January 13, 2014

HEALTH INFORMATION EXCHANGES' DIRTY LITTLE SECRET: THE INFRASTRUCTURE'S INABILITY TO ENFORCE HEALTH PRIVACY LEGISLATION

Gretchen E Harper, DePaul University College of Law

Available at: https://works.bepress.com/gretchen_harper/1/
The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.\footnote{Anon., U. S. Privacy Study Commission, 1977.}

I. INTRODUCTION

Though the privacy of personal information may seem to be waning in American culture in the era of proliferating social media sites, the push for privacy in health information has remained.\footnote{Facebook would be the third most populous country behind China and India, were the social media site a physical region. See The Rise of Social Networking: Changing the Web as We Know It, ITU NEWS, available at http://www.itu.int/net/itunews/issues/2010/06/35.aspx.} Unlike the restaurant check-in or the posted pet photo, data related to an individual’s health and morbidity is information our society continues to consider highly confidential. Along with the boom of electronic information exchanges and the ubiquity of personal data in various mediums, comes a great concern: privacy. Medical information is among the most sensitive types of personal information.\footnote{Anita L. Allen, PRIVACY LAW AND SOCIETY 742 (2d ed) (2011).} The privacy of health information continues to be a vexing issue as the computerization of medical records proliferates, and the perception of an individual’s control over their health information depreciates. Several technological and legislative campaigns have attempted to institute constraints on health information, but more is needed in order to effectively secure highly sensitive medical information from those that should not be granted access.

This article will discuss the current developments surrounding the privacy of health information through legislative efforts, namely the Health Insurance Portability and Accountability Act (“HIPAA”) and its recent incorporation of the Final Omnibus Rules, the new
challenges imposed on securing certain types of health information as medical records migrate to health information exchanges, and the technological infrastructure that may impact the effectiveness of access restrictions. This article will first begin with a brief history of HIPAA, and the implementation of legislation that has altered its rules since its inception in 1996. It will then look at the burgeoning establishment of health insurance exchanges following the Affordable Care Act, and the issues surrounding the compliance of federal privacy legislation in the wake of the exchanges. The article will explore current technological initiatives that address electronic privacy concerns, and finally, propose a model of technological and federal regulatory collaboration that creates cohesion, consistency, and security for health information as it navigates the health information exchanges.

II. THE IMPORTANCE OF HEALTH PRIVACY

Privacy has been an intangible, yet inherent, concept rooted in our culture for centuries. In the context of personal information, “privacy” has been used as a term to more broadly incorporate “privacy,” “security,” and “confidentiality.” While in the same vein as “privacy,” which addresses what information, if any, should be accessible, “confidentiality” encompasses the use of that information and who may have access to it, and whether that access requires permission. “Security,” on the other hand, is the infrastructure that forces adherence to the confidentiality decisions made in determining privacy and confidentiality, via technological

5 The first evaluations of the concept of privacy have often been attributed to the 1890 Samuel Warren and Louis Brandeis article, “The Right of Privacy,” in which the authors provided analysis on the law’s ability to protect privacy in the wake of new, more invasive technology, i.e. the proliferation of the newspaper industry. See also Joy Pritts, The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research, INSTITUTE OF MEDICINE, available at http://www.iom.edu/~media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.docx (last visited on Nov 24, 2013).
6 Id. at 3.
7 Id.
and/or administrative barriers set in place to further those decisions.\textsuperscript{8} For the purposes of this discussion, the general term privacy will be used to encompass “privacy,” “security,” and “confidentiality.”

It is difficult to think of an area more private than that of a patient’s medical record. Its rich history of physical and mental health behaviors, socioeconomic and demographic information, and even financial stats, provide the reader with very intimate details about an individual’s past and present.\textsuperscript{9} Unsurprisingly then, consumers consistently report that protecting the privacy of their health information is a significant concern, even more so when their information is transferred electronically.\textsuperscript{10} A recent study revealed that of the 1,847 participants, the majority of participants were “very” or “somewhat” concerned about the privacy of health information exchanges (70%) or the security of health information exchanges (75%).\textsuperscript{11}

In fact, certain subsets of individuals weigh their health privacy so heavily that they will take whatever measures necessary to protect and secure certain portions of their health information that they feel could be damning if placed in the wrong hands.\textsuperscript{12} “Unauthorized disclosure of sensitive health information about mental illness, substance use disorders, or genetic traits can cause enormous harm, including social stigma, employment discrimination, insurance discrimination, and, for addictions, possible criminal prosecution, job termination, forfeiture of legal protections such as protection under the Americans with Disabilities Act, or

\begin{flushleft}
\textsuperscript{8} Joy Pritts, The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research, INSTITUTE OF MEDICINE, available at http://www.iom.edu/~media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx (last visited on Nov 24, 2013).

\textsuperscript{9} Id. at 5.

\textsuperscript{10} Id.


\textsuperscript{12} Pritts, supra note 5, at 6.
\end{flushleft}
the right to receive disability benefits.”\textsuperscript{13} For those individuals whom, because of chronic illness, addiction, or genetic history appear particularly vulnerable to adverse effects in the event of disclosure, the fear of disclosure can drastically alter their behavior. Some may decide to pay for their care out of pocket, so as not to produce an insurance claim, which would alert their provider of their condition or diagnosis.\textsuperscript{14} For others, it results in the partial disclosure of relevant information to their health care providers, which can be just as problematic to a proper treatment regimen.\textsuperscript{15} Worse still, in more severe cases, fears of disclosure can serve as a disincentive to seek treatment altogether.\textsuperscript{16} The privacy of health information, and public perception thereof, has a very real impact on the health care industry. Thus, the success of the transition from a paper-based medical record toward an electronic exchange depends on the “accuracy, correctness and trustworthiness of the information, and the privacy rights of individuals to control the disclosure of personal information.”\textsuperscript{17}

III. HIPAA: THE BEGINNING OF FEDERAL HEALTH PRIVACY PROTECTION

While being a rooted tenet in common law, and a guarantee in the Constitution, “[f]ederal medical privacy and confidentiality laws are of relatively recent vintage.”\textsuperscript{18} Recognizing the importance of protecting the privacy of health information and the need for a federal privacy standard, the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-

\begin{footnotes}
\item[15] Id.
\item[16] Id.
\item[18] Allen, supra note 3, at 742. The U.S. Constitution guarantees “the right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures.” See U.S. CONST. amend. IV.
\end{footnotes}
191, was enacted on August 21, 1996.19 For the first time, this legislation effectively created a floor of national protections for the privacy of health information.20 HIPAA gave the Department of Health and Human Services (HHS) the power to adopt a “suite of uniform, national standards” for transactions, security of health information, and electronic signature.21 Through HIPAA, Congress delegated authority to enact national medical data privacy and security standards to HHS, with responsibility dispersed among the Office of National Coordinator (ONC), the Centers for Medicare & Medicaid services (CMS), and the Office for Civil Rights (OCR).22 HIPAA privacy standards apply to all health information regardless of format: electronic, paper, or oral.23 The HIPAA rules apply to, and preempt all contrary state laws, notwithstanding “more stringent” state statutes, in which case the state’s regulations will be upheld.24

Through HIPAA, Congress ordered the development of a new regulation set designed to simplify the administration of health insurance through an electronic exchange.25 HIPAA’s Administrative Simplification Provisions, designed to standardize transactions and health care data, are segregated into five basic rules: transaction and code sets, privacy, security, unique identifiers, and enforcement.26 The HIPPPAA Privacy Rule provided comprehensive federal protection for the privacy of health information, and applies to all covered entities, as designated by definition within the statute.27 Generally, unless specifically permitted by HIPAA, uses and

19 Allen, supra note 3, at 742.
20 Id.
24 Id. at 419.
25 Id. at 414.
26 Id.
disclosures of protected health information (PHI)\textsuperscript{28} by covered entities require written patient authorization. Examples of permitted uses include: 1) disclosure to the same individual of which the information is based upon, 2) disclosure for purposes of treatment, payment, and health care operations, 3) in emergency situations, 4) when prior patient consent has been given, and 5) when required by law.\textsuperscript{29} Covered entities must make reasonable efforts, even when disclosure is permitted, to use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose.\textsuperscript{30}

IV. HIPAA’S HEIGHTENING OF FORCE VIA THE HIPAA OMNIBUS FINAL RULE

In 2009, the American Recovery and Reinvestment Act (ARRA) was enacted, in part to support and promote the adoption of electronic health records (EHR’s) and the diffusion of health information technology.\textsuperscript{31} Approximately 160 billion dollars of federal funding has been funneled into programs aimed at improving and preserving health care, in part to support the adoption of electronic health information exchanges and the diffusion of health information technology.\textsuperscript{32} The federal government anticipated that public concern would accompany a transfer of health data onto a vast electronic exchange, unless there was “public assurance that the privacy and security of patient information in such systems were protected.”\textsuperscript{33} ARRA mandated several changes to health information privacy and security for HIPAA-covered entities through the establishment of the Health Information Technology for Economic and Clinical

\textsuperscript{28} HIPAA defines “protected health information” as “individually identifiable health information” that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” See 45 C.F.R. § 160.103 (2013).

\textsuperscript{29} “Treatment” is defined as the “coordination or management of health care services.” “Payment” is defined as “the activities of a health care provider to obtain reimbursement.” “Health care operations” includes “quality assurance initiatives, medical reviews, legal services, specified insurance functions, and general administration.” See 45 C.F.R. § 160.103 (2013).

\textsuperscript{30} 45 CFR § 164.502 (2013).


\textsuperscript{32} http://www.hhs.gov/recovery/.

Health Act of 2009 (HITECH Act).\(^{34}\) Prior to the HITECH Act, the HIPAA Privacy and Security Rules applied to electronic PHI, but only when in the possession of covered entities.\(^{35}\) Specifically, the Security Rule required covered entities to ensure the confidentiality of e-PHI by implementing and maintaining administrative, technical and physical safeguards.\(^{36}\) In addition, the Privacy Rule required appropriate safeguards to protect the privacy of personal health information, and set limits on when information could be used or disclosed without patient consent.\(^{37}\) The Rule also gives patients rights over their health information, including the right to examine and obtain copies of their records, as well as remedy errors within the records.\(^{38}\) Subtitle D of the HITECH Act, however, significantly expanded the scope of both the Privacy and Security Rules under HIPAA.\(^{39}\)

As with most large governmental enactments, the ARRA-mandated update to HIPAA was not a speedy one. Initiation of interim rules began in October 2009, and eventually led to the final implementation of the HIPAA Final Omnibus Rule, which was effective on March 26, 2013.\(^{40}\) The Final Rule represents the most significant development in health care privacy and security laws since the original HIPAA regulations were published.\(^{41}\) “Much has changed in health care since HIPAA was enacted over fifteen years ago,” said HHS Secretary Kathleen

\(^{35}\) Id.  
\(^{36}\) Id.  
\(^{37}\) See 45 CFR § 160 (a) and (e) (2013).  
\(^{38}\) Id.  
\(^{40}\) *HHS releases HIPAA Omnibus Rule*, ¶ 100-621, Department of Health and Human Services, 78 Federal Register 5566 (January 25, 2013). Note: though the rules became effective March 26, 2013, no entities were required to comply with the Final Rules until September 2013.  
Sebelius, in regards to the need for evolving HIPAA legislation. 42 “The new rule will help protect patient privacy and safeguard patients’ health information in an ever expanding digital age.” 43

The Final Rule addresses not only privacy and security rules governing protected health information (PHI), but also covers enforcement rules, breach notification rules, and genetic privacy provisions related to patient health information. 44 Arguably the most far-reaching, the Final Rule makes business associates of covered entities directly liable for complying with HIPAA requirements. 45 The Final Rule also specifically names the following three types of entities as falling within the “business associate” definition: 1) entities that both transmit and routinely access PHI on behalf of a covered entity (e.g., health information organizations, e-prescribing gateways, etc.), 2) personal health record vendors serving covered entities, and 3) business associate subcontractors. 46 Under the new rules, business associates (including regional health information organizations, health information exchanges, and software vendors) can be held accountable under the substantially higher fines for HIPAA violations to the same extent as a covered entity. 47 Some of the largest breaches reported to HHS have involved business associates. 48 In addition to the Final Rule’s business associate definition expansion, penalties for noncompliance attach to violating institutions, with a maximum penalty of 1.5 million dollars per

43 Id.
44 Lisa J. Acevedo & Jennifer L. Rathburn, supra note 33, at 4-5.
45 Id. at 4.
48 Press, Release, New rule protects patient privacy, secures health information, supra note 41.
violation.\textsuperscript{49} The changes also strengthen the HITECH Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS.\textsuperscript{50} The Rules also provide for a mandatory restriction request, which requires that a covered entity agree to an individual’s request to restrict disclosure of protected health information about the individual to a health plan when the disclosure “is for carrying out payment or health care operations” and the protected health information “pertains solely to a health care [item] for which the individual or person other than the health plan . . . has paid the covered entity in full.”\textsuperscript{51} Limitations on use and disclosures of PHI and prohibitions on PHI sales absent individual authorization were also further added to HIPAA, as were more objective breach standards and notification requirements in the event thereof. Lastly, the Final Rule prohibits most plans from using or disclosing genetic information for underwriting purposes, pursuant to the Genetic Information Nondiscrimination Act, which was enacted in 2008.\textsuperscript{52} The Final Rule became effective as of March 26, 2013, but full compliance was not required until September 23, 2013.\textsuperscript{53}

The Final Rules have extensive implications for both those entities that have traditionally fallen under HIPAA’s authority, and the new entities that have been incorporated during HIPAA’s expansions. The Final Rules extend the need for data constriction as further disclosure/nondisclosure options are afforded to patients on an individual level. In order for institutions to comply with the new self-pay and genetic information nondisclosure requirements, the entity must be able to restrict access accordingly. However, in order to restrict access to certain types of health information within the record, the capability to do so must exist within the

\textsuperscript{49} New rule protects patient privacy, secures health information, supra note 44.
\textsuperscript{50} Id.
\textsuperscript{51} HIPAA §164.522(a)(VI)(b) (2013).
\textsuperscript{52} HHS releases HIPAA Omnibus Rule, ¶ 100-621, Department of Health and Human Services, 78 Federal Register 5566 (January 25, 2013).
\textsuperscript{53} Id.
technological infrastructure of the exchanges. Further, the Final Rules move HIPAA enforcement away from the previous voluntary compliance network to a more draconian, penalty-based system.\textsuperscript{54} Adding teeth to the Act through a hefty new fine structure, and expansion of provisions that covered entities must follow, is likely to push compliance to the forefront.

V. **HEALTH INFORMATION EXCHANGES & THE INFRASTRUCTURE BREAKDOWN**

The regulatory environment in the United States following the HITECH Act, HIPAA notwithstanding, was no less stagnant, creating a further layer of complexity for patient privacy protection and compliance. On March 23, 2010, the Obama Administration established the first universal health care system in the history of the United States, signing into law the most expansive reform since the creation of Medicare and Medicaid in 1965.\textsuperscript{55} Under the Affordable Care Act, federal government-sponsored incentives are given to state and local health care systems, to be used towards health care technology and infrastructure implementation, including health information exchanges.\textsuperscript{56} Through the Health Information Technology Policy Committee and the Health Information Technology Standards Committee, Section 1561 of the Act requires the development of interoperable and secure standards and protocol that facilitate electronic exchanges.\textsuperscript{57} These exchanges provide a means of connecting health care providers and facilities to communicate health information in a way that will enhance patient treatment, reduce redundancies in medical services, and ultimately enhance the care of all patient populations.\textsuperscript{58}


\textsuperscript{56} **HIPAA: Impacts And Actions By States**, NATIONAL CONFERENCE OF STATE LEGISLATURES (February 2013), available at http://www.ncsl.org/research/health/hipaa-a-state-related-overview.aspx#Health_IT.

\textsuperscript{57} Id.

\textsuperscript{58} Id.
Though billions were allocated to the health care exchange initiative as part of the ARRA in 2009, the ACA’s further financial allocations were designed to accelerate the implementation and infrastructure needed to realize the benefits of electronic health records.

The term “health information exchange” encompasses two concepts: the action of electronic sharing of health-related information among organizations and the organization itself that provides the service to enable the sharing of health information across an electronic medium. Further, there are three forms of health information exchange: 1) a directed exchange where information is securely transferred between providers to encourage care coordination, 2) a query-based exchange in which a provider may obtain patient data from a repository, and 3) a consumer mediated exchange which gives the patient the ability to aggregate and use their own health information from all of their concurrent providers.

The Office of the National Coordinator for Health Information Technology has supplied funding for various HIE programs at both the state and federal levels. The Nationwide Health Information Network Exchange was developed under this financial umbrella and consists of stakeholders from federal agencies, delivery networks, and provider organizations, with a common goal of developing and implementing standards, services, and technology that will “foster secure health information exchange over the Internet.” In furtherance of the federal confederation’s goals, the ONC also awarded millions in grants to various states to pursue and develop their own information exchanges at a more local level. Over 90 million dollars of

---

60 Id.
62 Id.
63 Id. States received anywhere from 4.5 million (Delaware) to an upwards of 38 million (California) for their exchange programs, as of January 27, 2011. Further funding in total of $16 billion was provided under the HIE
federal funds have been divvied out in total, with the sole purpose of facilitating electronic exchanges.\textsuperscript{64}

With essentially fifty different initiatives on the table, there is the potential for fifty unique models of information exchange. Primarily, health information exchange structures have fallen into one of five models: 1) no consent, 2) opt-out, 3) opt-out, with granularity of choice, 4) opt-in, and 5) opt-in, with granularity of choice.\textsuperscript{65} The consent required for each model is somewhat self-explanatory. Individuals under the opt-out exchange are automatically enrolled unless they notify the administrator of their desire to be excluded, whereas opt-in requires the individual to give consent initially, or they will not be included within the exchange.\textsuperscript{66} An opt-out with granularity of choice allows the patient to opt out completely or just opt for a subset of data to be excluded within the exchange. An opt-in with restrictions model makes no patient health information available at the outset, but patients may allow all or only subsets of select data to be included for transmission.\textsuperscript{67}

Of the fifty states, twenty-two states have introduced and/or passed legislation that addresses patient consent for participation of their health information within the exchange. Sixteen of these states have utilized the opt-out model.\textsuperscript{68} The opt-out model tends to be the most popular for those states lacking any direct legislation around consent, most likely because this

\textsuperscript{64} Total grants, both from the initial allocation under and the HIE Challenge Grant Program totaled $96,291,512. See Health Information Exchange Challenge Grant Program, HEALTHIT.GOV, available at http://www.healthit.gov/providers-professionals/health-information-exchange-challenge-grant-program (last visited November 26, 2013).


\textsuperscript{66} Id. at 13-15.

\textsuperscript{67} Id.

\textsuperscript{68} Id.

12
approach is less costly and resource-intensive in obtaining all individual consent.\(^69\) However, in line with the protection of those within the opt-out model, the states must give sufficient notice to citizens in an effort to ensure that those that wish to be excluded have been afforded the opportunity to do so.\(^70\) Of over 200 organizations surveyed, 109 do not offer patients the ability to limit sharing of their information based on data type or source.\(^71\)

State statutes that provide more stringent health care privacy protections remain in effect even after HIPAA, and this conflict can affect the implementation of health insurance exchanges when at the state level.\(^72\) Although not specifically written for the ACA, the HIPAA Final Rules “will apply to virtually all people insured or treated, including those newly covered through exchanges, private employer coverage, and Medicaid expansions.”\(^73\) With more and more stringent penalties via the HIPAA Omnibus Rules, it is critical that covered entities and business associates can actually comply with the privacy and security laws, regardless of the format. Yet, the current technical capabilities of these entities operating on an electronic exchange do not allow for such a protection.


\(^70\) *Id.*


\(^72\) *HIPAA Privacy Rules for the Protection of Health and Mental Health Information*, supra note 21.

VI. **STATUTES V. SCIENCE: TECH SOLUTIONS TO THE PRIVACY PROBLEM**

Health plans, health care entities, and other providers that intend to participate in the health information exchange are likely to find a host of privacy and security stumbling blocks in their efforts to comply with the Final Rules. With electronic exchange of information comes greater convenience and efficiency in health care delivery, but not without greater data risk and liability. Some of the trickiest policy-related issues that health information exchanges face include: 1) how to best protect especially sensitive patient data; 2) how to deal with the patchwork of state regulations regarding consent; and 3) how to segregate patients’ self-pay information and other data points that the individual wishes to give even further protection under the HIPAA Final Omnibus Rules.

The implications of more stringent regulations, however, are causing great harm to the very populations of which the privacy regulations are trying to protect. In order to avoid inadvertent disclosure of particularly sensitive information, such as mental health or substance abuse treatment records, some HIEs, as a matter of policy, exclude any and all access to that data. Rather than trying to filter through the data to determine which portions of the information packet can be disclosed, total exclusion of that record is executed. In further policy sweeps, organizations that customarily contain that information, such as mental health centers, are excluded from the exchanges entirely. For instance, the Rochester Regional Health Information Organization’s exchange doesn’t allow substance abuse treatment centers to transmit

---

75 *Issue Brief: Privacy and Security in Health Care: A fresh look*, supra note 45, at page #.
77 Id.
78 Id.
79 Id.
patient data within the exchange, while the Colorado Regional Health Information Organization does not include any mental health clinics in their exchange network due to the need for patient consent.\textsuperscript{80} Others require manual filtering of sensitive data before sending the patient’s information on to the exchange.\textsuperscript{81} This “all or nothing” approach to inclusion of information that contains more heavily regulated information will only lead to large gaps in the individual’s continuum of care, and defeat the very goal of care coordination of which the health information exchanges were designed to effectuate.

\textbf{A. IS DATA SEGMENTATION THE ANSWER?}

In the wake of the HIPAA Final Omnibus Rules, and the ever-growing patchwork of state-specific privacy regulations, technological efforts have emerged as possible solutions to the complex issue that is keeping highly sensitive patient health information protected, yet fluid. Data segmentation is "the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization or individual as being undesirable to share."\textsuperscript{82} In other words, data segmentation is a technological means by which health care providers can separate the highly sensitive health information from the more general medical information, withhold access to certain information, and implement time frames of availability for that information by stakeholder.\textsuperscript{83} Essentially, data segmentation provides a means for electronically implementing choices under state and federal privacy laws.\textsuperscript{84}

\textsuperscript{80} Marianne McGee, \textit{supra note 76}. \textit{See also} Daniel & Posnack, \textit{supra note 63}, at 3.
\textsuperscript{81} Daniel & Posnack, \textit{supra note 63}, at 3.
\textsuperscript{82} \textit{Id.} at 2.
\textsuperscript{83} \textit{Id.}
Data Segmentation in health care can support granularity with respect to the following decisions: 1) what specific data is eligible for transfer on the exchange; 2) who may have access to the information; 3) when will access be granted for a particular data set; and 4) how long may access be granted for that particular viewer.\textsuperscript{85} Segmenting data to this level of granularity can benefit stakeholders who must comply with both federal and state laws that require this level of specificity.\textsuperscript{86}

A health information exchange with proper data segmentation would work as follows: Patient A, an individual that is HIV positive, goes to his primary care physician for his monthly exam, to monitor his condition and ensure compliance with his extensive medication regimen.

Patient A, an affluent and political figure in the community, chooses to pay for his care regarding his HIV diagnosis out-of-pocket, as he is fearful that information regarding his disease could get leaked to the media. With proper data segmentation, Patient A’s medical record for his primary care physician would reside within the health information exchange, yet the only records seen by entities other than his physician would be related to his other medical services, i.e. general health exams, and not his HIV diagnosis. In this case, and with many others under a data segmentation model, the patient’s information is as fluid as the patient wishes the information to be, yet is transferrable for purposes of care coordination.

Though the value of data segmentation is apparent, several obstacles will impede the widespread adoption of this technology. One of the biggest roadblocks to proper data segmentation in the current tech environment is the vast amount of legacy data.\textsuperscript{87} Electronic


\textsuperscript{86} \textit{Id.}

\textsuperscript{87} \textit{Id. at ES-11}. 
health information must be structured and coded so that computers can distinguish between the differing types, (e.g., general medical information versus information about HIV/AIDS treatment) and then treat them as distinct pieces of metadata.\textsuperscript{88} Many doctor offices and hospitals all across the nation have some combination of scanned paper documents, semi-interactive free text fields, and fully interactive electronic health records.\textsuperscript{89} Some of these documents, namely the legacy records, make it impossible to strip the metadata down to the granularity needed to necessitate data segmentation, which require the data to be presented in a codified manner so as to effectively tag the sensitive information.\textsuperscript{90}

Furthermore, more provider interaction with patients regarding their privacy is needed with a higher level of information granularity.\textsuperscript{91} Data segmentation will only work effectively with a proper patient consent management structure in place, which allows patients to effectively sign off on the disclosure of the sensitive, segmented data.\textsuperscript{92} A patient consent management tool enables the patient to designate who they want to share data with (using the above Patient A example, let’s say the patient consents to information disclosure to the AIDS Research Alliance of Chicago), and what data they wish to share (medication lists), and for what purposes (research).\textsuperscript{93} When a request for data is received, the software examines the request and presents the user with the relevant patient policies for that request (e.g., "The request is from an allowed physician but only allergy data is allowed to be communicated"), as well as any disclosure

\textsuperscript{88} Daniel, Posnack, & Pritts, supra note 82, at ES-2.
\textsuperscript{89} Id.
\textsuperscript{90} Id.
\textsuperscript{91} Id. at ES-3.
\textsuperscript{92} See Michael Berry & Naom Arzt, Managing Consent in an HIE Environment, HiMSS (February 7, 2013), available at http://www.himss.org/News/NewsDetail.aspx?ItemNumber=16405, for a discussion on patient consent management as it pertains to health information exchanges.
\textsuperscript{93} Dr. John D. Halamka, Consent tool lets patients control who/what/when access to EMRs, MED CITY NEWS (March 7, 2012), available at http://medcitynews.com/2012/03/consent-tool-lets-patients-control-who/what/when-access-to-emrs/.
allowances/prohibitions under the pertinent state and federal laws.\textsuperscript{94} Though extremely effective in limiting the proper information at the proper time, patient consent management tools require time on the part of the providers and active participation on the part of the patients, which can sometimes be difficult to achieve.\textsuperscript{95} In light of this, many health information exchange initiatives have moved towards asking patients to sign a comprehensive “catch all” consent form that leaves the patient with no choice other than to consent to share all sensitive information if they wish to participate in the HIE network.\textsuperscript{96}

However, this all or nothing structure does not effectuate the purpose of the exchanges. The purpose behind the establishment of health information exchanges was to “facilitate and expand the secure, electronic movement and use of health information among organizations according to nationally recognized standards.”\textsuperscript{97} The foundational notion behind the program is that the timely sharing of electronic health information can improve health care quality, efficiency, and safety.\textsuperscript{98} It does so by ensuring that health providers have access to comprehensive clinical information that allows them to provide better patient care.\textsuperscript{99} It also vastly expands the amount and quality of health-related data, which can improve public health programs and clinical research, and support quality, efficiency, and safety improvements.\textsuperscript{100} None of these goals can be fully realized if the exchanges are systematically excluding several subsets of individuals. Especially when those are individuals who utilize the health care system.


\textsuperscript{95} Halamka, \textit{supra note 91}.

\textsuperscript{96} Helen Oscislawski, \textit{supra note 68}, at 6.


\textsuperscript{98} \textit{Id}.

\textsuperscript{99} \textit{Id}.

\textsuperscript{100} \textit{Id}.
even more so than their counterparts, as their diagnoses that set them in the highly sensitive categories often require extensive medical services from a myriad of practitioners.\textsuperscript{101} Electronic implementation at the expense of the behavioral health, substance abuse, HIV, and self-pay patient is not a solution.

\textbf{VII. \textsc{The Case for Technologies and Legislative Collaboration}}

The need for data segmentation is known, and many health information exchange initiatives have begun to look to technological solutions to address the issue that sensitive information presents for the electronic exchanges.\textsuperscript{102} In 2006, the National Committee on Vital and Health Statistics recommended that the government assess the functionality of providing individuals with control over the access of their electronic health information when disclosed through the Nationwide Health Information Network.\textsuperscript{103} The HITECH Act required the Health IT Policy Committee to advise the ONC on a policy framework for a nationwide exchange, and in doing so, to examine the technologies that protect health information from disclosure.\textsuperscript{104} A 2010 report by the Presidential Council of Advisors on Science and Technology encouraged “a more granular protection of health information privacy,” more specifically, “the use of universal exchange language based on tagging of data elements, separated into the smallest individual pieces possible for HIE’s.”\textsuperscript{105} One year later, the ONC issued a Data Segment Initiative, known

\begin{flushright}
\textsuperscript{101} For example, “according to the latest CDC data, only twenty-five percent of people living with HIV in the U.S. have achieved viral suppression. In other words, three out of four people living with HIV in the United States have not been successfully supported in navigating the entire HIV care continuum.” See \textit{Improving the Quality of Health Care for Mental and Substance Abuse Conditions: Quality Chasm Series}, Chapter 5, available at http://aids.gov/federal-resources/policies/care-continuum/.

\textsuperscript{102} Helen Oscislawski, \textit{supra note 68}, at 6-7.


\textsuperscript{104} \textit{Id.}

\textsuperscript{105} \textit{Realizing the Full Potential of Health Information Technology to Improve Health Care for Americans: The Path Forward}, Report to the President (December 2010), available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.
\end{flushright}
as the Standards and Interoperability (S&I) Framework. The initiative includes private and public stakeholders working to establish interoperability impediments, and then finding solutions to those impediments. The initiative will focus on two use cases: one related to the sharing of information about patients in federally-assisted alcohol or drug abuse programs, and the other related to restricting information on self-pay visits from the insurer’s view.

Most recently, the Data Segmentation for Privacy Charter and Members Initiative (DS4Pi) arose from the S&I Framework led by the ONC, with a goal of setting up successful pilot tests of privacy protection as prototypes for workable solutions to the HIPAA privacy and security compliance complications. Staggered pilots testing different modalities have been initiated with various methods of tagging metadata for proper data segmentation. “By executing the various phases of the S&I Framework, DS4Pi has shown that standards can be used to apply privacy metadata at various layers of an information exchange using structured documents (document entry, document header, envelope, and transport) in order to restrict the flow of certain information while allowing others to flow more freely.” The initiative has proved that data segmentation standards can be used in health care in ensuring application and enforcement of obligations when handling sensitive health information.

---

106 See Standards & Interoperability Framework, available at http://wiki.siframework.org/ (last visited November 26, 2013). This is an “open government initiative,” an effort created by the Obama Administration, which relies on private participation to realize governmental objectives. In this case, under a set of guidelines and goals, private participants join the initiative and relinquish their work product to the S&I Framework as a potential solution to the interoperability impediments with HIEs.

107 Id.

108 Helen Pfister and Susan Ingargiola, supra note 100.


110 Id.


112 Id.
Therefore, legislative efforts should require specific quality standards in the continued development of HIE’s, with data segmentation stipulations and rules that set the floor for exchange capabilities, rather than further stipulating unrealistic privacy requirements. Current provisions are not actually attainable due to the antiquated status of our technological infrastructure, and a shift in focus for legislation to technological development is crucial to successful privacy efforts in the electronic environment. Results have shown that data segmentation is a possible addendum to the current infrastructure, and it is important that the data and results of the initiative do not go unutilized in our current exchange environment.

Most health information exchange models have been structured around the parameters set forth in the HIPAA Act, the HITECH Act, and other applicable federal and state privacy laws governing patient information. As of the date of this article, there continues to be no federal law that specifically governs networked electronic health information exchanges. Data segmentation provides a means for electronically implementing patient disclosure adoptions under new privacy laws. Therefore, in lieu of further regulations regarding patient privacy, the focus of the Office of the National Coordinator and other affected agencies should be on implementation of more stringent guidelines on health information exchange vendors. Specifically, the exchanges should possess the capability for data segmentation such that HIPAA and other sensitive information laws (e.g., HIV/AIDS; genetic information; STDs; etc.) can actually be enforced. The exchanges must be built with the capability of capturing the granularity needed in order to properly protect highly sensitive information, and further reinforced by legislative backing that forces providers to employ the technological and administrative protection.

113 Helen Oscislawski, supra note 68, at 4.
114 Id.
115 Duane Deconteau & Jonathan Coleman, supra note 81, at Why Segment Data? slide.
As data segmentation has the power to greatly effectuate change in the protection and security of patient information, the fostering of technological solutions to the current HIE barriers is a far better use of government resources. The Final Rules offer no exceptions for poorly designed systems, and as such, the importance of data segmentation implementation and agency guidelines on infrastructure requirements will become increasingly necessary, not only from a privacy standpoint, but also from a financial one as well.\textsuperscript{116} A law is only as good as its implementation. Further infrastructure efforts and structured requirements for vendors entering the HIE space will allow for the full implementation of the privacy standards.

\textbf{VIII. CONCLUSION}

For decades, stakeholders throughout the various sectors of health care have pushed for an electronic exchange by which health information could be transferred from entity to entity with ease, improving coordination of care and quality of health care.\textsuperscript{117} With the enactment of the American Reinvestment and Recovery Act and the Affordable Care Act, federal backing was directed toward health technology initiatives, and health information exchanges at both the state and federal level are becoming increasingly functional.\textsuperscript{118} This positive technological advancement, however, has put a strain on the privacy of an already sensitive type of information: health data.

When thinking about a health information exchange environment, it often feels like there are two diametrically opposed concepts competing. On one hand, the patient’s information needs to be accessible and mobile enough to be viewable in both the physician’s


\textsuperscript{118} See Press Release, Department of Health and Human Services, Data exchange growing through EHR adoption, new study finds (August 5, 2013) (on file with author).
office in their Illinois hometown, and the urgent care clinic in San Francisco. On the other hand, the highly sensitive nature of health information requires access controls and consent management at levels that ensure only the intended user has access. In an attempt to harmonize the two competing interests, legislative efforts were enacted, aimed at safeguarding particularly vulnerable information in the wake of the health information exchanges. The HIPAA Omnibus Final Rules and state privacy statutes have instituted provisions to further patient autonomy, and intensified the repercussions for covered entities and business associates that do not uphold the privacy and security rules. However, the technological structure lacks the sophistication to carry out the legislative purpose in separating data with proper granularity.

Data segmentation has the potential to “accommodate the requirements of the current legal framework while still enabling the significant benefits that result from electronic exchange to accrue.” Federal agencies and task forces have done much to research the issue, and have come to the general consensus that technological efforts should be developed to enable data segmentation at the initial record creation stage. Initial data segmentation will allow those responsible for the care of an individual’s sensitive health information (i.e. business associates, covered entities, and subcontractors) to have the capabilities to comply with the newly enacted legislation. Yet, not much has progressed beyond this point. Until there is more emphasis on the technological architecture that the health information exchanges so greatly depend on, it is unlikely that much effective progress will be made. Further, it is integral to the exchanges’ success in adhering to the privacy requirements that legislative and technology stakeholders collaborate in their efforts to ensure patient privacy on an electronic forum. Not all protected health information is created equally. However, with the proper combination of legislation that holds custodians accountable for the privacy and security of protected health information, along

119 Daniel & Posnack, supra note 82, at 3-4.
with the technology to segment and secure data accordingly, all protected health information can receive the appropriate level of protection as it navigates the electronic health information exchange.