden on states, it forces them to consider the long-term financial sustainability right from the beginning and reinforces the idea that the federal government's investment in these programs is part of the initial set-up phase. The State HIE Cooperative Agreement Program has provided the incentives and means for states to develop their own health IT infrastructure through the use of HIE.

2. Regional Extension Centers (RECs)

RECs create cooperative programs with non-profit organizations to support providers in specific geographic areas with implementing and utilizing health IT that complies with standards, certification criteria, and implementation specifications for MU-technology.[232] The primary functions of RECs are to: (a) assist providers, particularly those in small group practices or practices that lack resources, with implementing, utilizing, upgrading, and maintaining EHR, (b) disseminate best practices and research related to Health IT, including HIEs, (c) participate in HIEs, (d) utilize the expertise and capabilities of federal Agencies and departments, and (e) help with ongoing training of health professionals and others in the health care industry on how to use health IT.[233]

As of the date of this writing, there are sixty-two REC partners who have collectively received $677 million for the first two years of work,[234] starting in 2010.[235] A REC is a four-year contract with the federal government, paid out to

228. *See generally State Cooperative Agreement*, *supra* note 213.

229. *See infra* notes 220-23.

230. MO HEALTH CONNECTION, MO-HITECH HEALTH INFORMATION EXCHANGE STRATEGIC PLAN 51 (Mar. 17, 2010).

231. NY EHEALTH COLLABORATIVE, *supra* note 213, at 5.

232. *Regional Extension Center (REC): REC History*, HEALTHIT.ORG, http://www.healthit.gov/providersprofessionals/rec-history (last visited Jan. 5, 2014) [hereinafter *REC History*].

233. 42 U.S.C. § 300jj–32(c) (2012).

234. OFFICE OF NAT'L COORDINATOR FOR HEALTH INFO TECH., GET THE FACTS ABOUT REGIONAL EXTENSION CENTERS 1 (2014), *available at* http://www.healthit.gov/sites/default/files/pdf/fact-sheets/get-the-facts-about-regional-extension-centers.pdf [hereinafter GET THE FACTS ABOUT RECS].

235. Advancing Washington's Health Information Infrastructure, HIIAB Board Meeting 18 (Sept. 16, 2009).

the REC in two-year increments.[236] A REC may receive a grant between $1 million and $30 million.[237] Like the state HIE Cooperative Agreement Program, the REC program is cooperative and requires fifty percent matching contributions, unless waived by the Secretary after determining the national economic conditions make this cost-sharing requirement detrimental to the program and Congress is notified of the waiver.[238] This cost-sharing requirement has not prevented organizations from entering this program, with all sixty-two REC partners signing up within five months.[239]

While the financial opportunity under this program is large for a REC, the true importance is the training and assistance the program offers to providers and other people in the health industry. For example, by July 2013, over 147,000 providers enrolled in a REC[240] and these providers now have assistance in choosing and integrating various types of health IT. Moreover, RECs can take the lead on educational and outreach efforts that inform providers about the benefits of health IT and the importance of connecting with HIOs. These outreach and training programs will hopefully help providers transition into a new delivery system and reduce resistance to EHRs and HIEs, which was seen in the past.[241] Additionally, since RECs work closely with the people who use the new technology, RECs are also in a prime position to evaluate and develop new innovations to improve HIE and make the delivery of health care more efficient.[242] Therefore, RECs address the technical barriers to HIE by helping providers integrate health IT into their practice.

3. Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs

The Medicare and Medicaid EHR Incentive Programs are directed at providers and health care organizations and are designed to incentivize providers to become meaningful users of EHR.[243] While these programs do not

236. *Id.* at 17.

237. *Id.*

238. 42 U.S.C. § 300jj–32(c)(5) (2012).

239. *REC History*, *supra* note 232.

240. *Regional Extension Center (REC): REC Support for Health Information Exchange*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/rec-support-health-information-exchange (last visited Jan. 5, 2014) [hereinafter *REC Support*].

241. *See supra* Part II.B.

242. *REC Support*, *supra* note 240.

243. Daniel F. Gottlieb, *CMS Proposes Medicare and Medicaid Reimbursement Rules for Earning Incentive Payments for Meaningful Use of Certified Electronic Health Record Technology*, WILLIAM MGMT. ASSOCIATES INSIGHTS, Spring 2010, at 43, 44. Meaningful EHR user is an eligible professional who: a) uses certified EHR technology, b) whose EHR technology is connected to an HIE in accordance to the law, and c) who reports quality and other measures through their EHR system. 42 U.S.C. § 1395w-4(o)(2)(A) (2012). An eligible professional is a: 1) doctor of medicine or osteopathy, 2) doctor of dental surgery or medicine, 3) doctor of podiatric

address HIEs, they deserve a brief mention because they provide the key "carrot and stick" incentives for the implementation of health IT. For any HIO to be successful it needs the support of providers, who must use EHRs.[244] The Medicare and Medicaid EHR Incentive Programs are the federal government's attempt to ensure providers use EHRs and that providers have the ability to exchange information through an HIO.

While the Medicare and Medicaid EHR Incentive Programs are similar, they are two distinct programs. Both provide an additional payment for a period of time to eligible participants who are using EHR in a meaningful way. However, eligible professionals may participate in only one program in a given year.[245] Under the Medicare EHR Incentive Program, an eligible professional who demonstrates they use EHR in a meaningful way, may receive up to $44,000 over five years.[246] To receive the full payments, the provider must have demonstrated "meaningful use" by 2012, as the caps on payments decrease over time.[247] Those who did not start participating by 2014 are not eligible to participate, and all payments cease after 2016.[248] Additionally, starting in 2015, providers seeking Medicare fee-for-service reimbursement who were eligible to participate in the Medicare EHR Incentive Program, but who have not yet demonstrated "meaningful use" of their EHR, will be subject to a Medicare payment adjustment.[249] This decrease in payment to providers will increase over time, but cannot exceed five percent.[250]

The Medicaid EHR Incentive Programs are run by each state's Medicaid Agency.[251] Currently, fifty-one states and territories are offering these

medicine, 4) doctor of optometry or 5) chiropractor receiving Medicare payments. Gottlieb, *supra* note 243, at 44.

244. *See supra* Part II.B.1.

245. *The Official Web Site for the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms (last modified October 7, 2014) [hereinafter *EHR Incentive Program*]. Eligible hospitals and critical access hospitals may receive payment from both. *Id*.

246. *Id.* Additional payments may be available to those who serve in Health Professional Shortage Areas (HPSA). Generally, providers will receive an additional payment of 75% of their allowable charges under the Medicare Physician Fee Schedule, up to a cap. Gottlieb, *supra* note 243, at 43-44.

247. *See* CTRS. FOR MEDICARE & MEDICAID SERVS., AN INTRODUCTION TO THE MEDICARE EHR INCENTIVE PROGRAM FOR ELIGIBLE PROFESSIONALS 14 (2010), *available at* http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Beginners_Guide.pdf [hereinafter MEDICARE EHR PROGRAM].

248. *See id.*

249. *Id.* at 16.

250. 42 U.S.C. § 1395w-4(a)(7)(a)(iii) (2012).

251. *EHR Incentive Program*, *supra* note 245. Medicare EHR is administrated through the Center for Medicare and Medicaid Services (CMS). *Id*.

programs.[252] Under the Medicaid EHR Incentive Programs, eligible professionals, hospitals, and critical access hospitals located in an area where the program is offered may participate, so long as they begin participating by 2016.[253] In the first year, participants may receive payments for adopting, implementing, or upgrading their EHR technology.[254] After that, participants must show they are using EHR according to the federal MU-requirements. Eligible professionals may receive up to $63,750.[255] Unlike the Medicare EHR Incentive Program, there are no payment adjustments under the Medicaid EHR Incentive Programs and thus, so long as participants continue to meet the eligibility requirements, they will receive the fixed payment.[256] Possible payment is not based on the amount of Medicaid services provided, or when the participants start, so long as they start by the year 2016.[257]

Together these programs are providing incentives for the adoption of EHRs. These programs are paying providers to use their EHR systems and, under the Medicare Incentive Program, penalizing providers who fail to utilize it. By tying reimbursement to the use of EHR, the Medicare Incentive Program represents the federal government's long-term commitment to using health IT to reform the health care delivery system.

4. Administration of the Medicaid EHR Incentive Program

The Administration of the Medicaid EHR Incentive Programs is meant to be a short-term program that provides financial assistance to states for administering and overseeing the Medicaid EHR Incentive Program.[258] States

252. *See Medicaid State Information*, CTRS. FOR MEDICARE & MEDICAID SERVS., http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/MedicaidStateInfo.html (last modified June 26, 2013).

253. *See* CTRS. FOR MEDICARE & MEDICAID SERVS., AN INTRODUCTION TO THE MEDICAID EHR INCENTIVE PROGRAM FOR ELIGIBLE PROFESSIONALS 18 (2012), *available at* http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_Medicaid_Guide_Remediated_2012.pdf [hereinafter MEDICAID EHR PROGRAM].

254. *EHR Incentive Program*, *supra* note 245.

255. *Id.* Eligible professionals are: 1) doctors of dental surgery or medicine, 2) nurse practitioners, 3) certified nurse midwives, 4) dentists, and 5) physician assistants who provide services in Federally Qualified Health Centers (FQHC) or Rural Health Clinics (RHC) run by a physician assistant. *Id.* They must have a minimum of 30% Medicaid patient volume, or practice in a FQHC or RHC and have a minimum 30% patient volume of needy individuals. *Id.* Pediatricians only need to have 20% Medicaid patient volume, however Children's Health Insurance Program (CHIP) patients do not count toward the Medicaid patient volume criteria. *Id.*

256. MEDICAID EHR PROGRAM, *supra* note 253, at 17.

257. *Id.* at 19.

258. *See* Letter from Cindy Mann, Director, Ctrs. for Medicare & Medicaid Servs., to State Medicaid Directors (Aug. 17, 2010) (on file with CMS under SMD #10-016), *available at* http://www.dhcs.ca.gov/Documents/OHIT/StateMedicaidDirectorletter.pdf [hereinafter Mann Letter]; *see also* Helen Pfister & Susan Ingargiola, *New Trend in Sustainable HIEs: Fair Share*

may seek ninety percent reimbursement for costs associated with: (a) administering the Medicaid EHR Incentive Programs to eligible Medicaid providers and hospitals, (b) overseeing the Medicaid EHR Incentive Programs to minimize fraud and abuse, and (c) pursuing initiatives that encourage the adoption of certified EHR technology and HIE.[259] This program is meant to be a filler program to help cover costs not addressed by other programs. States may only receive reimbursement for costs associated with the long-term vision of HIE, such as electronic reporting of structured laboratory data and enabling e-prescribing, as long as they are not duplicated by other technical assistance efforts.[260] Therefore, the Administration of the Medicaid EHR Incentive Programs financially motivate states to participate as stakeholders in the implementation of health IT by reducing their costs.

IV. HITECH'S EARLY IMPACT

With new legislation and substantial opportunity for capital, stakeholders—states, providers, universities, and industries—are collaborating to transform the health care delivery system through the use of EHRs and readily available, accurate data. All fifty states and several territories have accepted grants from the state HIE Cooperative Agreement Program to establish an information exchange,[261] and more than sixty RECs have been created to advance the adoption and use of EHRs and other health IT.[262] Further, with the decreasing Medicare reimbursement rates around the corner for providers who fail to use EHRs,[263] and the roll out of new ACA-provisions, the sense of urgency from stakeholders to implement a robust, integrated health IT platform that uses an HIE, continues to grow. While the country is moving toward a new delivery system structured around health IT, early efforts by stakeholders have revealed mixed results, and suggest the need for further policy corrections and governmental support to ensure full implementation.

On one hand, EHR adoption among hospitals is growing rapidly and is predicted to further increase before the Medicare EHR Incentive Program's deadline in 2015.[264] As of May 30, 2013, over 200,000 eligible providers registered for the Medicare EHR Incentive Program, meaning that over

Finance Support, IHEALTHBEAT (Aug. 11, 2011), http://www.ihealthbeat.org/insight/2011/new-trend-in-sustainable-hies-fair-share-financial-support.

259. Mann Letter, *supra* note 258, at 13.

260. *Id*. at Enclosure C.

261. *See State Cooperative Agreement*, *supra* note 213.

262. GET THE FACTS ABOUT RECS, *supra* note 234, at 1.

263. MEDICARE EHR PROGRAM, *supra* note 247, at 16.

264. Kendra Casey Plank, *Growth in EHR Adoption Rates Could Slow Before Peaking Again Ahead of 2015*, 21 BNA'S HEALTH CARE POL'Y REP., Jul 15, 2013, at 1147, 1179.

200,000 eligible providers have implemented and are using certified EHRs.[265] This shows that physicians are more open to the idea of EHRs and that more providers have the necessary infrastructure to connect with an HIO. Moreover, many of these eligible providers were utilizing EHR more than what was required during the early stages of the program, indicating that providers have been able to overcome practical integration issues.[266] Additionally, a study found that once implemented, physicians exclusively use certain aspects of their EHR systems, suggesting providers are overcoming the technical barriers to adopting EHRs and finding value in EHRs.[267] Physicians' willingness to adopt EHRs is a key indicator of success for HIOs, as it represents the first step in building the infrastructure for a new centralized system, where information can systematically converge to provide parties with accurate and timely answers.

Further, some early results indicate the health industry is well on its way to the second step in building the infrastructure—the creation of HIOs. With EHR expansion, the market for information exchanges is growing. Overall, direct exchange transactions across the country increased by ninety-five million in just over one year.[268] One of Texas's HIOs, *Greater Houston HealthConnect*, claims it brought in nearly one million dollars in hospital and administration fees in 2013.[269] Illinois's HIE is expected to soon be profitable from subscription and transaction fees.[270] Early results from these HIOs suggest that with a lean business model, an HIO can flourish because some providers desire and want information available through the HIO.

On the other hand, some early results suggest further stumbling blocks for HIOs. While EHR implementation is expanding, studies show significant differences in who is implementing EHRs. For instance, solo practices and small practices are less likely to implement an EHR than large practices.[271] Additionally, small hospitals are less likely than large hospitals to implement an EHR system and are also adopting them at slower rates.[272] This disparity

265. Adam Wright et al., *The Medicare Electronic Health Record Incentive Program: Provider Performance on Core and Menu Measures*, 49 HEALTH SERV. RESEARCH 325, 337 (2014).

266. *See id.* at 342.

267. *Id.* at 344.

268. *See ONC Refutes Claims*, *supra* note 64, at 4.

269. *Id*. at 5.

270. *Id*. In Illinois, users must pay an annual $195 fee to connect to the Illinois HIE and currently, 150 hospitals in Illinois are connected to the Illinois HIE. *Id*.

271. Sowmya R. Rao et al., *Electronic Health Records in Small Physician Practices: Availability, Use, and Perceived Benefits*, 18 J. AM. MED. INFO. ASS'N 271, 274 (2011).

272. Catherine M. Desoches et al., *Small, Nonteaching, and Rural Hospitals Continue to be Slow in Adopting Electronic Health Records System*, 31 HEALTH AFF., 1092, 1095 (2012) (finding the number of small hospitals adopting EHR systems were growing 15% lower than the number of large hospitals adopting EHR systems). *See* Ashish K. Jha et al., *A Progress Report On*

between providers impedes the development of HIOs and limits success because it excludes an important portion of the health industry. If primary care physicians in small practices do not adopt EHRs, the HIO's ability to coordinate care is impaired because the HIO is unable to connect hospitals and primary care physicians. Further, this disparity hinders the ability of HIOs to facilitate research because the gathered data will exclude an entire population. Moreover, as a policy concern, this gap in information could lead to further health disparities among underserved populations. For example, if, in fact, the use of health IT improves quality of care, then people who live near, and can afford to go to large health systems, will have the opportunity to receive better, more effective care. Thus, further assistance by the federal and state government may be necessary to ensure these groups of providers are able to take advantage of health IT.

Additionally, research shows concern that providers who have implemented EHRs are not utilizing all of the functions, such as electronic notes and e-prescribing.[273] One study revealed that out of 237, 267 eligible providers, ninety percent claimed an exclusion from one or more measurements of EHR function, with the majority claiming two or more exclusions.[274] This means that providers are not using all functions necessary to fully use EHRs in a meaningful way, and further suggests that providers are not integrating EHRs into their clinical practices and instead, are relying on loopholes in the law.[275] This could become problematic for the financial stability and ultimate goals of HIOs. For example, many HIOs plan on charging transaction fees.[276] If providers are not utilizing the full range of services, HIOs cannot capitalize on revenue generated by fees.[277] Further, if providers are not fully using their EHRs, the value of HIOs to other providers is diminished because HIOs are unable to supply complete and adequate information,[278] and ultimately, HIOs become less useful to prescribers. Moreover, if records are incomplete, the ability of HIOs to reduce health costs and improve quality is impaired.[279]

Electronic Health Records In U.S. Hospitals, 29 HEALTH AFF. 1951, 1953 (2010) (finding that medium-size hospitals were 50% less likely to have adopted a basic EHR system than large hospitals in 2009 and small-size and critical-access hospitals were 70% and 80% less likely to have adopted an EHR system, respectively).

273. Rao et al., *supra* note 271, at 274.

274. Wright et al., *supra* note 265, at 238, 40.

275. *See id*. at 343 (faulting CMS for allowing providers to exempt out of the certain meaningful use requirements).

276. *See* Alder-Milstein et al., *supra* note 48, at 1491.

277. *See id*. at 1489.

278. *See id.*

279. *See supra* Part II.B.3.

Further research is necessary to determine whether this trend is merely a representation of the practice integration barrier, which will decrease as providers receive technical assistance from RECs, or, tough mandates are needed to assure full use of EHRs. Since funding for the sixty-two RECs expired in August of 2014,[280] there is an additional question of whether providers will have access to the necessary assistance needed to continue overcoming the integration barrier. Yet, there is hope for the programs that assisted over 153,000 providers (forty-six of the nation's primary care physicians)[281] because they can apply for a year-extension and take additional steps toward financial sustainability.[282] Moreover, the need for technical assistance will continue, and its availability will likely determine whether health IT is widely implemented and fully utilized.

Another issue remains, concerning the availability of ONC-certified technology that qualifies for MU-incentive payments under the Medicare and Medicaid EHR Incentive Programs. Providers and organizations claim the limited supplies in Health IT and delays in necessary updates are making compliance with the 2014 MU-requirements implausible.[283] The Centers for Medicare and Medicaid Services (CMS) stated that by the end of September 2013 about 44,000 providers applied for a hardship exemption in order to stay in the Medicare EHR Incentive Program and avoid the 2015 penalty.[284] The complaints prompted CMS to finalize a modification allowing hospitals and eligible professionals more flexibility in how they meet MU-requirements.[285] While some providers and organizations praise the modified requirements, others find them too limited in scope to provide any real relief because the flexibility only applies to the 2014 reporting period.[286] Others still voice frustration with the Medicare and Medicaid EHR Incentive Programs and the MU-requirements, finding that HHS, CMS, and ONC are too focused on defining how EHRs should be used and are not paying enough attention to

280. ALTARUM INST., MODERNIZING HEALTH CARE: LEVERAGING OUR REGIONAL EXTENSION CENTERS 1 (2013), *available at* http://altarum.org/sites/default/files/uploaded-related-files/LeveragingRegionalExtensionCenters_0.pdf.

281. *Regional Extension Centers (RECs): Advising Providers in All Phases of Electronic Health Record Implementation*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/regional-extension-centers-recs (last updated Oct. 2, 2014).

282. Gabriel Perna, *Kansas REC Gets Funding Extension*, HEALTHCARE INFORMATICS (Feb. 11, 2014), http://www.healthcare-informatics.com/news-item/kansas-rec-gets-funding-extension.

283. Kendra Casey Plank, *CMS Reopens Hardship Exception Application Deadline for EHR Program*, HEALTH IT L. & INDUS. REPORT, Oct. 7, 2014, at 8, 8.

284. *Id.* at 9.

285. Darius Tahir, *CMS Finalizes EHR Meaningful-Use Rule, Adds Some Flexibility*, MODERN HEALTHCARE (Aug. 29, 2014), http://www.modernhealthcare.com/article/20140829/NEWS/308299938.

286. *Id.*

fostering innovation and improving interoperability among EHRs.[287] The delays indicate the growing frustration among providers towards the implementation of health IT and the unpreparedness of the industry to meet the 2015-implementation deadlines.

Further, while the number of exchange interactions is increasing, the exchanges are occurring on a local level or between organizations using the same EHR vendors.[288] Thus, concerns remain about the interoperability of EHR systems. One ONC-report claims that "[e]lectronic health information is not yet sufficiently standardized to allow seamless interoperability, thereby limiting the potential uses of the information to improve health and care."[289] These concerns are heightened because many of the major EHR vendors are offering HIE networks that are limited to providers and organizations within that particular vendor.[290] For instance, EPIC offers its customers *CareEverywhere*, an HIE network that connects EPIC customers with other customers.[291] Similarly, *eClinicalWorks*, an EHR system designed for small practice, offers *Electronic Helath eXchange*, an HIE that connects practices who use *eClinicalWorks*.[292] While these HIEs connect practices and providers, the network is limited and does not allow the exchange of information among all groups and providers. It simply allows organizations to connect providers to the system, facilitating the delivery of integrated care, but to patients who receive care only within the organization. These narrow networks do not serve the goals of providing and integrating health care throughout the nation, or the goal of compiling data sets for the use of research. Further, narrow vendor-specific networks have the potential to weaken the financial stability of HIOs, by facilitating communication within the vendor's network and thus, decreasing the need to belong to an HIO's large network consisting of multiple EHR vendors. This is because providers within a health care system typically all have the same EHR vendor, so they do not regularly need to exchange information with providers that use different vendors.

Moreover, while some HIOs are capitalizing on the expanding HIE market, many early HIOs are struggling to become financially sustainable. A recent survey, conducted by a Florida research company, predicts that HIOs will face

287. Kendra Casey Plank, *Provider Groups Convey Frustration About Health IT Programs to Burwell*, HEALTH IT L. & INDUS. REPORT, Oct. 20, 2014, at 8, 8.

288. *See generally* Alex Ruoff, *Health Executives Say Federal Government Should Be More Proactive on Interoperability*, HEALTH IT L. & INDUS. REPORT, Sep. 29, 2014, at 1.

289. Kendra Casey Plank, *ONC Says HIT Adoption Continues to Grow, But Little Progress on Clinical Data Exchange*, HEALTH IT L. & INDUS. REPORT, Oct. 13 2014, at 10, 11.

290. *See generally* Alex Ruoff, *Small, Private Health Information Exchanges Replacing Large, Public Ones*, HEALTH IT L. & INDUS. REPORT, Oct. 7, 2014, at 22 [hereinafter *Private Replacing Public*].

291. *Id.* at 23.

292. *Id.*

sustainability issues, concluding that by 2017 as few as ten of the thirty currently functioning HIEs will be operational.[293] The survey found that it is unlikely that providers and insurers will pay user fees, until it is certain that they will financially benefit from participating in HIOs and at this point, few find that HIOs add enough value to support the fees.[294] An event in 2012 suggests that the survey may be accurate, when Washington D.C.'s Regional Health Information Organization (RHIO) shut down after determining it could not maintain current operations.[295] Washington's RHIO operated on federal grant money and over time, could not continue.[296] Such early results cast doubt on whether the initial grant money will be enough to maintain HIOs and the results further suggest that success will depend on additional state or federal assistance. As the public funding for HIE ends in 2015, this is becoming a larger concern.[297] Thus, more government funding may be needed or perhaps the private sector, through smaller HIE networks, will fill the market need as it has already begun to do.[298]

Overall, HITECH's early impact suggests the U.S. is preparing and moving forward in using HIOs and health IT as the centerpiece of the delivery system. More providers are implementing the necessary infrastructure and are seeing a need for the HIEs.[299] However, collectively, the nation has not overcome the initial barriers, such as interoperability and data security, and further market corrections are necessary. First, policymakers need to pay close attention to who is implementing health IT, to ensure it does not increase health disparities. Second, additional support and tougher regulations may be necessary to ensure providers are fully using the technology, in order to guarantee the value of the system. Lastly, the government must decide what level of involvement it would like to have in health IT moving forward.

Currently, the government is preparing to take more of a passive role in the development of the health IT infrastructure. If it continues down this path, the government should strongly consider the early implications, previously discussed. Leaving the free market to its own devices, with only minimum guidance by the ONC, will result in health IT becoming the infrastructure of a new health care delivery system, but the system will result in new challenges. One new concern is whether there will be effective competition among health

293. *ONC Refutes Claims*, *supra* note 64, at 2.

294. *Id.*

295. Kyle Murphy, *DC HIE Carries on without RHIO*, EHR INTELLIGENCE (Nov. 12, 2012), http://ehrintelligence.com/2012/11/12/dc-hie-carries-on-without-rhio/. *See also* Fischer, *supra* note 63.

296. Murphy, *supra* note 295.

297. *See generally Private Replacing Public*, *supra* note 290, at 23.

298. *Id.* at 22-23.

299. *See supra* notes 228-34 and accompanying text.

IT suppliers.[300] For example, as health IT becomes the health care infrastructure, health care organizations and providers will become more reliant on health IT, making its demand more inelastic and giving health IT vendors more negotiating leverage and price-setting power.[301] Concerns have surfaced on whether EHR vendors are blocking interoperability efforts through such increased power.[302]

Another rising barrier is frustration from physicians regarding the implementation of health IT programs. As the government rushes to meet its own deadlines, the burden of implementing the programs falls more heavily on providers. For example, the president of the American Medical Association, Steven J. Stack, describes the government's initiative as "aggressively moving forward."[303] He further claims that the incentive programs, while well intended, are confusing and burdensome to providers and could jeopardize patient care.[304] Additionally, Stack suggests that the current EHR system designs are poor and insufficient to meet the government's lofty requirements, placing additional burdens on providers.[305] The government would best be served by extending the adjustment period, providing more incentives, and delaying the penalties. Its current focus should be on improving interoperability and data security, as well as collecting data on the progress of recent implementation and the current health IT market. If the government wishes the market to develop the infrastructure, the government must allow time for the market to adapt to the new demand created by the government.

V. CONCLUSION

The HITECH Act attempts to improve quality, decrease costs, and advance the field of medicine through the development and implementation of HIOs and EHRs. EHRs assist in the development of a complete medical record and HIOs oversee the exchange of that record between parties involved in a patient's care. Together HIOs and EHRs build an infrastructure that connects various parties participating in the patient's care. This new infrastructure allows parties to efficiently communicate with each other by increasing the availability of timely, complete, and accurate information to interested parties.

300. Alex Ruoff, *FTC Official: Trade Regulators Examining Health IT Market for Signs of Info Blocking*, HEALTH IT L. & INDUS. REPORT, Oct. 9, 2014, at 6, 6 [hereinafter *Examining Health IT Market*].

301. *See generally* Kenneth D. Mandl and Issac S. Kohane, *Escaping the EHR Trap—The Future of Health IT*, 366 NEW ENGLAND J. OF MEDICINE 2240 (2012).

302. *Examining Health IT Market*, *supra* note 300, at 6.

303. Kendra Casey Plank, *Heath IT Initiatives Putting New Burdens on Doctors, AMA Exec Says*, HEALTH IT L. & INDUS. REPORT, Oct. 27, 2014, at 7, 7.

304. *Id.*

305. *Id.*

Thus, EHRs and HIOs build a virtual network to integrate various stakeholders participating in the delivery of health care.

This integration of the delivery care system benefits heath care in several ways. First, it improves quality of care by reducing medical errors and assists with coordination of care. Second, it reduces overall cost by reducing administrative expenses and waste resulting from unnecessary tests and procedures. Third, it advances the field of medicine by supplying providers with large amounts of data, which can be used to detect emerging public health concerns and advance clinical medicine. Therefore, integration meets the goals of the HITECH Act.

However, barriers exist in the development and implementation of HIOs and EHRs, thus impeding integration. First, concerns regarding the privacy and security of personal health information create hesitation. Distrust remains between the user and technology. Second, implementation is extremely expensive and requires substantial capital. Third, providers struggle with integrating technology into clinical practice in a meaningful way, prohibiting the system from providing users complete value. The federal government counters these barriers by strengthening HIPAA and providing capital to the health industry to assist with some of the implementation costs.

In strengthening several HIPAA provisions, the federal government attempts to build trust in health IT by reinforcing the basic infrastructure for its use, and by increasing legitimacy in the system through stricter enforcement provisions. The Privacy Rule defines what can be done with PHI and the relationship between parties. Moreover, it outlines the obligations of the parties to each other. The Security Rule creates a checklist to assist parties in meeting those obligations, and the enforcement mechanisms provide assurance that parties meet their obligations. Together, these provisions create a legislative framework to govern and foster the utilization of health IT.

The HITECH Act modifies HIPAA in a significant way by including HIOs within the HIPAA legislative framework. The Act defines HIOs as business associates and makes business associates directly liable for portions of the Privacy and Security Rules. This gives HIOs a basic infrastructure around which to evolve, since they must follow the checklist the Security Rule creates. More importantly, HIOs and participants of the HIO now have defined relationships, giving them an idea of their obligations to each other and to third parties. This is important because it reduces uncertainties, builds trust, and allows parties to more accurately assess risks and liabilities. Therefore, including HIOs in HIPAA's legislative framework provides HIOs with an infrastructure around which to develop and gives participants confidence in HIOs. By increasing trust and assurance, the new law increases participants' willingness to join an HIO.

Furthermore, the HITECH Act modifies HIPAA's enforcement provisions, making it potentially stricter. It gives the Secretary discretion to issue penalties

based on strict liability and gives the OCR the authority to conduct random audits. The stricter enforcement adds legitimacy to the Privacy and Security Rules and makes HIOs accountable for breaches, giving parties confidence that the HIO will do everything possible to avoid possible breaches. Yet, while the enforcement mechanisms can reinforce the infrastructure set out by the Privacy and Security Rules, they could also disincentivize the participation in HIOs. The enforcement mechanisms give the Secretary substantial discretion in issuing penalties, and if the Secretary becomes too strict, HIOs face potential bankruptcy and participants could be dissuaded from joining because it could potentially increase their risk of liability. Therefore, the Secretary must gently balance the need to enforce the law to ensure participants' confidence with the need to be lenient, in order to prevent parties from not participating due to potentially higher risks of liability. Clearer guidelines separating HIOs and participants' liability would also encourage the participation in HIOs.

In addition to creating an infrastructure to support HIOs through HIPAA, the federal government provided substantial capital to support its vision. The HITECH Act issued grants to help the health industry overcome the different barriers. Given the substantial cost of implementing HIOs, the state HIE Cooperative Agreement Program provides substantial capital for the development and implementation of HIEs. Since providers, for the most part, are unfamiliar with health IT, the federal government created the REC grants to help providers overcome the technical barriers in selecting the appropriate EHR system and practice integration. Lastly, the Medicare and the Medicaid EHR Incentive Programs provide financial motivation for providers to adopt and use health IT by increasing reimbursements. The Medicare EHR Incentive Program even takes it one step further by decreasing reimbursements for failing to utilize health IT in a meaningful way. Together, these programs are assisting and nudging the health industry to adopt a new delivery system with health IT at its core.

In response to the federal government's assistance and nudge, stakeholders in the health care industry are coming together to implement EHRs and HIOs. Their efforts suggest the U.S. health industry is indeed moving toward an electronic era. The future for HIOs looks promising, although they might end up being smaller and more localized than originally envisioned. While promising, further federal and state assistance is likely. In the short-term, attempts are needed to guarantee widespread, equitable implementation of health IT to prevent further health disparities. Additionally, more aid is needed to help with practice integration to ensure user satisfaction and prevent pushback. In the long-term, as technology evolves and providers' needs change, the government will need to modify and issue new regulations regarding the use of health information, in order to support the changing environment and reinforce its infrastructure. For instance, big data and issues around data ownership are likely to become larger concerns in the near future.

Despite the need for continuous reinforcement by the government, the private industry is likely to build off of the infrastructure created by the HITECH Act, and establish a new delivery system around health IT. However, the private industry will likely need more time than the government allotted, in order to understand and meet the demands of the health industry.

KALLE DEYETTE*

* B.S., Santa Clara University; J.D., M.H.A., Saint Louis University School of Law and College for Public Health & Social Justice (anticipated 2016).

The author would like to thank her family and friends for their enduring support, and Ron Levy, Executive-in-Residence for the Department of Health Management and Policy at Saint Louis University College for Public Health and Social Justice, for his guidance, as well as the hardworking members of the Saint Louis University Journal of Health Law & Policy.