DATA SEGMENTATION IN ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS

September 29, 2010

Prepared for:

Jodi Daniel, JD, MPH, Director, Office of Policy and Planning
Steven Posnack, MHS, MS, Division Director, Federal Policy
Joy Pritts, JD, Chief Privacy Officer
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by:

Melissa M. Goldstein, JD
Associate Professor
Department of Health Policy, School of Public Health and Health Services
The George Washington University Medical Center
2021 K Street, N.W., Suite 800
Washington, DC 20006

Alison L. Rein, MS
Director
AcademyHealth
1150 17th Street NW, Suite 600
Washington, DC 20036

With research assistance from:

Melissa M. Heesters, JD
Penelope P. Hughes, JD
Benjamin Williams
Scott A. Weinstein

The content of this whitepaper does not necessarily reflect the views or policies of the Office of the National Coordinator or the Department of Health and Human Services. The authors are solely responsible for the content.

Table of Contents

DATA SEGMENTATION IN ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS

EXECUTIVE SUMMARY

The issue of whether and, if so, to what extent patients should have control over the sharing or withholding of their health information represents one of the foremost policy challenges related to electronic health information exchange. It is widely acknowledged that patients' health information should flow where and when it is needed to support the provision of appropriate and high-quality care. Equally significant, however, is the notion that patients want their needs and preferences to be considered in the determination of what information is shared with other parties, for what purposes, and under what conditions. Some patients may prefer to withhold or sequester certain elements of health information, often when it is deemed by them (or on their behalf) to be "sensitive," whereas others may feel strongly that all of their health information should be shared under any circumstance.

This discussion raises the issue of data segmentation, which we define for the purposes of this paper as 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. This whitepaper explores key components of data segmentation, circumstances for its use, associated benefits and challenges, various applied approaches, and the current legal environment shaping these endeavors.

Data segmentation in the health care context can support granularity of choice with respect to the following:

- What specific data are eligible for exchange (from individual data elements to defined categories of data, such as all behavioral health records);
- Who has access to the information (from individual providers to other health care entities);
- Under what circumstances access is granted (*e.g.*, emergency access, treatment, *etc.*); and
- For what period of time access is granted (*e.g.*, unlimited, one-time access, *etc.*)

Collectively, these decisions reflect a set of information management preferences that theoretically could be executed by a number of parties, including individual patients, health care providers, provider organizations, or other legal entities. At present, however, these determinations are rarely made by the individual, and the question of who actually should have authority to determine and apply such preferences has emerged as a significant issue.

The impetus for protecting personal health information through the use of data segmentation is partially rooted in state and federal privacy laws addressing stigma and social hostility. Frequently cited laws such as the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (Part 2) vigorously protect specific health information from exchange without patient consent. Additionally, a host of less well-recognized, but equally stringent, state laws protect a broad range of information, for example health data related to minors or incidents

of sexual violence. Other justifications for the use of data segmentation in protecting health data include long-recognized principles of patient autonomy and the need to encourage greater patient trust and participation in the health care system.

Data segmentation provides a potential means of protecting specific elements of health information, both within an EHR and in broader electronic exchange environments, which can prove useful in implementing current legal requirements and honoring patient choice. In addition, segmentation holds promise in other contexts; the electronic capture of data in structured fields facilitates the re-use of health data for operations, quality improvement, public health, and comparative effectiveness research.

When discussing various data segmentation options in the health care context, several challenges also arise. These include:

- *Technical considerations, including the use of structured data.* Legacy systems and provider documentation practices (*e.g.*, reliance on free-text fields) often result in the recording of unstructured data. This scenario can complicate segmentation, which relies on the documentation of information in a structured and codified manner that can be managed through the application of rules engines and other intelligence systems.
- *Defining "sensitive information."* Pre-determining categories of information can ease the implementation of segmentation – both technically and logistically – but many patients express a strong preference for systems that enable them to convey their personal preferences more fully.
- *Consumer engagement.* Some approaches to segmentation would require and support deeper engagement on the part of the patient in determining and assigning segmentation preferences. These require consideration not only of the capacity of patients in this respect, but also their motivation to assume responsibility for the potentially daunting tasks associated with assigning and recording such preferences.
- *Provider reluctance.* At present, providers play a critical role in obtaining, documenting and honoring patient preferences with respect to personal health information. They also rely on the availability of accurate and relevant health information in order to provide appropriate and high-quality care. Segmentation policies must address the needs and concerns of providers as well as patients, including their concerns regarding quality and safety of the care provided, workflow implications, and liability.

Despite these issues, and largely due to existing legal requirements, electronic exchange with some level of data segmentation has succeeded to varying degrees in the U.S. The more developed solutions at this point are in very early stages, however, and others tend to enable segmentation only in contained environments. Varied segmentation policies, practices and applications have emerged, including the following:

- *Patient-controlled segmentation models.* In these models, patient preferences are recorded or entered by the patient and applied as information is exchanged. PHRs and health record banks are the primary examples of such models. However, this approach only allows patient control over a copy of his / her health record (not the provider's

documentation) and cannot guarantee that patient preferences will be honored once the information is released to another entity.

- *Individual provider-controlled models.* These models allow providers to act as patient proxies in recording patient preferences with respect to data sharing. Communication between patient and provider is critical to the success of these models, as is provider willingness. Some systems have successfully supported the exchange of information according to patient preferences, but typically operate as closed systems and do not permit segmentation preferences to extend to other settings.
- *Other systems, including organization-controlled models, hybrid models and innovative tools.* These systems often enable segmentation of information according to one or more jurisdictional, organizational or individual patient directive. Pilot programs are also in development to enable the use of consent management systems in exchanging health information between systems. When developing organizational policies, exchanges have indicated that receiving the input of key stakeholders, including consumers, is vital to success.

Other industries and international health information exchange efforts also offer promising examples and insight regarding data segmentation. Social networking sites in particular can illustrate how the public views privacy and the amount of granular control over personal information individuals generally prefer. International health information exchange efforts also can offer examples of ways to approach various issues related to data segmentation.

It is clear that enabling patient expression of preferences with respect to data sharing is critical to supporting consumer engagement. While consumer demand for segmentation tools may not be high at the present time, there is growing concern over the increasing availability of health information, which on its own or in combination with other data types might be used in ways not supported by individual patients and consumers. Notably, the advent of personalized medicine and increased availability of genetic information has been perceived by many as significantly changing the privacy discussion. Absent the ability to segment out specific data points within an EHR, the only alternative may be for entire health records to be exchanged routinely. This practice likely would lead consumers to engage in more privacy protective behaviors, thereby compromising achievement of better patient care and engagement in their health and health care. It could also diminish the overall utility of electronically-captured data for purposes other than direct care delivery.

As such, it will be important for policy makers to consider various approaches to moving not only the discussion, but also the meaningful realization of data segmentation, forward. Data segmentation efforts to date have explored a variety of approaches that show some early, but limited, success. To accelerate this forward momentum, we would suggest, among other pursuits, the following:

- *Build a Bridge to Greater Autonomy*: Rely on policy levers that will move us closer to the goal of supporting individual, subjective preferences for information management;

- *Provide Direct Financial and Other Support to Stimulate Change*: Consider various means of supporting the development of segmentation-enabling processes and technologies; and

- *Generate Evidence*: Given the significance of the transformation from paper to electronic means of data capture and sharing, establish and execute on a set of updated research priorities.

We support the idea of casting a wide net in search of appropriate means of providing patients more granular control over the exchange and use of their identifiable health information, and point to the efforts underway in other countries as evidence that this is a worthwhile endeavor. While still a challenge, data segmentation holds promise for accomplishing the ultimate goal of accommodating the needs and desires of the multiple stakeholders engaged in the electronic exchange of health information.

INTRODUCTION

In the context of electronic health information exchange, one of the most difficult issues encountered by policy makers at all levels is that of whether, and if so by what means and to what extent, to honor the preferences of individuals to share or withhold their health information from those who may benefit from its access (*e.g.*, providers of care, public health departments). In our highly-fragmented health care system, these stakeholders might not ordinarily have such access, especially when relying on paper records for clinical documentation.

Electronic health information exchange (hereinafter "electronic exchange"), whether it occurs via a state or other type of Health Information Organization (HIO),[1] via the Nationwide Health Information Network (NHIN),[2] or through NHIN Direct,[3] is perceived as the key mechanism by which we will be able to better integrate (albeit virtually) health care in the U.S. It is also widely believed that the use of electronic exchange is an essential condition for providing well-coordinated, high-quality care. That said, there continues to be vigorous debate about the role of the individual patient[4] in determining whether and how such information should flow.

On the one hand, it is widely acknowledged that information about patients and their health needs to go where it is needed, when it is needed, and be accessible to those who can use it to make important treatment and other care-related decisions. On the other hand, there is recognition that, if we truly are to reap the benefits of electronic exchange, patients must be assured that appropriate privacy and security provisions are established and enforced. Moreover, patients need to be assured that their needs and preferences are considered in the determination of what information is shared with other parties, for what purposes, and under what conditions. Implicit in this discussion is the idea that some patients may prefer to withhold or sequester certain elements of health information, often when it is deemed by them (or on their behalf) to be "sensitive." It is in this context that the issue of data segmentation in health care arises.

---

[1] As used in this paper, the term "HIO" means an organization that oversees and governs the exchange of health-related information. *See* The National Alliance for Health Information Technology, *Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms*, April 28, 2008.

[2] "NHIN" refers to "a set of standards, services and policies that enable secure health information exchange over the Internet." *See* Office of the National Coordinator for Health Information Technology. *Nationwide Health Information Network: An Overview*. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nationwide_health_information_network/1142

[3] "The NHIN Direct project develops specifications for a secure, scalable, standards-based way to establish universal health addressing and transport for participants (including providers, laboratories, hospitals, pharmacies and patients) to send encrypted health information directly to known, trusted recipients over the Internet." *See* NHIN Direct. *The NHIN Direct Project: What is Direct?* Available at: http://nhindirect.org/.

[4] Although the terms "patient" and "consumer" are sometimes used interchangeably, for the purposes of this paper we generally use the word "patient" to mean a person who is engaged in the process of expressing his / her preferences (typically in a care setting or context) with respect to the inclusion in and / or exchange of his / her health information through electronic exchange. We use the word "consumer" in particular contexts, such as "consumer participation" in focus groups or "consumer groups."

What is Data Segmentation in the Health Care Context?

At its core, the term "data segmentation" refers to 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. This basic definition, however, does not account for the multiple permutations of segmentation in the health care context (*i.e.*, granularity), nor does it adequately capture the varied considerations required for development of segmentation policy. After an initial discussion of the policy rationale for data segmentation, the core components of segmentation (as commonly applied in the electronic exchange context) are described below.

Why Segment Health Care Data?

State and federal laws related to sensitive health information often drive the need for data segmentation. As health information is exchanged electronically, numerous laws and regulations that define and protect certain types of sensitive health information will apply. Most states currently have laws addressing information in health records related to HIV status, mental health conditions and substance abuse, while some states also have laws protecting genetic information.[5] A recent overview of health provisions in state statutes illustrates the wide variety of conditions that may be considered sensitive.[6] The state of Illinois, for example, has statutes restricting access to information related to alcoholism and substance abuse, cancer, genetic test results, head and spinal cord injuries, HIV / AIDs, mental health and developmental disabilities, and STIs, while the state of Wyoming places condition-specific restrictions on information related to genetics, mental health and STIs.[7] In addition, federal laws and regulations including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides for the promulgation of privacy and security regulations (the HIPAA Privacy and Security Rules),[8] the Health Information Technology for Economic and Clinical Health (HITECH) Act[9] and the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (Part 2),[10] among others, specify privacy rights related to sensitive health information.

Privacy laws protecting the confidentiality of sensitive health information have long been used to address the stigma and social hostility associated with specific health issues, with the level of protection applied by law varying with respect to the type of disease at issue.[11] Such laws typically conform to prevailing social norms concerning stigmatizing conditions and

---

[5] Consumer Partnership for eHealth. *Protecting Sensitive Health Information*, June 2010, at 2-3. Available at: http://www.nationalpartnership.org/site/DocServer/Sensitive-Data-Final_070710__2_.pdf?docID=7041.

[6] Pritts, J. et al. "The State of Health Privacy: A Comprehensive Survey of State Health Privacy Statutes," August 8, 1999. Available at: http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf (Volume 1) and http://ihcrp.georgetown.edu/privacy/pdfs/statereport2.pdf (Volume 2).

[7] *Id.*

[8] 45 C.F.R. §§ 160, 164 (2009). Please see the Legal Analysis section later in this paper for a fuller discussion of HIPAA and the HIPAA Privacy Rule.

[9] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII, Division A of the American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, §§ 13001-13424, 123 Stat. 115, 228-279 (2009).

[10] 42 C.F.R. pt. 2 (2009). These regulations were promulgated pursuant to the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Pub. L. No. 91-616, 84 Stat. 1848, and the Drug Abuse Office and Treatment Act of 1972, Pub L. No. 92-255, 86 Stat. 65. The rulemaking authority granted by both statutes relating to confidentiality of records can now be found at 42 U.S.C. § 290dd-2 (2006).

[11] Gostin, L.O. et.al. "The Law and the Publics Health: A Study of Infections Disease Law in the United States." *Columbia Law Review*, Vol. 99, No. 1, January 1999, pp. 59 – 128.

contemporary standards regarding methods of assessment and intervention.[12] In addition, experts note that the role of law in addressing stigma related to a health condition may change as the strength or power of the stigma changes.[13]

While there is variation in the application and requirements of these laws, in general they limit the exchange of certain health information without patient consent,[14] often quite stringently and explicitly. For example, Part 2 strictly limits the disclosure and use of information regarding individuals in federally assisted alcohol or drug abuse treatment programs, and any information that could reasonably be used to identify an individual seeking or obtaining education or treatment is protected.[15] In addition, pursuant to HITECH, patients paying out-of-pocket in full for treatment have the right to request that providers restrict the disclosure of their personal health information to health plans.[16] In some states, the law even precludes disclosure of certain types of sensitive information in an emergency.[17] Typically, the underlying purpose of such laws and regulations is to encourage greater participation and trust in the health care system through protection of a patient's most personal and private health information, thus addressing a possible disincentive for seeking services.[18] However, because the patchwork of laws regarding sensitive information in health records is neither consistent nor comprehensive, compliance can be challenging for those initiating electronic exchange.[19]

In the face of this challenge, some organizations have chosen simply to exclude entire categories of health information from exchange, resulting in the absence of important health data in patients' records. For example, the Colorado Regional Health Information Organization (CORHIO), discussed in more detail later in this paper, has chosen for the near term to exclude from exchange any records originating from mental health clinics. The organization attributes this policy decision to the perceived difficulty of separating out references to mental health that may appear in an individual's record and that may require consent for disclosure.[20] Data segmentation offers a potential solution to this dilemma by offering the possibility of sequestering select information from the rest of a record for purposes of exchange. In theory, data segmentation is the tool that could accommodate the requirements of the current legal

---

[12] Gostin, L.O. "Public Health Law Reform." *American Journal of Pubic Health*, Vol. 91, No. 9, September, 2001, pp. 1365-68.
[13] Burris, S. "Disease Stigma in U.S. Public Health Law." *Journal of Law, Medicine and Ethics,*" Vol. 30, No. 2, Summer 2002, pp. 179-90.
[14] For the purposes of this paper, we use the term "consent" generally to refer to patient permission to include personal health information in and / or exchange it through electronic exchange.
[15] Goldstein, M.M. and A.L. Rein. *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*," March, 2010. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf.
[16] HITECH § 13405, 123 Stat. 115, 264-265 (2009) (to be codified at 42 U.S.C. § 17935).
[17] *See, e.g.*, Maine, ME. REV. STAT. ANN. tit. 5, § 19203, and Massachusetts, MASS GEN LAWS ch. 111, § 70F, which prohibit disclosure of HIV testing results even in an emergency.
[18] Pritts, J.D. "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." *National Academy of Sciences*, 2008, at 12. Available at: http://www.iom.edu/Activities/Research /HIPAAandResearch.aspx.
[19] Consumer Partnership for eHealth, *supra* note 5, at 3.
[20] Phone call with Carrie Book, Chief Information Officer, Colorado Regional Health Information Organization, May 19, 2010.

framework while still enabling the significant benefits that result from electronic exchange to accrue.

In addition to meeting the requirements of state and federal law, data segmentation can also be used to offer a fuller expression of patient preferences with respect to the sharing of personal health information, thus supporting underlying principles of personal autonomy and encouraging patient engagement. For a variety of reasons – ranging from fear of discrimination to concern for physical safety – individuals may prefer to keep certain types of health information strictly private.[21] Personal autonomy, in the context of bioethics, is the principle on which an individual patient's right to make and carry out informed decisions regarding his / her health is based, including decisions regarding access to personal health information.[22] Autonomy has been described as "the accepted rationale" for ensuring the confidentiality and privacy of health information,[23] and there is considerable justification for basing policies regarding consent to the sharing of one's health information on the principles of autonomous decision making.[24] As such, patient autonomy should be a key consideration in the development of policies related to the electronic exchange of health records. Segmentation could potentially provide a robust tool for realizing principles of personal autonomy by empowering patients with a technical means of protecting specific data elements within a patient's health record.

Along with supporting patient autonomy, segmentation can also build respect for patient privacy and trust, which are critical elements with respect to patient participation in information sharing.[25] According to research by the California HealthCare Foundation, 15 percent of patients who know their information will be shared would hide information from their doctor, and another 33 percent would consider hiding information.[26] As a result, the Consumer Partnership for e-Health, among other organizations, has urged consumer groups that focus on the protection of electronic health data to consider solutions that enhance patient trust generally, as well as strengthen the patient-provider relationship.[27] Data segmentation, in particular segmentation at a granular level, could offer a means of enabling patient control over personal health information within an electronic environment, and may therefore hold great potential for enhancing patient trust and engagement in the care process.

There are also legitimate medical reasons for enabling the segmentation of data within a medical record. For example, studies have identified hindsight and outcome bias in the medical context – that is, the inclination for a provider to place undue emphasis on a prior diagnosis in the record –

---

[21] Goldstein, *supra* note 15.
[22] Goldstein, M.M. "Health Information Technology and the Idea of Informed Consent," *Journal of Law, Medicine, and Ethics*, Vol. 38, No. 1, March 26, 2010, pp. 27-35.
[23] Terry, N.P. and L.P. Francis. "Ensuring the Privacy and Confidentiality of Electronic Health Records," *University of Illinois Law Review*, Vol. 2007, No. 2, February 28, 2007, pp. 681-736.
[24] Goldstein, *supra* note 22.
[25] *See e.g.*, Health IT Policy Committee, Privacy and Security Tiger Team. *Letter to David Blumenthal, Chairman of the Office of the National Coordinator for Health IT*, August 19, 2010. Available at: http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf (discussing trust between patients and their providers as a core value to guide ONC's work to promote HIT).
[26] California HealthCare Foundation. *Consumers and Health Information Technology: A National Survey*, April, 2010. Available at: http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.
[27] Consumer Partnership for eHealth, *supra* note 5.

as a significant contributor to medical errors.[28] The ability for a patient to purge or at least sequester an erroneous diagnosis from a medical record could help reduce the negative outcomes that can occur as a result of these biases.[29]

In addition to individual preferences or concerns about loss of privacy, segmentation plays an important role in the context of the broader consumer protection landscape. One area of concern is that of compelled disclosure of health information for non-care related purposes. Laws that address privacy (*e.g.*, HIPAA, the Genetic Information Nondiscrimination Act of 2008 (GINA)[30]) do little to address compelled disclosure of information – often health-related – for employment, insurance, loan and other applications.[31] For example, experts have noted that it is lawful for employers to require individuals to sign authorizations of unlimited scope for the release of their health records as a condition of being employed.[32] Further, once data are disclosed to a non-HIPAA covered entity, there are very few legal restrictions preventing further dissemination.[33]

Given the likely volume of such "compelled authorizations" per year,[34] and based on the fact that greater availability of health information in electronic form will likely make it more readily available for such disclosures, some argue that the need for increased individual control is heightened. The transition from paper to electronic data capture could greatly increase the amount of data people may be compelled to disclose for employment, insurance, and other purposes. It has been suggested that, as a direct result, medical privacy may be compromised to a degree that would have been impossible with paper records only, which are by nature fragmented and therefore protected to some degree by the logistical difficulty associated with their identification and collection.[35] Further, even with adequate data protection against unauthorized disclosure, individuals may not wish to disclose all or a large portion of their health data, particularly in cases of sensitive data, or in situations where the data would be held by someone whom the individual knows (such as in the case of small towns or employment in small companies).[36]

What Types of Information do Patients Typically Wish to Segment?

There has been substantial debate regarding what constitutes sensitive information, and many have argued that the criteria for determining which pieces of health information warrant a sensitive label is highly subjective. However, in general, those who have attempted to distinguish sensitive information have considered it to be information that presents unusually

---

[28] Henriksen, K. and H. Kaplan. "Hindsight Bias, Outcome Knowledge and Adaptive Learning," *Quality and Safety in Health Care*, Vol. 12, Suppl. II, December 1, 2003, pp 46-50.
[29] *Id.*
[30] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (to be codified in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).
[31] Rothstein, M.A. and M.K. Talbott. "Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy," *JAMA*, Vol. 295, No. 24, June 28, 2006, pp 2882-85.
[32] Rothstein, M. A. and M.K. Talbott. "Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications," *The American Journal of Bioethics*, Vol. 7, No. 3, March 1, 2007, pp. 38-45.
[33] Rothstein, *supra* note 31.
[34] *Id.*
[35] *Id.*
[36] *Id.*

high risks of harm to the patient in the event of disclosure.[37] Such risks of harm could include discrimination, social stigma, or even physical harm (for example, harm resulting from the release of personal health information in situations involving intimate partner violence).[38] Over time, consensus has emerged that certain categories of health information require more focused protection than others and, as discussed earlier, many state and federal laws have designed laws and policies accordingly. Categories often considered to be sensitive include domestic violence, genetic information, mental health records, reproductive health records, substance abuse records, and records for patients having a personal relationship to an individual at the relevant health care facility.[39]

It is important to note, however, that it is not necessary for information to be defined as sensitive in order for it to be appropriate for segmentation. Patients may want to segment information purely due to personal preferences or based on individual values.[40] Also, a patient may have unique circumstances or sensitivities resulting in a desire to keep private certain personal health information that would not be considered sensitive by statute or conventional wisdom.

Components of Data Segmentation

At What Level is the Information Blocked (i.e., capture, access, or view?)

Though this has not (yet) been a source of great discussion in the context of segmentation, the variety of exchange models under consideration and development in the U.S. will likely affect the stage of exchange at which segmented information is blocked. In some exchanges, for example, the information shared is available in computable form and can readily be incorporated into other data repositories. This means that electronic copies of the information could be disseminated further into the health care system. In other exchanges, the information is only made available in a read or view-only mode. In such a system, absent manual entry into an electronic health record (EHR) or other data repository, the information is not actually copied (and is therefore potentially less widely available). It is possible that individual preferences for information sharing could be influenced by these variations.

Who Gets to Make the Determination?

In many discussions of data segmentation, it is presumed that individual patients should determine the rules and protocols for the sharing of their information. Many consumer advocates view this as the ultimate goal of data segmentation, but it should be mentioned that other entities within and surrounding the health care sector now have (and likely will continue to have) some authority in this domain. Such entities include:

- Legal entities (*e.g.*, states)
- Institutions (*e.g.*, hospitals)
- Organizations (*e.g.*, HIOs)

[37] Consumer Partnership for eHealth, *supra* note 5.
[38] *Id.*
[39] *Id.*
[40] Goldstein, *supra* note 15.

An individual with a history of drug and alcohol abuse, for example, may wish to authorize blanket consent to have any of his / her health information available to all of his / her current and possible care providers under any circumstance. As described above, however, many state laws stipulate that certain sensitive information cannot be shared absent express consent. Further, as will be discussed in greater detail later in this paper, the application of numerous institutional and organizational protocols have implications for the execution of direct patient preferences.

Who Has Authority / Ability to Apply Segmentation Preferences?
Though segmentation determinations may be intended to accommodate or address individual preferences with respect to information sharing, it is not (yet) typical for individuals to apply their preferences directly to a system or systems. At present, this direct application model is only accommodated by systems developed for the personally controlled health record (PCHR / PHR) market. The dominant model is for preferences to be put in place by a provider (possibly via an EHR or other application), or by an institution or organization acting on the individual's behalf. In different ways and through a variety of media, each of these methods can and have been used to record, manage and adjudicate segmentation preferences.

Core Components (i.e., the what, who, why and when)

Consistent with the saying "the devil's in the details," so too is the way of segmentation. Simply put, data segmentation involves making choices among many options and for varying reasons. For this reason, most individuals and institutions prefer to establish a set of parameters around the act of segmentation that better define and limit electronic exchange. These include the following:

- What data are eligible for exchange?
  Individual preferences for information sharing are highly subjective, and vary greatly depending on personal values, perspectives, experiences, and beliefs. What one person considers highly personal and sensitive, another person may willingly share. Despite this variation, state and federal laws, institutions and organizational entities have all – in various ways – established categories of sensitive information that are afforded special or different treatment.

- Who can gain access?
  Individual preferences also vary with respect to the determination of who they will trust with all or certain parts of their health information. For example, an individual may wish to share information about a rare disorder only with a specific set of health care providers. Further, these preferences are likely to be highly contextual. Extending the above example, that individual may alter his / her sharing preferences to be more inclusive of other providers in an emergency situation. In addition, we know from research[41] that patients trust their providers (*e.g.*, doctors, nurses, pharmacists) far more than they trust other entities (*e.g.*, employers, health insurers) with their information.

- Under what circumstances (why)?

[41] *See e.g.*, Henry J. Kaiser Family Foundation. *Kaiser Health Tracking Poll: April 2009*, April 23, 2009, Publication #7892. Available at: http://www.kff.org/kaiserpolls/7892.cfm.

Another factor influencing individual preference with regard to segmentation is the purpose of information sharing. That is, for what reason does the requesting (or permitted) party desire the information? Survey data have shown that a large majority of the public wants electronic access to their health information – both for themselves and for their health providers – because they believe such access is likely to increase the quality of their health care.[42] By comparison, a significant proportion would object to exchange of that same information if it were to be used for other purposes. Data from a 2006 survey in which Americans were asked about the benefits and concerns of online health information reveal that 77 percent were "very concerned" about their medical information being used for marketing purposes.[43] A recent Canadian study also found that the willingness to share data decreases when data will be used for commercial, for-profit use and marketing.[44] In addition, a study by Johns Hopkins in 2003 found that 31 percent of respondents were willing to share medical records for research purposes if it would increase medical knowledge, but over 50 percent of those same respondents were unwilling to allow the use of their records in research without consent.[45] However, a 2006 survey commissioned by the Markle Foundation found that 75 percent of respondents were willing to share de-identified personal health information for research purposes.[46] Interestingly, one recent study of PHR users found that respondents were more willing to share personal health information for research purposes when provided with some amount of granular control over which information would be shared.[47]

- For what period of time?
  The final core component of segmentation is the issue of time frame or duration. Though less frequently discussed in the literature than other aspects of segmentation, this element refers to the possibility that individuals would prefer to segment out certain parts of their health care record from a specified period of time.[48] For example, an individual with a history of substance abuse may, having recently spent time in a rehabilitation facility, wish to segment all health information captured during that time period in order to prevent it from being shared with other non-facility providers.

The Public Data Segmentation Debate

On June 22, 2006, the National Committee on Vital and Health Statistics (NCVHS) sent a letter to Michael O. Leavitt, then Secretary of the U.S. Department of Health and Human Services (HHS), entitled "Privacy and Confidentiality in the Nationwide Health Information Network."[49]

---

[42] Markle Foundation. *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*, November 2006. Available at: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.
[43] *Id.*
[44] Willison D.J. et al. "Consent for Use of Personal Information for Health Research: Do People With Potentially Stigmatizing Health Conditions and the General Public Differ in Their Opinions?" *BMC Medical Ethics*, Vol. 10, No. 10, July 24, 2009, pp 1-12.
[45] Terry, *supra* 23.
[46] Robert Wood Johnson Foundation. *Project HealthDesign E-Primer 2: Rethinking the Power and Potential of Personal Health Records*, December 2007. Available at: http://www.projecthealthdesign.org/media/file/ProjectHealthDesignPrivacyePrimer.pdf.
[47] Weitzman, E.R. et al. "Sharing Medical Data for Health Research: The Early Personal Health Record Experience," *Journal of Medical Internet Research*, Vol. 12, No. 2, May 25, 2010.
[48] Goldstein, *supra* note 15.
[49] NCVHS. *Letter to the Secretary of Health and Human Services re: Recommendations Regarding Privacy and*

The letter recommended that HHS should "assess the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means. Decisions about whether individuals should have this right should be based on an open, transparent, and public process."[50]

In an effort to provide policy makers with greater detail regarding its recommendations, the NCVHS Subcommittee on Privacy, Confidentiality and Security (Subcommittee) conducted hearings on April 17, 2007. Testimony was presented by experts in several of the medical professional fields that are thought of as handling particularly sensitive health information, as well as others with relevant expertise. NCVHS engaged in extensive deliberations on these matters, which culminated in a series of recommendations submitted to the Secretary in February of 2008.[51] It should be noted that NCVHS's deliberations considered the issue of segmentation (referred to by the group as "sequestering") in the limited context of exchange within the NHIN, and for treatment purposes only. That said, the group's discussion and recommendations referenced several components outlined above, such as the desired level of individual control, the types of data that might be subject to special treatment, and the level of granularity permitted.

The recommendations made by NCVHS were intended to strike a balance between the unique desires expressed by individuals and the necessity to account for other interests and policy considerations as well as the feasibility of implementation. The advisory body concluded that "NHIN policies should permit individuals limited control, in a uniform manner, over access to their sensitive health information disclosed via the NHIN."[52] This system would require the following:

- Identification of categories of sensitive health information;
- Allowance of optional sequestering of certain categories;
- Inclusion of notations to health care providers of sequestered health information;
- Implementation of computer-based decision support; and
- Establishment of provisions for emergency access to all of an individual's health information.

The group also recommended that a public dialogue should be undertaken to develop the specifics of these policies, and that pilot projects should be initiated to test their implementation.

On June 15, 2010 the Subcommittee held a hearing to discuss further the issue of sensitive information in medical records. While the 2008 recommendations issued by NCVHS provided five examples of categories of sensitive information that would be appropriate for segmentation (domestic violence, mental health, reproductive health, substance abuse and genetic information), the Subcommittee felt the need to explore these and other categories of information

---

Confidentiality in the National Health Information Network, June 22, 2006. Available at: http://www.ncvhs.hhs.gov/060622lt.htm.

[50] *Id.* at R-6.

[51] NCVHS. *Letter to the Secretary of Health and Human Services re: Individual Control of Sensitive Health Information via the Nationwide Health Information Network for Purposes of Treatment*, February 20, 2008. Available at: http://www.ncvhs.hhs.gov/080220lt.pdf.

[52] *Id.* at 2.

that may deserve special protection further.[53] In this latest hearing, the Subcommittee specifically considered genetic information, mental health information, the health information of children and adolescents and other sensitive information, such as the health records of VIPs and of young adults covered under a parent's insurance policy.[54]

Discussion and examination of issues related to data segmentation have also occurred under the auspices of the Health Information Technology Policy Committee (HIT Policy Committee), a Federal Advisory Committee formed to make recommendations to the National Coordinator for Health Information Technology on HIT policy issues.[55] In the HITECH Act, Congress instructed the HIT Policy Committee to make recommendations with respect to data segmentation;[56] as part of that consideration, on June 29, 2010, the Privacy and Security Tiger Team (Tiger Team), a workgroup of the HIT Policy Committee, sponsored a Consumer Choice Technology Hearing.[57] The hearing focused on the use of technology to implement individual choice, examining both its capabilities and limitations in that respect.

Additionally, the HIT Policy Committee directed the Tiger Team to focus on a series of questions related to the exchange of personally identifiable health information.[58] One issue examined by the Tiger Team at the request of the Office of the National Coordinator (ONC) has been "the ability of technology to support more granular patient consents (*i.e.*, authorizing exchange of specific pieces of information while excluding other records)."[59] Draft recommendations by the Tiger Team with respect to this issue conclude that technology enabling granular segmentation is promising, but still in the early stages of development, thus necessitating further exploration and innovation.[60] The recommendations stress that a successful technical solution must demonstrate effective use by patients and fulfillment of patient expectations.[61] They also note that until such a technical solution is developed and uniformly applied, it is critically important to educate patients regarding the extent to which their preferences realistically can be honored.[62]

HEALTH INFORMATION PRIVACY LAWS THAT DRIVE THE NEED TO SEGMENT DATA

This section generally describes the legal environment in which data segmentation in electronic exchange is developing, but is not intended to be a comprehensive legal review. Numerous and varied laws, both state and federal, form the structure of this environment, but it is beyond the

---

[53] NCVHS. *Hearing of the Subcommittee on Privacy, Confidentiality and Security: Sensitive Information in Medical Records*, June 15, 2010. Available at: http://www.ncvhs.hhs.gov/100615tr.htm#introduction.
[54] *Id.*
[55] HITECH, Pub. L. No. 111-5, § 13101, 123 Stat. 115, 228-230 (2009) (to be codified at 42 U.S.C. 300jj-11).
[56] HITECH § 13101.
[57] Health IT Policy Committee, Privacy and Security Tiger Team. *Consumer Choice Technology Hearing Transcript*, June 29, 2010. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_945903_0_0_18/Consumer-Choice-Technology-Hearing-062910.pdf.
[58] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25.
[59] *Id.* at 4.
[60] *Id.* at 16.
[61] *Id.* at 15.
[62] *Id.* at 12.

scope of this paper to review all of these laws. Instead, select individual statutes and regulations will be examined along with certain specific health conditions or types of data that are generally considered sensitive and therefore protected by legislation. The section will also explore some of the types of health records most commonly protected by state laws, including mental health and HIV-related records, as well as a few topics addressed less frequently in discussions of segmentation, such as intimate partner violence. Despite the considerable variation in the applicable state and federal laws, however, they do have a common, overarching purpose—encouraging and enhancing patient participation in the health care system. By constructing a protective legal environment for sensitive health information, privacy protective behavior by patients, such as avoiding treatment for a sensitive health issue, may be lessened.

Individual Laws

HIPAA and the Privacy Rule

The HIPAA Privacy Rule is the key federal law that shapes the legal environment underlying data segmentation in electronic exchange.[63] The Privacy Rule generally allows the disclosure of protected health information (PHI) [64] for the purpose of treatment, payment or health care operations without the express permission of the patient. There are exceptions to this rule, however. For example, release of psychotherapy notes requires specific authorization by the patient except under very limited circumstances.[65] In cases such as these, the information at issue (*e.g.*, psychotherapy notes) may need to be segmented from other clinical data in order to maintain the privacy of the information and protect it from unlawful disclosure.

The Privacy Rule's "minimum necessary" requirement may also hold particular relevance for segmentation of data in electronic exchange. The Rule requires covered entities to take reasonable steps to limit the use or disclosure of and requests for PHI to the minimum necessary to accomplish the intended purpose,[66] but does not apply to disclosures to or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information.[67] Thus, the amount and type of information that an entity may appropriately exchange may vary with the intended purpose of the disclosure. If an entity exchanges information for treatment purposes only, its operations are not constrained by the minimum necessary requirement. If the entity exchanges PHI for purposes more accurately described as payment or health care operations (or other permitted purposes), however, it may be necessary to segment the data to meet the minimum necessary standards.

---

[63] For a discussion of HIPAA's basic structure, *see* Goldstein, *supra* note 15.

[64] The Privacy Rule defines protected health information as "individually identifiable health information" that is held or transmitted by a covered entity in any form, including electronic, paper, and oral media, subject to certain limited exceptions (such as the exclusion of employment records). 45 C.F.R. § 160.103 (2009).

[65] Exceptions include use by the originator of the psychotherapy notes in treatment, use by the covered entity in specific types of training programs and use by the covered entity in defending a legal action brought by the individual patient. 45 C.F.R. § 164.508 (a)(2). HITECH directed the Secretary of HHS to examine the definition of psychotherapy notes with regard to including test data related to mental health evaluations. HITECH, Pub. L. No. 111-5, § 13424(f), 123 Stat. 115, 277 (to be codified at 42 U.S.C. § 17953). Final recommendations / conclusions on the issue have not yet been issued.

[66] 45 C.F.R. § 164.502(b) (2009).

[67] 45 C.F.R. § 164.502(b) (2009).

Finally, it is important to note that HIPAA provides a baseline standard of privacy protection for health information—federal and state laws that offer more stringent privacy protections are not superseded by the Privacy Rule.[68] A considerable body of privacy law at the state level currently exists[69] and, as a result, an entity's decisions regarding data segmentation will likely be affected by state privacy laws.

HITECH

The HITECH Act recently amended HIPAA by expanding its reach, strengthening certain aspects of the regulations, and increasing federal enforcement tools.[70] Regulations implementing the law's provisions are currently being promulgated, some of which will affect data segmentation in electronic exchange directly. For example, providers now must honor a patient's request to restrict disclosure of PHI related to treatment or services for which the patient has paid out-of-pocket where the purpose of the disclosure is for payment or health care purposes and is not otherwise required by law.[71] The provision does not apply to disclosures made for treatment purposes. Thus, for example if an individual paid cash for treatment of a sexually transmitted disease, he or she has the right to prohibit disclosures for payment or health care operations purposes but not for those related to treatment. In order to comply with this provision, an exchange therefore may need to develop a segmentation mechanism by which a person's information could be exchanged for treatment purposes, but not for payment or health care operations purposes.

In addition to expanding the privacy protections of HIPAA, HITECH created an incentive program "for adoption and meaningful use of certified EHR technology" that will impact choices regarding the creation of electronic exchange systems.[72] The Centers for Medicare & Medicaid Services (CMS) recently issued a final rule outlining key concepts regarding meaningful use of EHR technology and providing a definition of meaningful use.[73] The rule will phase in more robust criteria in three stages, with the first stage beginning in 2011 and focusing on capturing health information in a coded format, tracking health information and key clinical conditions, and communicating that information for care purposes and quality reporting.[74] Stages 2 and 3

---

[68] 45 C.F.R. § 160.203 (2009).

[69] Goldstein, M.M. et al. *Emerging Issues in Health Information Privacy*, in "Health Information Technology in the United States: Where We Stand, 2008" (Blumenthal, D. et al. eds., 2008). Available at: http://www.rwjf.org/pr/product.jsp?id=31831.

[70] HITECH Pub. L. No. 111-5, §§ 13101-13424, 123 Stat. 115, 228-279 (2009).

[71] HITECH § 13405, 123 Stat. at 264-265 (2009) (to be codified at 42 U.S.C. § 17935); see also Modifications to the HIPAA Privacy, Security and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40867, 40899 - 40901 (proposed July 14, 2010) (to be codified at 42 C.F.R. Parts 160 and 164).

[72] HITECH, Title IV, Division B, Pub. L. No. 111-5, §§ 4101-4201, 123 Stat. 115 (2009).

[73] Medicaid and Medicare Programs; Electronic Health Record Incentive Program; Final Rule, 42 C.F.R. Parts 412, 413, 422 and 495, et al., 75 Fed. Reg. 44314, July 28, 2010. Additionally, ONC issued a final rule describing the certification criteria an EHR must meet in order for eligible providers and hospitals using the EHR to receive meaningful use payments. In creating the rule, ONC made an effort to align standards, implementation specifications, and certification criteria with the final meaningful use Stage 1 objectives and measures. *See* Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, 45 C.F.R. Part 170, 75 Fed. Reg. 44589, July 28, 2010.

[74] CMS Press Release. *CMS Proposes Definition of Meaningful Use of Certified Electronic Health Records (EHR) Technology*, December 30, 2009. Available at: http://www.cms.hhs.gov/apps/media/press/release.asp?Counter=3564.

will expand on the Stage 1 criteria and, according to some experts, criteria in all three stages should enable progress in standardization.[75] As discussed in more detail later in this paper, structured and standardized data such as that captured in coded format enable both segmentation of sensitive information and, ultimately, its exchange across disparate systems.

Finally, HITECH lists areas of consideration for standards development, including required technologies that can protect the privacy and security of health information, such as technical solutions allowing segmentation of sensitive data.[76]

Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2)

Federal regulations promulgated in the early 1970's to protect the identities of persons in alcohol or drug abuse treatment programs[77] also affect the legal environment in which the electronic exchange of health information will occur. These laws were intended to assure individuals that information related to substance abuse treatment would be kept private, recognizing that without such assurances, many patients would choose not to seek treatment for these serious health issues.[78] According to experts, research indicates that 95 percent of people meeting the criteria for substance abuse dependency do not perceive a need for help, and patient trust in the confidentiality of services is critical in order to enlist patients in treatment programs.[79] In keeping with this view, Part 2 strictly limits disclosure and use of information about individuals seeking or obtaining diagnosis, referral or treatment in federally assisted alcohol or drug abuse treatment programs.[80] Any and all information that might reasonably be used to identify an individual is protected by Part 2, and all permissible disclosures are limited to information necessary to carry out the purpose of the disclosure.[81] The regulations apply both to freestanding programs and programs that are part of larger organizations, for example a detoxification unit in a general hospital or a substance abuse clinic in a county mental health department.[82]

Nearly all disclosures allowed under Part 2 require specific patient consent.[83] This paradigm might require the segmentation of relevant data in order to ensure its protection and compliance with the law,[84] particularly in situations where a treatment program is part of a larger entity with multiple departments generating data for the same patient. Any information that could connect the patient to the substance abuse treatment program must not be released without proper

---

[75] Phone call with Dr. Ben Adida, Lead Architect and Investigator, Indivo PCHR Project, March 11, 2010.
[76] HITECH, Pub. L. No. 111-5, § 13101, 123 Stat. 228, 230 (2009) (to be codified at 42 U.S.C. 300jj-11).
[77] 42 C.F.R. pt. 2 (2009).
[78] H. REP. NO. 92-775, at 24 (1972), *reprinted in* 1972 U.S.C.C.A.N. 2045, 2072.
[79] Westley, H.C. "Federal Substance Use Disorder Confidentiality," *SAMHSA*, April 15, 2010, at 31, 40. Available at: http://www.samhsa.gov/presentations/Clark_42cfrpart2vFINALupdated.ppt.
[80] 42 C.F.R. § 2.3(a).
[81] 42 C.F.R. §§ 2.11, 2.13(a). For more detail on the basic structure of Part 2, *see* Goldstein, *supra* note 15. In addition, Part 2 defines disclosure as a communication or verification of patient identifying information, which can include names, addresses, Social Security numbers, fingerprints, photographs, or similar information by which the identity of a patient can be determined. The regulations' requirements apply to individuals or entities that hold themselves out and actually provide alcohol or drug abuse diagnosis, treatment, or referral for treatment, as well as to medical personnel or staff whose primary function is the provision of alcohol or drug abuse diagnosis, treatment, or referral for treatment.
[82] 42 C.F.R. § 2.11.
[83] 42 C.F.R. § 2.32.
[84] *Id.*

consent. In addition, Part 2 generally prohibits anyone who receives information from a substance abuse program from re-disclosing it, and requires that any information released must be accompanied by a written notice informing the recipient that federal law prohibits its re-disclosure unless expressly permitted by the patient or as otherwise authorized by the regulations.[85]

Like HIPAA, Part 2 sets a federal privacy floor. State laws that are less protective regarding disclosure and use of information about individuals in federally assisted alcohol or drug abuse treatment programs are preempted, while state laws that are more stringent are preserved.[86]

Protecting Select Conditions / Types of Data

Mental Health
State laws typically provide greater protection to in-patient mental health information than to health information generated in other settings, thereby producing data segmentation challenges for system developers in both policy setting (*i.e.*, accommodating varied systems of law) and technological implementation.[87] Under the most stringent laws, mental health records may only be disclosed without consent in the case of emergencies.[88] As in the case of Part 2, such laws therefore might require hospitals that have in-patient mental health wards to treat records generated in such wards differently than records generated in other hospital departments. Additionally, state laws might also contain provisions preventing re-disclosure of behavioral health records without consent, necessitating a means of addressing the flow of records to third parties once they have been released.[89]

Data Regarding Minors
Access by parents to the health records of minor children presents another area of legal complexity with respect to data segmentation in electronic exchange. Depending on state law, which can vary considerably, data systems may be required to segment the health information of minors in a way that will prevent unlawful disclosure to a parent.

HIPAA also includes several important exceptions regarding the disclosure of PHI to personal representatives, including the disclosure of information related to the health records of minors. Pursuant to the Privacy Rule, a parent is generally considered the personal representative of a minor.[90] As such, the parent generally has access to and control over that minor's health care record.[91] There are circumstances, however, under which the parent will not be considered the minor's personal representative under HIPAA, including, for example, where relevant state or other law allows the minor to consent to a health care procedure, and where the minor does in

[85] *Id.*
[86] 42 C.F.R. § 2.20 (2009).
[87] Pritts, J. et al. "Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information," August 2009. AHRQ Contract No. 290-02-0015, *RTI International*. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_910326_0_0_18/DisclosureReport.pdf.
[88] *Id.*
[89] *Id.*
[90] 45 C.F.R.§ 164.502(g)(3)(i).
[91] *Id.*

fact give consent.[92] While considerable variation exists, where a minor is allowed to consent to a procedure under state law, some states allow the minor to control access to medical records related to that procedure. New York law, for example, allows minors to consent to a variety of medical procedures and, where a minor has consented to a procedure, the law prevents the disclosure of information related to that procedure without the minor's consent.[93] Similarly, Washington, DC law allows a minor of any age to consent to a limited amount of outpatient treatment for mental health and protects the related records.[94]

Another important exception to HIPAA's general rule of parental access to the health records of minors applies in the case of abuse, neglect or endangerment. Pursuant to the Privacy Rule, covered entities are allowed on a case-by-case basis to prevent disclosure of an individual's health record to a personal representative in order to protect the individual involved.[95] There may therefore be instances where a covered entity must separate a minor's health care records in order to prevent disclosure of the records to a personal representative who could cause harm to the minor.[96]

Intimate Partner Violence and Sexual Violence

Intimate partner violence (IPV) and sexual violence (SV) have also been the subject of state and federal efforts to address the privacy of medical records. For example, the Violence Against Women Act of 2000 required the Department of Justice (DOJ) to develop national protocols for sexual assault medical forensic examinations.[97] The resulting protocols recognized that victims of sexual violence may avoid seeking assistance or treatment after an attack due to stigma, embarrassment, fear of assailants or other reasons.[98] As such, a recommendation was included that forensic exam records should be maintained separately from other medical records in order to preserve confidentiality.[99] Further, the protocols noted that restricting access to such records is particularly important in small and rural communities where hospital workers may know the patient or the suspect.[100] Sexual assault forensic exams, also known as rape kits, typically include a physical examination, toxicology labs, STI and pregnancy testing, and the prescription of medication. The protocols developed by the DOJ apply to every state and are meant to offer "guidance to jurisdictions in creating and implementing their own protocols, as well as

---

[92] 45 C.F.R.§ 164.502(g)(3)(i)(a).

[93] Feierman, J. et al. "Teenagers, Health Care and the Law: A Guide to the Law On Minors' Rights in New York State," *New York Civil Liberties Union Reproductive Rights Project*, July 2002. Available at: http://www.nyclu.org/files/thl.pdf.

[94] D.C. CODE § 7-1231.14(b) (2008); D.C. MUN. REGS. tit. 22, § 600.7 (2008); D.C. CODE §§ 7-1202.01 (2008).

[95] 45 C.F.R. 164.502(g)(5)

[96] Title X of the Public Health Service Act provides public funding for family planning services (42 USC § 300). While Title X mandates that all services are provided confidentially, including services provided to minors (42 C.F.R. § 59.11), the regulations require grantees to encourage the involvement of parents in a minor's decision to seek family planning services. (Omnibus Budget Reconciliation Act of 1981, Pub. L. No. 97-35, § 931(b)(1), 95 Stat. 570 (1981) (codified at 42 U.S.C. § 300(a) (1991))

[97] Violence Against Women Act, Div. B, Title IV of the Victims of Trafficking and Violence Protection Act of 2000, Pub. L. 106-386 §1405, 114 Stat. 1515 (2000).

[98] U.S. Department of Justice, Office on Violence Against Women. "A National Protocol for Sexual Assault Medical Forensic Examinations," at 90 *President's DNA Initiative*, September 2004. Available at: http://www.ncjrs.gov/pdffiles1/ovw/206554.pdf.

[99] *Id.*

[100] *Id.*

recommending specific procedures related to the exam process."[101] As a result, a number of states, including Alaska, Missouri and New Jersey,[102] have developed protocols and guidelines with language recommending that sexual assault forensic exam records be maintained separately.

While IPV hospital examination protocols generally recommend detailed documentation of incidents in the medical record, there is also recognition of the importance of ensuring the privacy of those health records. For example, the state of Iowa requires that hospitals interview IPV victims in private and maintain the confidentiality of the related health records.[103] In addition, testimony at a recent NCVHS meeting stressed the critical importance of protecting any information in a health record that may reveal the location of an IPV victim to ensure the victim's safety.[104] This protection requires attention not only to information being disclosed for treatment purposes, but also to information that may be disclosed for payment or operation purposes. Additionally, as health interventions are beginning to focus on the relationship between IPV and HIV, screenings for IPV are increasingly included as elements of HIV testing programs. Some state laws regarding HIV testing, such as the law in New York, specifically require that any IPV screening that occurs in the context of HIV testing must be kept confidential within medical records.[105]

Genetic Information

Because of the unique nature of genetic information and the increasing use of such information for a variety of purposes, protecting the privacy of this data is a growing concern.[106] Both federal and state laws have begun to address the issue in a variety of ways. GINA focuses on protecting individuals from discrimination by employers or health insurers on the basis of their genetic information.[107] Title I of GINA prevents group health plans and health insurers from basing premiums on genetic information, using genetic information as a basis for determining eligibility, or requiring that individuals undergo genetic testing.[108] Title II of GINA strictly limits an employer's right to request, require, or purchase an employee's genetic information.[109] Although the scope of GINA's protection is broad, the law does not apply to benefits such as long-term care, disability, and life insurance.[110] However, because GINA defines "genetic information" as information about an individual's genetic tests, as well as the genetic tests of an

---

[101] *Id.* at 14.

[102] *See, e.g.*, Alaska Department of Public Safety. *Alaska Statewide Protocols for Sexual Assault Response Teams*. Available at: www.dps.state.ak.us/Ast/docs/SARTProtocols.pdf; Missouri Department of Public Safety. *Sexual Assault Forensic Examination (SAFE) Program Report Form*. Available at: www.dps.mo.gov/dir/programs/safe/documents/SAFEForms.pdf; New Jersey Department of Law and Public Safety. *Attorney General Standards for Providing Services to Victims of Sexual Assault*. Available at: www.njdcj.org/agguide/standards/standardssartsane.pdf.

[103] IOWA ADMIN. CODE r. 481-51.7(3) (2008).

[104] NCVHS, *supra* note 53.

[105] N.Y. COMP. CODES R. & REGS. tit. 10, § 63 (2008).

[106] NCVHS, *supra* note 53.

[107] GINA, Pub. L. No. 110-233, 122 Stat. 881 (to be codified in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

[108] GINA §§ 101-106, 122 Stat. at 883-905.

[109] GINA §§ 201-213, 122 Stat. at 905-920. Experts have noted that, with the passage of health reform legislation addressing discrimination by health insurance companies on the basis of genetic information, Title I of GINA may have lost its significance so that only Title II remains relevant today. *See* comments of Mark Rothstein, NCVHS, *supra* note 53.

[110] GINA §§ 201-213.

individual's family members or the manifestation of a disease or disorder in an individual's family members,[111] it prevents the use of family medical histories in employment and insurance decisions in addition to genetic information about the individual.[112]

State laws regarding genetic information generally have focused on protecting patients from the use of such information by health insurers to deny coverage, although a minority of states have laws regarding genetic information that are broad enough to encompass the disclosure of information by health care providers.[113] These laws may apply solely to genetic testing, or may apply more broadly to genetics-related information, including information such as family health history or inherited characteristics.[114] State laws related to genetic information also vary in their consent requirements for information disclosure purposes: some require an individual's consent for disclosures for treatment purposes, while others do not. A small minority of states require consent for the release of information for treatment purposes even in the case an emergency.[115]

Despite the variation in state law, it is clear that the legal environment surrounding disclosure of genetic information recognizes the sensitive nature of such information and increasingly is making attempts to protect it. Accordingly, some experts have indicated that the increasing prevalence of genetic information in individuals' health records may increase an HIO's need to consider methods of protecting that information.[116] For example, testimony at the recent NCVHS hearing on sensitive information discussed the potential use of genetic information in the context of an individual with a behavioral health condition.[117] If an HIO chooses to include genetic information in electronic exchange, it may need to be capable not only of sequestering an individual's genetic information, but also the genetic information and medical history of an individual's family members. For example, Massachusetts law requires that the identity of an individual who has received a genetic test be protected from disclosure by encryption or encoding.[118]

HIV-Related Information

While most states have laws restricting the disclosure of information related to HIV, the scope of these laws can widely vary. In some states, the law may apply only to information maintained by a public health department, while in other states it may apply more broadly to any health care

---

[111] GINA § 201, 122 Stat. at 906. Analysts have observed that, by providing a statutory definition of genetic information (which thereby defines what is sensitive and thereby deserves protection), GINA could serve as a starting point for creation of appropriate segmentation policies for sensitive data. NCVHS, *supra* note 53.

[112] Office for Human Research Protections, U.S. Department of Health and Human Services. *Guidance on the Genetic Information Nondiscrimination Act: Implications for Investigators and Institutional Review Boards,* March 24, 2009. Available at http://www/hhs/gov/ohrp/humansubjects/guidance/gina.html.

[113] Pritts, *supra* note 87.

[114] *Id.* S*ee, e.g.*, Tex. Occ. Code 58.001(2007) and N.J. Stat. Ann. 10:5-47(a),(b) (2008)

[115] Pritts, *supra* note 87.

[116] Phone call with Dixie Baker, Chair of Privacy and Security Workgroup, Health IT Standards Committee and Member, Privacy and Security Workgroup, Health IT Policy Committee, May 3, 2010.

[117] NCVHS, *supra* note 53, at 13.

[118] MASS. GEN. LAWS ANN. ch. 111 § 70G (West 2009). Rather than create an encryption or encoding system, MAeHC excluded genetic information entirely from the exchange. Additionally, MAeHC decided not to include free text notes of any kind in the exchange, recognizing the difficulty of extracting family history information, for example, from free text fields. *See* phone call with Nael Hafez, Senior Pilot Executive, and Barbara Lund, Director of Technical Services, Massachusetts e-Health Collaborative, April 22, 1010.

provider.[119] In at least 16 states, laws and regulations also prohibit re-disclosure of HIV-related information, with some states requiring that written notice regarding the confidentiality of the information released accompany any such disclosure.[120] Also, at least 19 states have laws protecting HIV-related information that may be broad enough to cover the disclosure of information regarding medications that could be used to identify an individual as having HIV as well.[121] For example, Connecticut law protects "any confidential HIV-related information,"[122] defined as including any information "pertaining to" a person with HIV or relating to that person's sexual partners—including information that reasonably could identify an individual as having HIV.[123] Such laws recognize the capacity of information beyond test results to indicate that an individual may have HIV and the resulting need to restrict access to such information in order to protect the confidentiality of an individual's HIV status. Many of the experts interviewed for this paper specifically mentioned the possible downstream inferences that could be made from the inclusion of such data in an EHR when discussing challenges for developers of data segmentation systems.

OPPORTUNITIES AND CHALLENGES IN ADVANCING DATA SEGMENTATION

As discussed above, there are multiple permutations of data segmentation in the health care context, and just as many perspectives on whether, or to what extent, it should be enabled or discouraged. This variation is in part due to the fact that multiple interrelated considerations, both technical and non-technical, surface when deliberating this issue. At one end of the spectrum, enabling the complete and meaningful accommodation of individual preferences may require significant technical advances that, while potentially feasible, are not well supported or enabled by the broader health care system. Conversely, disregard for such preferences (as stated either directly by individuals or on their behalf) may impact stakeholder participation and certainly could violate legal requirements and other policy directives.

One of the major benefits of converting from paper to electronic means of capturing information is that it makes the task of sharing that information between providers, patients, and other interested and appropriate parties, at least theoretically, much easier—it is relatively simple to make copies of electronic data from EHRs and other data sources, and the transmission of that information can be instantaneous[124] and performed at low or no cost. Further, information recorded in structured fields within an EHR is easier to categorize and sort accordingly, which helps enable segmentation where desired. By contrast, segmenting information within paper records (which may be performed to fulfill the minimum necessary requirement of HIPAA, for example) typically requires redaction of information by hand because whatever is written on a single sheet of paper necessarily is associated with all other information on that paper. If one merges all of the single pieces of paper on an individual with co-morbid conditions, even from only one provider's office, the volume quickly becomes unwieldy and non-portable, which means that it cannot be used as effectively to support care delivery and coordination processes.

---

[119] Pritts, *supra* note 87.
[120] *Id. See, e.g.,* FLA. STAT. § 381.004 (2008)
[121] Pritts, *supra* note 87*; see, e.g.,* 35 PA. CONS. STAT. ANN. § 7603 (West 2010).
[122] CONN. GEN. STAT. § 19a-591 (2009).
[123] CONN. GEN. STAT. § 19a -581 (7), (8) (2009).
[124] Consumer Partnership for eHealth, *supra* note 5.

In addition, not only is the adoption of, or conversion to, systems that support data segmentation in the best interest of individual patients who want to express their information management preferences, but it is also critical to supporting the goal of improving our health care system. Several initiatives, including those discussed at a recent Institute of Medicine (IOM) workshop,[125] for example, have focused on the importance of leveraging HIT systems to generate more and better information that can be used to support rapid learning within health care. With the goal of fostering an environment that yields continuous quality improvement, workshop organizers pointed out the importance of capturing electronically nearly all clinical (and other relevant) health data in such a way that it can be leveraged, not only for the provision of quality care, but also for a variety of other "secondary" purposes, such as public health surveillance, disease modeling, and comparative effectiveness research. This priority is also evidenced in many provisions of the HITECH Act, as well as the broader health care reform legislation of 2010.[126]

Although systems supporting electronic data capture are better able to support these objectives, data segmentation is still viewed by some analysts as problematic, infeasible, and possible only at some point in the future. Perhaps this skepticism is based on the reality that, at this point in the transition from paper to electronic collection and exchange of health information, we are forced to accommodate the challenges posed by both. That is, we still work in a mostly-paper world and have developed complex processes to support that environment, but we simultaneously are trying to evolve to a different medium that requires critical examination and often replacement of those entrenched processes. Interestingly, many experts believe that the technical issues involved in the development of electronic data capture and exchange, while significant, pose far less of a challenge than others discussed in this paper, including policy considerations, the absence of standard data definitions and terminologies, entrenched institutional and provider practices, and consumer capacity issues. That is not to say that the technology isn't critically important, but rather that highly granular segmentation is indeed technically feasible—assuming that the other issues are addressed as well.

Outlined below are five key challenge areas associated with the segmentation of health information in the context of electronic exchange. They are presented in no particular order of importance or significance, and each merits thoughtful consideration and evaluation—both at the broad policy level and as applied to a particular exchange initiative. It should also be noted that

---

[125] Institute of Medicine. "Electronic Infrastructure for the Learning Healthcare System: The Road to Continuous Improvement in Health and Health Care. Workshop #1: Opportunities, Challenges, Priorities." *Sponsored by*: Office of the National Coordinator for Health Information Technology, July 27-28, 2010. Available at: http://www.nationalehealth.org/ShowContent.aspx?id=436.

[126] *See, e.g.*, HITECH, Pub. L. No. 111-5, § 13101, 123 Stat. 115, 230 (2009) (to be codified at 42 USC 300jj-11) (requiring development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information in a way that improves health care quality, reduces medical errors and advances the delivery of patient-centered medical care, as well as improves public health activities and facilitates identification of and response to public health threats); Patient Protection and Affordable Care Act (PPACA), Pub. L. No. 111-148, § 3002(d), 124 Stat. 119, 363 (2010) (amending § 1848(m) of the Social Security Act (42 U.S.C. 1395w-4(m)) (requiring Secretary of HHS to integrate quality measures with meaningful use reporting requirements for physicians participating in the Physician Quality Reporting Initiative); § 3015, 124 Stat. 119, 387 (2010) (amending Title III of the Public Services Act (42 U.S.C. 241)) (requiring Secretary of HHS to align data collection and aggregation efforts with standards for the interoperability of HIT systems).

the descriptions below are intended to surface these complexities, but do not necessarily offer guidance or point to a set of solutions.

Technical Considerations

The ability to segment information within an EHR and, more broadly, in the context of electronic exchange, largely depends (from a technical feasibility standpoint) on a number of factors, including the ability to capture information in structured data fields, the application of common data definitions and terminologies so that such information can be interpreted correctly by others, and the use of common standards for sharing the information.

Legacy Systems

One major issue that hampers segmentation efforts is the persistence of "legacy" data systems that generally fail to meet the requirements enumerated above.[127] Early EHR systems generally were designed to bring large amounts of data into a system without a focus on getting data out of the system.[128] Further, many systems were developed simply to translate information that was recorded in paper format into electronic format. The systems were not designed with segmentation in mind, and typically contain unstructured data that are not computable. Also, most legacy systems are highly customized to meet the specific needs of an organization and require individualized mapping schemes in order to translate data from their particular system to a standardized structure and code.[129] In addition, these systems typically represent significant investment on the part of provider organizations and would be very expensive (both in terms of direct and indirect costs) to replace or retrofit.[130] Unfortunately, legacy systems also tend to be based on older software and hardware technologies that cannot match more efficient methods of performing certain tasks, may include procedures or terminologies that are no longer relevant in the current environment, and can hinder or compromise the capacity to achieve certain desired outcomes.[131]

Most newer EHRs on the market today have the capacity to capture data in a structured fashion so that it resides in fixed, computable fields and corresponds to a coding mechanism that identifies the data element, its characteristics, and location within the system. This means, for example, that during a clinical encounter a provider might record a diagnosis by selecting from a list in a drop-down menu that is specifically designated to record diagnoses. The provider's choice in turn corresponds to a standard coding schema that can be identified and appropriately interpreted (in some cases) by another system. In many legacy systems, however, one of two situations typically exists: (1) the provider is relegated to typing the name of the diagnosis into a free-text field that is designed to capture any miscellaneous information recorded during a clinical encounter (resulting in non-structured data); or (2) a menu of options exists but is "home

[127] Phone call with Gregory Caulton, Principal, PatientOS, February 2, 2010.
[128] Phone call with Dr. Ben Adida, *supra* note 75.
[129] Phone call with Ioana Singureanu, Eversolve, L.L.C., March 10, 2010.
[130] *Id.*
[131] Zandieh, S.O. et al. "Challenges to EHR Implementation in Electronic Versus Paper-Based Office Practices," *Journal of General Internal Medicine*, Vol. 23, No. 6, March 28, 2008, 755-61; Congdon, K. "How Much Will and EHR System Cost You?" *Healthcare Technology Online*, September 14, 2009. Available at: http://www.healthcaretechnologyonline.com/article.mvc/How-Much-Will-An-EHR-System-Cost-You-0001.

grown" and does not relate to a broader coding terminology that would be recognized or interpretable by other systems.[132]

Few vendors have attempted to structure the fields within EHRs in a way that is compatible with other systems, in part because, historically, compatibility was not what their customers needed. Products created by the same vendor, but for different customers, may be highly customized and even use different standards, making the exchange of segmented records difficult.[133] In fact, it is not uncommon for large vendor companies with multiple deployed products to sell their products as developer's kits, which are then customized by individual institutions in a way that is not necessarily interoperable.[134] Finally, many experts have emphasized the problems created by vendor lock-in, which has restricted organizations in their ability to exchange information with those external to their system. However, as organizations move to more modular solutions, such as those advocated by some open source developers, vendor lock-in and the related challenges could be alleviated.[135]

Data Entry

Provision of optimal EHR technologies alone, however, will not result in the availability of structured data. Even if the provider is not directly involved in deciding what information should be segmented, the act of recording data in a way that supports segmentation typically requires some alteration of the "usual" clinical workflow. Providers are accustomed to recording information about patient encounters, whether in paper or electronic form, in whatever manner best reflects their style of practice. Also, many clinicians skip or choose the default option on data fields and overly rely on the entry of free text, perhaps due to the perceived lack of flexibility and functionality of current EHR products.[136] This is problematic for segmentation in at least two respects: 1) it represents an opportunity cost for recording higher quality data in structured fields that can later be pulled and analyzed for operations, quality improvement, and other research purposes; and 2) it makes the task of identifying and sequestering potentially sensitive information much more challenging.

On one hand, if information in free text were to reference a condition or medication deemed by the patient as being too sensitive to share, for example, then – in order to protect the information – the entirety of that field would need to be withheld from exchange.[137] Moreover, for any given patient over time, the same type of information could be recorded in multiple fields and labeled as both sensitive and non-sensitive data within the record. On the other hand, providers who choose to use free text but desire to keep sensitive information *out* of the electronic record might obscure references to such information and / or even refer to sensitive health issues in cryptic notations known only to that clinician. For example, in a study of behavioral health

---

[132] Phone call with Ioana Singureanu, *supra* note 129; Maher, T. and L. Bloemer. "EHR Conversion Lessons," *Hayes Review*, December 2009. Available at: http://www.hayesmanagement.com/media/newsletters/2009_December_article4.php.

[133] Phone call with Ioana Singureanu, *supra* note 129.

[134] Phone call with Dr. David Winn, Founder and Chairman, e-MDs, April 26, 2010.

[135] Phone call with Clint Crowe, CEO, HealthForge, April 20, 2010.

[136] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 112.

[137] Phone call with Gregory Caulton, *supra* note 127.

providers using EHRs, the clinicians referred to sensitive information included in free text in generic terms, such as referring to aspects of incest trauma as "inappropriate contact."[138]

Locating Data in the System

When deconstructing a record for the purpose of segmentation, information that may need to be redacted is often intermingled, and therefore difficult to extract.[139] Of particular concern is the fact that data points related to a particular health issue may be scattered in many parts of the record, including both free text and structured fields.[140] Data in an EHR that indicates HIV status, for example, could be found in numerous fields, including white blood cell count results in a lab field; an antiretroviral prescription in the medication field; the presence of other related diagnoses (*e.g.*, Kaposi's sarcoma) in a problem list; and / or the reference to an HIV support group referral within the free text. As a result, the task of identifying every area of the EHR where sensitive information may appear has been perceived as daunting—free text portions of an EHR in particular, given that natural language processing technologies are widely viewed as being insufficiently developed to identify all references to information that might be considered sensitive.[141] For this reason, many vendors, providers and other data stewards have expressed reservations about their ability to comply with such segmentation requests. Conversely, if a strategy of casting a wider net is employed in order to ensure that every mention of the sensitive issue is captured, the result is likely to be a record with significant and potentially undesired gaps in information.[142]

For this reason, some organizations have chosen to segment certain categories within specific data types (*e.g.*, all mental health-related medications). Similarly, as discussed earlier, organizations such as CORHIO have considered it simpler to exclude records altogether that are sourced from mental health clinics rather than try to filter out references to mental health issues within individuals' data. In CORHIO's case, developers considered it particularly impractical to attempt to identify all data points related to mental health in a primary care record.[143]

Terminology & Codes

Because structured data content can be categorized and organized, it is a critical cornerstone for data segmentation. However, recording of information in a structured fashion is not sufficient—consistent interpretation of that information is also needed, particularly consistent interpretation of the discrete pieces of information that are being accessed or exchanged. Such consistency requires the use of standard terminology and codes so that systems receiving the information can interpret it accurately and identify it appropriately as potentially requiring an action related to segmentation (*e.g.*, the designation of "sensitive"). In essence, exchange of information in a way that respects the consent preferences of the individual patient requires that all parties have the capacity to interpret the information included in a data field, and then apply some set of rules –

[138] Salomon, R.M. et al. "Openness of Patients' Reporting with Use of Electronic Records: Psychiatric Clinicians' Views." *Journal of the American Medical Informatics Association*, Vol. 17, 2010, pp. 54-60.
[139] Phone call with Carl Dvorak, Executive Vice President, Epic Systems, May 12, 2010.
[140] Phone call with Dr. Jamie Ferguson, Executive Director of Health Information Technology Strategy and Policy, May 24, 2010.
[141] Phone call with Gregory Caulton, *supra* note 127.
[142] Phone call with Dr. John Mattison, Chief Medical Information Officer, Kaiser Permanente, May 24, 2010.
[143] Phone call with Carrie Book, *supra* note 20.

consistently – to that information. That is, from a technology perspective, agreement on both structure and language is critical.

Currently, there is no single standard code set used in EHRs, which complicates segmentation for developers, who must use toolsets and solutions that enable work in different standards. Some have described the current situation as similar to using multiple-gauge railroad tracks within a single rail system and have expressed a desire for policy makers to choose one particular gauge.[144] Other solutions that have been discussed include: 1) providing incentives to and / or requiring providers to begin recording and reporting select information according to a more constrained set of standards, and 2) encouraging the broader use of mapping technologies that could translate code sets so that information can be shared and correctly interpreted across systems.[145]

An example of the latter method has been evidenced in the Kaiser Permanente environment. In June 2009, Kaiser took part in a community-based electronic exchange project to translate data for exchange purposes between different systems.[146] The demonstration involved two organizations that use different data standards (both of which are sufficiently structured) exchanging information with NHIN software.[147] In addition, as described later in this paper, Kaiser established a partnership in January 2010 with the Veterans Health Administration (VHA) to share medical records as part of a pilot in San Diego, CA. The project allows patients who visit both Department of Veterans Affairs (VA) Hospitals and Kaiser clinics to benefit from electronic exchange.[148] Kaiser has a different software system from the VA, but can share records with the agency using the same technology as used in the NHIN exchange project.

Building Intelligence

Databases are dumb[149]—the data contained therein must be "told" what to do in support of the user's specific objectives. In order to instruct systems on how to apply the segmentation preference / requirements of an individual, an organization, or a state, an accompanying set of directions – often referred to as "rules engines" – must be developed. Rules engines are software systems that execute a set of orders and can be used to customize data output responses to particular situations.[150] For example, an adult with a blood disorder may request that her providers withhold information related to the condition, except in the event of an emergency hospitalization. If she were to be admitted to an emergency department, a rules engine could automatically release the usually-sequestered information so that it would be available to the treating clinicians.

---

[144] Phone call with Dr. David Winn, *supra* note 134.
[145] Phone call with Ioana Singureanu, *supra* note 129.
[146] California e-Health Collaborative. *Successful Demonstration of Health Information Exchange Opens ARRA Stimulus Options for California*, June 26, 2009. Available at: http://www.californiaehealth.org/news/caehc_pressrelease_20090626.pdf.
[147] *Id.*
[148] Darce, K. "Medical breakthrough: VA, Kaiser to Share Records," *San Diego Union-Tribune*, January 6, 2010. Available at: http://www.signonsandiego.com/news/2010/jan/06/a-medical-breakthrough-va-kaiser-to-share-records/.
[149] Phone call with Ioana Singureanu, *supra* note 129.
[150] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.

Rules engines can be developed and applied to EHR data within a closed system, which allows for the establishment of rules and data protocols that conform to specific institutional policies (*e.g.*, non-release of certain clinical information to specific staff). They can also be built to support the collaboration of multiple organizations – say in the establishment of an HIO – so that a common set of rules for information management can be applied consistently across participants. Many examples of both models exist, and are described further in the next section.

Conveying Information Sharing Across Multiple Systems

As referenced above, far less common in practice is the capacity to provide an additional layer of intelligence that is sometimes referred to as a "database of consents." This type of application stores individual preferences for information management (*e.g.*, withhold all references to congenital heart condition from all providers except for the cardiologist, OR require permission for all disclosures not directly related to the provision of care), and can then be referenced before any information sharing action is taken. An important distinction between a rules engine that supports the information management of a provider organization and a consent database is that the former is intended to reflect institutional policies with regard to information sharing, whereas the latter is intended to reflect an individual's preferences for the sharing of his / her information.

These consent systems can be deployed within a specific organizational structure, but likely will provide the highest level of utility to consumers when they can serve as the ultimate authority that sets the rules to which all organizations must adhere. As discussed in more detail in the Consumer Engagement section below, this is not yet a viable option.

In the interim, another option that may prove to be more technically feasible in the near term (and also more aligned with current information sharing practices) is that of creating flagging / tagging standards that can convey the presence or absence of potentially sensitive information within a summary record (as discussed in more detail below). Specifically, the Continuity of Care Record (CCR) and the Continuity of Care Document (CCD)[151] are designed as ways of passing information between entities, and their use is being encouraged as a means of exchanging at least a core set of clinical information between providers to support care coordination. At present, however, standards do not exist to support the transmission of these summary documents in a way that retains flags alerting the recipient to the presence of potentially sensitive information that is to be afforded special treatment. The information can be sent, but the notation is lost.

Defining Sensitivity

As referenced earlier in this paper, many policy discussions regarding data segmentation (in particular those convened by NCVHS) have focused on the issue of whether and, if so, how to define what types of data (if any) should be afforded special treatment. That is, should consumer preferences regarding information sharing be supported through the determination and strict application of definitions for what constitutes "sensitive" information, or should policies that

[151] The CCR and CCD are two clinical records standards used to aggregate and export clinical data. They are both designed to collect a core set of data in a standard format and enable it to be exchanged. Any organization exporting these documents must follow strict rules and standards in order for the documents to be interpreted correctly by the recipient. *See* Kahn, S. and V. Sheshadri. "Medical Record Privacy and Security in a Digital Environment," *IT Professional*, March/April 2008, pp. 46-52, at 48-49.

allow for greater subjectivity and individual autonomy be considered? Implicit in this discussion are the related questions of whether sensitive health information should be treated differently from other kinds of health information and, if so, who should decide what information falls into that category? Finally, should those decisions be based on societal norms or individual preferences?

In general, institutional stewards of patient information tend to rely primarily on federal and state definitions (often based on legal requirements) that categorize certain information as being sensitive. In order to comply with such definitions, and sometimes to enable some control on the part of the patient, most organizations that permit segmentation have done so by pre-defining a set of rules for applying restrictions on data sharing. Among other approaches, they have:

- Identified particular key words (or fields in an EHR) that should be treated as sensitive;
- Identified clinical categories that should be treated as sensitive;
- Differentiated information based on its type (*e.g.* medications, labs); and / or
- Differentiated information based on its source (*e.g.* all information from federally-assisted substance abuse facilities)

These approaches, while challenging in some ways, have allowed organizations to establish and operationalize standard policies without applying undue burden on providers, IT professionals, and others who might be challenged by the need to accommodate more individualized requests.

Many consumers, however, believe that one-size-fits-all determinations of this nature, absent input from individuals, are misguided. Some, believing that such determinations are purely subjective, have asserted that it would be impossible to specify *a priori* the set of information or data types that different individuals may want to sequester. According to a recent Agency for Healthcare Research and Quality (AHRQ) publication on consumer engagement, based on focus group research, "there was near universal agreement in all the groups that, if medical data are to be stored electronically, health care consumers should have some say in how those data are shared and used."[152] The report further indicates a lack of support for the establishment of general rules that would apply to all health care consumers; it was thought that people should be able to exert some control individually. Applied to the issue of defining sensitivity, these results indicate support for a more subjective approach whereby patients are afforded the opportunity to define in their own terms what information they consider to be too sensitive to expose, and what information they would share with others. As described in more detail later in this paper, the Massachusetts eHealth Collaborative (MAeHC), for example, spent a considerable amount of time engaging the community in defining what information would be considered sensitive and determining patient preferences. They also worked with provider organizations and incorporated provider perspectives when creating their processes and procedures.[153]

[152] Schneider, S. et al. "Consumer Engagement in Developing Electronic Health Information Systems." Prepared for: *Agency for Healthcare Research and Quality*. AHRQ Publication No. 09-0018-EF, July 2009, at 29. Available at: http://www.healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09%E2%80%900081%E2%80%90EF.pdf%00%00.

[153] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.

In acknowledgment of this perspective, experts often stress the need to engage the patient in the process of data segmentation.[154] Indeed, policies and practices that encourage patient participation in establishing information management and use preferences, either on their own or with assistance from a provider or other professional acting on their behalf, may result in greater patient satisfaction. Given that individuals may make different information management decisions at different points in their lives or under different health conditions, the importance of revisiting these preferences periodically has also been stressed.[155]

So what are the hurdles to accommodating the desire for a more individualized approach? Part of the answer lies in the response to a related question. That is, how should the needs of individual patients be considered relative to those of various other stakeholders who may desire access to the information in question and / or prefer not to confront the practical and logistical implications of distinguishing it from other non-sensitive information.

Even if a particular segmentation approach is technically feasible and desirable from a policy point of view, it may be impractical or difficult to achieve logistically. The ability to segment sensitive data appropriately and effectively, in addition to complying with established criteria in the electronic exchange process, requires the consideration of a variety of interests, the careful management of large amounts of "scattered"[156] data, and the coordination of rules across disparate policy and technology environments.

Stakeholders often mention these and other considerations when articulating a preference for the establishment of some baseline policies and information management protocols to support the segmentation of specific sensitive information. Many technology vendors, for example, have expressed a preference for the specification and definition of what constitutes sensitive information so that they can develop one solution that meets the needs of multiple clients.[157] For example, vendors have noted that, when diverse state laws result in the need to apply different rules regarding sensitive information in different locations, it is challenging to create and support such applications.[158] In addition, some exchange organizations have also suggested that consistent laws and policies regarding sensitive information would facilitate the appropriate sharing of information.[159]

In any event, if policy makers do find it necessary and desirable to establish a standard definition of what constitutes sensitive information, the questions remain of who and at what level such determinations should be made. Various possibilities include individual providers, HIOs, and states, although some advocate that, given the magnitude of the practical and technical challenges involved, the task should be undertaken by the federal government. Regardless of the particular author of such a definition, numerous stakeholders will struggle with its application as well its enforcement.

---

[154] Phone call with Robert Shelton, Co-Founder, Chairman and CEO, Private Access, Inc., May 12, 2010.
[155] Phone call with Dr. Mark Snyder and Lori Potter, Kaiser Permanente, May 3, 2010.
[156] In this context, "scattered" data refers to the likelihood that clinical encounter and other patient health information recorded in an EHR is likely to be recorded in a variety of ways and in a number of places throughout the record.
[157] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.
[158] *Id.*
[159] Phone call with Perry Yastrov, Director, Arizona Medical Information Exchange, April 28, 2010.

Consumer Engagement

Exercising individual preferences for information sharing (*i.e.*, making segmentation decisions) presumes a level of understanding about what is possible, what is desirable, and what the potential consequences of those decisions may be. Packed into this process are some very real concerns about the capacity of individuals to appreciate these nuances and act accordingly, as well as more logistical concerns about how individuals could reasonably be expected to articulate their preferences in a manner that could be honored by multiple, diverse data holders in the health care environment. The section below approaches the consumer engagement discussion in three basic parts: 1) What are the issues related to capacity (can they do it)? 2) What are the concerns related to motivation (do they want to do it)? and 3) What are the concerns related to logistics (how can they reasonably do it)?

Capacity

It is widely recognized that the U.S. health care system does a fairly poor job of engaging patients and their families in decisions about and processes of care. As noted in a recent Robert Wood Johnson Foundation brief, patients say they are bewildered by the system's complexity, intimidated by its medical and legal jargon, and usually unable to obtain meaningful information about quality or cost.[160] One key capacity challenge is that of engaging people in a potentially overwhelming process that often requires making choices absent full information, clinical context, appreciation of consequences, or adequate provider support. Many health policy experts expect or at least hope that, when equipped with more and better information to support decision making, consumers will become more active participants in and self-managers of their own health and health care. A central question then becomes whether it is possible to provide consumers with sufficient and appropriate information such that they can make decisions not only about their health and health care, but also about the ways in which they want their health information to be segmented for use according to their values, beliefs and preferences in support of those decisions? To address this question, we briefly explore below the concepts of decision significance and frequency, both of which may have implications for a person's capacity and desire to express granular preferences for information sharing.

As individuals in a free society, we are accustomed to making thousands of decisions each day—many of little significance or consequence, and others of much greater import. For the former type, it is unlikely that a lack of complete information or contextual understanding will have serious implications or be of much consequence to the individual. For more complex decisions, however, such as whether a patient should share or withhold from other parties his / her full mental health history, the concept of "bounded rationality" (the notion that, in decision making, rationality of individuals is limited by the information they have, the cognitive limitations of their minds, and the finite amount of time they have) becomes more relevant.[161] Certainly, lay persons typically are at an information disadvantage relative to medical professionals responsible for their care, and are much less well acquainted with the way data flows through the health care system.[162] In addition, the health information in question is not always provided or discussed in

[160] Robert Wood Johnson Foundation. *Spotlight on Consumer Choice*, December 4, 2009. Available at: http://www.rwjf.org/healthpolicy/product.jsp?id=51409.
[161] Jones, B.D. "Bounded Rationality," *Annual Review of Political Science*, Vol. 2, 1999 pp. 297-321.
[162] "Protected Health Information," Department of Health and Human Services, 2003. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/udmn.pdf.

a meaningful context or well understood by the patient, which raises additional concerns about health literacy. Further, we know that most patients have little sense of how their information is shared (or not), and what provisions exist to protect it (or not) outside the boundaries of their doctor's computer or file cabinet.[163]

Related to the complexity issue is the issue of volume, or decision overload. Studies have shown that, while people may prefer to choose from as many alternatives as possible, decision-making ability is compromised when too many choices are offered.[164] A related body of research suggests that the process of making too many "minor" decisions can hamper people's ability to focus on decisions of greater significance.[165] Researchers have hypothesized that when people are faced with "too much choice," they feel burdened by the responsibility of choosing between good and bad decisions and are less able psychologically to distinguish between the choices.[166] It has also been hypothesized that the "too much choice" effect would be more pronounced in choices such as medical treatment decisions, since these decisions involve greater costs associated with making a "wrong" choice and take substantial time and effort to make an informed comparison.[167]

If patients are able to navigate successfully a series of complex information management decisions, the "portability" of those decisions remains a challenge in the context of electronic exchange. As discussed in more detail below, patients have no way of expressing their information management preferences all at once (*e.g.*, through a single entity or portal) in such a manner that ensures accommodation (*i.e.*, adherence) by all data holders and seekers. As such, patients can be asked to articulate their preferences numerous times, in a variety of different ways. Assuming this is the case, implementing fine-grained controls for data segmentation on numerous occasions may result in patients forgetting which of the many options have been selected.[168] For example, patients may forget which information they shared with each provider and, subsequently, which information they want blocked from all providers. This constant flux is likely to hamper the patient's ability to make strategic decisions regarding his / her health care.

These findings related to consumer decision-making capacity have implications for policy makers and others desiring to identify optimal approaches for engaging patients in decisions about how, under what circumstances, and with whom their health information can be shared. Considering the numerous challenges and complexities referenced above, some would propose to

---

[163] Schneider, S, *supra* note 152, at 11, 18, 23; Peel, D.C. "The Case for Informed Consent: Why it is Critical to Honor What Patients Expect – For Health Care, Health IT and Privacy," *Patient Privacy Rights*, August 2010, at 10. Available at: http://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf.

[164] Iyengar, S.S. and M.R. Lepper. "When Choice is Demotivating: Can One Desire Too Much of a Good Thing?" *Journal of Personality and Social Psychology*, Vol. 79, No. 6, December 2000, pp. 995-1006; Jessup, R. K. et. al., "Leaving the Store Empty-Handed: Testing Explanations for the Too-Much-Choice Effect Using Decision Field Theory," *Psychology and Marketing*, Vol. 26, No. 3, February 2009, pp. 299-320; Iyengar, S.S. et al. "How Much Choice is Too Much?: Contributions to 401(k) Retirement Plans," in *Pension Design and Structure: New Lessons From Behavioral Finance*: (Olivia S. Mitchell & Stephen P. Utkus eds., 2004).

[165] Vohs, K.D. et al. "Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative," *Journal of Personality and Social Psychology*, Vol. 94, No. 5, May 1, 2008, pp. 883-98.

[166] Iyengar (2000), *supra* note 164, at 1004.

[167] *Id.*

[168] Phone call with Dr. Ben Adida, *supra* note 75.

eliminate or minimize patient engagement in segmentation decisions, thereby deeming individual consumers incapable of making such complex decisions and preferring instead to leave such matters to policy makers at the organizational, state, and / or national level. Others might constrain consumer segmentation preferences, and therefore choices, and / or establish a set of discrete and uniform options (and then focus consumer education efforts on those few key points). For example, patients might be afforded the right to segment based on the purpose of information exchange (*e.g.*, marketing), but have no ability to constrain access to their information for disclosures permitted by the HIPAA Privacy Rule.

Others might take an entirely different approach that involves the use of innovative technologies and communications tactics to support consumers in the processing of such complex decisions. For example, Private Access, an early-stage company developing privacy enhancing technologies for the transfer of medical information, is developing a unique graphical interface to assist users in the decision making process. The company has engineered trusted guides that enable users to identify their privacy preferences concerning the visibility and transfer of medical data. By answering questions in the guides, users are able to gauge the levels of security that are typically needed to accommodate their preferences and subsequently adopt these settings in the Private Access platform.[169]

An alternative model is presented in Indivo X, a PCHR system that enables individuals to "own" and manage health and wellness information. The Indivo X platform facilitates substitutability within the medical record landscape (that is, it serves as the central hub for information and can be updated to reflect the most recent, and therefore most accurate, data) and allows users to communicate with third parties.[170] Its centrally-located consumer preference hub allows for both a seamless transfer of medical data (limited at this point to exchange within a single provider organization) and also limits the need for patients to reiterate privacy decisions at each point of entry into the health care system. In essence, neither Private Access nor Indivo X limits choice *a priori*, but instead provides some level of assistance or guidance that is meant simultaneously to educate patients about issues relevant to segmentation and guide them through the process of executing those choices. Both systems are discussed in more detail later in this paper.

Motivation

Surveys have indicated that the public wants a wide range of choices with respect to how their information is shared, with whom, and for what purposes.[171] In a perfect choice environment, patients would have the time, interest, and incentives to learn about and consider a variety of factors relevant to their decisions. As medical information is shared in a less-than-perfect environment, however, there are varying levels of patient involvement and interest in information management. Studies have indicated that, while the majority of consumers would like to participate actively in the medical decision making process, others are less concerned.[172]

---

[169] Shelton, R.H. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913483_0_0_18/Private_Access_Testimony.pdf.

[170] Ahier, B. "Sharp Focus: Indivo Personall Controlled Health Record," *Healthcare, Technology and Government 2.0 Blog*, April 18, 2010. Available at: http://ahier.blogspot.com/2010/04/sharp-focus-indivo-personally.html.

[171] Schneider, *supra* note 152, at 29, 36.

[172] Thompson, R.R. "Variability in Patient Preferences for Participating in Medical Decision Making: Implication for the Use of Decision Support Tools," *Quality in Health Care*, Vol. 10, Supp. I, 2001, pp. i34-i38, at i34.

There are a multitude of factors that determine a patient's desire for involvement in decision making, including the desire for receiving information (the process of information evaluation) and the desire to take responsibility for the treatment decision itself.[173] It seems likely that the same varying degrees of participation exist in the realm of health information sharing, as studies show that some patients would like to leverage EHRs to help them customize their care experience and information sharing, while others are less concerned with the privacy of health information and willing to forgo providing input into how their information flows.[174]

Logistics

In addition to consumer capacity and motivation issues, one of the more obvious deterrents to direct patient articulation of their information sharing preferences is that no single vehicle exists for capturing and then propagating such preferences across multiple provider settings or other exchange entities. For example, a patient in a multi-hospital system may be able to (within the parameters established by the organization) create a directive, but the patient's preferences cannot be recorded automatically so as to be accommodated by a provider outside the system (or potentially even by individual hospitals within the same system).

While a harmonizing entity or universal consent directive that can interpret and operationalize patient preferences and resolve discrepancies across entities may one day be developed, a current impediment to data segmentation is patients' potential unwillingness to go through the same (or a similar) process multiple times. Ultimately, to the extent that the segmentation policies and protocols of various provider entities converge, this issue may be simplified. In the current environment, however, and assuming a high level of granularity, the process of establishing multiple consent directives likely would be too onerous for most patients even if it were well supported by the provider community.

In absence of the aforementioned "harmonizing entity," several technologies exist to allow patients to articulate information sharing preferences within a single network. For example, Microsoft HealthVault is a PHR that allows users to filter out parts of their record when sharing information directly with individual providers or other users within the community. However, when a user wants to allow a third-party "network," such as a hospital, to view and contribute to his / her PHR, the user must grant the network access to pre-determined parts of the record.[175] Alternatively, Google Health provides personal health information centralization services that allow users to load their health records into the Google system, ultimately creating one profile of health information from multiple providers. Similar to HealthVault, however, Google Health does not have the ability to communicate or enforce the execution of patient preferences with outside entities.[176]

---

[173] *Id.* at i36-i37.
[174] Robert Wood Johnson Foundation. *Patients Reveal a Willingness to Trade Hands-On Medical Care for Computer Consultations*, May 18, 2009. Available at: http://www.rwjf.org/pr/product.jsp?id=42849.
[175] Phone call with Kathleen Connor, Principal Program Manager, Microsoft HealthVault, March 11, 2010.
[176] Google Health. *About Google Health*. Available at: http://www.google.com/intl/en-US/health/about/index.html.

Provider Reluctance

Quality and Safety Concerns

Other challenges associated with the segmentation of health information in the context of electronic exchange fall within the category of provider reluctance. Chief among these is the concern that the non-inclusion or withholding of certain health information (whether it be deemed by the individual patient as significant or not) can compromise patient safety and inhibit the provision of high quality care. Many providers involved in the establishment of and / or participating in exchanges have expressed the concern that classifying any amount of information as sensitive, and thus allowing patients to sequester certain portions of their records, may create safety and quality of care issues. The basic issue is how patient preferences for (non) disclosure should be balanced with provider preferences for access to the *complete* clinical record.

Many experts believe that patients are ill-equipped to determine which pieces of information might be clinically relevant to a particular provider or in a specific clinical context, and therefore should not have the ability to (potentially) compromise their own safety by restricting access to their information. This sentiment is a particularly common refrain in discussions of medication safety and is ultimately the reason why so many electronic exchange initiatives offer a "break the glass" provision, or a way for a provider to access patient information that has been sequestered. On the other side of the discussion, many patient and consumer advocates counter that individuals should be afforded a choice, and that such decisions could ultimately be facilitated by enhanced patient / provider communication and the provision of more and better information.

Kaiser Permanente's Mid-Atlantic regional exchange provides an example of the complexity of these policy decisions and the interplay of legal considerations and the desirability of enabling segmentation given such safety concerns. Largely due to minor consent laws, policy makers at Kaiser chose to limit the information contained in its integrated EHR / PHR system[177] for individuals between the ages of 13 and 18 to just a few categories, including allergies, immunizations and the content of secure messages exchanged with clinicians.[178] Although parents are not given access to the minors' records in such instances, a key concern was the possibility that parents could coerce the minor into providing them with access—thereby necessitating some level of segmentation.[179] Kaiser therefore determined *a priori* a specified list of procedures that it would treat as sensitive and not available to either the minor or parent. Despite this policy determination, and out of a concern for safety, Kaiser Mid-Atlantic opted to include information related to medications and allergies in the exchange which, they acknowledged, could (in some circumstances) reveal information that they had defined as sensitive.[180]

---

[177] Academy Health. "Partner Description: Kaiser Permanente." *HIT and HSR for Actionable Knowledge*, at 2. Available at: http://www.academyhealth.org/files/HIT/KP%20Description%20for%20AH%20HIT%20and%20Research%20Mtg9_18_09.pdf.

[178] Phone call with Dr. Mark Snyder and Lori Potter, *supra* note 155. See also D.C. Code §§ 7-1202.01 (2008) and Md. Code Ann., Health-Gen. §§ 4-301(k)(4)(ii); 20-102(f) (2008).

[179] Phone call with Dr. Mark Snyder and Lori Potter, *supra* note 155.

[180] *Id.*

Another factor often considered in this debate is whether an institution's segmentation policy could effectively mitigate safety concerns related to the availability of complete information on which to base clinical decisions. To address providers' concerns regarding incomplete information, it has been suggested that records from which certain information has been redacted should be flagged or tagged in order to increase providers' trust in the contents. The inclusion of some notation that information is missing would alert a provider that caution and special care may be warranted, and that additional dialogue with the patient (if possible) likely is necessary. However, some advocates have cautioned that the use of flags alone could undermine the critical trust element that exists in the patient-provider relationship.[181]

At least two approaches for such notation have been applied, each with merits and drawbacks. One solution involves provision of a general notice that information has been sequestered, but one that does not identify the specific category of data. Because it is more opaque and less likely to reveal the sensitive information, this approach might be preferred by patients. A disadvantage of this approach from the provider perspective, however, is that it may require further time and effort to discover the information deemed necessary for the provision of safe care.

Another approach, and one more commonly preferred by care providers, requires that the segmented category of data be noted specifically (*e.g.*, mental health information exists but has been sequestered from the record). While it permits the provider to make a more informed judgment as to whether the category is likely to be relevant to the current encounter, it may, in some cases, expose the sensitive information. A permutation of this approach is the scenario in which only the source of the segmented information is noted, not the data itself. This approach too may reveal more than desired by the patient. For example, a notation that information from the Betty Ford Clinic has been sequestered constitutes a pretty strong clue that the individual has been treated for substance abuse.

Implicit in the flagging discussion is the issue of whether an EHR is viewed more as the definitive source for clinicians to gain access to patient clinical information and therefore should be complete (*i.e.*, enable little or no segmentation), or whether it represents a set of information that is to be expanded and enhanced through further patient-provider communication. Of course, the two ideas are not mutually exclusive, but there tend to be strong views on either end of the continuum: those preferring absolute unfettered access as opposed to those willing to cede some control while hoping to make up for information gaps through enhanced patient engagement.

As an example, some exchanges effectively have established an expectation that the EHR should not be viewed as the definitive source of information, and should therefore be augmented with information generated through patient and provider communications. Such groups explain that setting this provider expectation, regardless of whether patient data are missing as a result of segmentation, leads to enhanced patient engagement. When establishing policies regarding segmentation within the MAeHC, for example, the developers encountered concerns from clinicians who were skeptical about the utility of a potentially incomplete record.[182] In response, the MAeHC leadership emphasized the need for clinicians within the exchange to speak with patients and obtain as much information as necessary through those conversations and other

[181] Consumer Partnership for eHealth, *supra* note 5.
[182] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.

channels in order to provide appropriate care.[183] Depending on the predominant view of the purpose of the EHR in a given exchange environment, the implications of segmentation for the participating entities will likely vary.

Quality of care is another factor commonly cited in the discussion of whether and to what extent data segmentation should be accommodated. Specifically, providers often suggest that, absent relevant and potentially important clinical information (*e.g.*, a complete list of medications), they will be unable to guarantee the provision of quality care, including the determination of how best to communicate clinical information to patients. As a key element of quality, care coordination also may be inhibited by a lack of information sharing. For example, a study of small medical practices found that a lack of interoperability between EHRs when exchanging information between practices resulted in incomplete information related to medications and a lack of access to test results, hampering effective care coordination.[184] This factor becomes particularly apparent in situations of care transition, where coordination of information and communication across providers can have significant implications for care quality and patient outcomes.[185]

Workflow Implications

Providers also have expressed concern about the workflow implications of supporting even moderately granular segmentation. In many emerging HIOs, and certainly within discrete provider entities, the default expectation is that clinicians play a role in guiding patients through the consent (and segmentation, if supported) processes. This expectation reflects the fact that most patients prefer to receive information and guidance directly from their health care providers (as opposed to other parties in the health care system (*e.g.*, insurers)). Despite this preference, providers typically do not have sufficient time in their patient encounters to spend on non-clinical matters, and might view those related to information management as such.[186]

Additionally, many clinicians may not view such interactions as a requisite or desired part of their role as a provider, which is often linked to concerns about the specific interface used for establishing segmentation preferences.[187] Some providers are reluctant to spend time interacting with EHRs in the presence of patients because of the perception that it disrupts the encounter,[188] and studies have shown that some providers believe the typical process for documentation in EHRs distracts them from their interactions with patients.[189] Similarly, some providers believe

---

[183] *Id.*

[184] O'Malley, J. M. Grossman, G. R. Cohen et al., "Are Electronic Medical Records Helpful for Care Coordination? Experiences of Physician Practices," *Journal of General Internal Medicine*, published online Dec. 29, 2009.

[185] Boyd, A.D. et al. "Top EHR Challenges in Light of the Stimulus: Enabling Effective Interdisciplinary, Intradisciplinary and Cross-Setting Communication," *Journal of Health Information Management*, Vol. 24, No. 1, Winter 2010, pp. 18-24, at 19.

[186] Developers of the Kaiser HealthConnect system for the Mid-Atlantic region recognized this concern when developing its policies for sensitive information and therefore decided to implement data segmentation on the basis of department (*e.g.*, behavioral health) as opposed to segmentation by individual provider. Phone call with Dr. Mark Snyder and Lori Potter, *supra* note 155.

[187] Phone call with Dr. David Winn, *supra* note 134.

[188] Boyd, *supra* note 185, at 21.

[189] Schiff, G. D. "Can Electronic Clinical Documentation Help Prevent Diagnostic Errors?" *New England Journal of Medicine*, Vol. 362, No. 12, March 25, 2010, pp. 1066-69, at 1066. On the other hand, studies have found that patients do not feel their physicians pays less attention to them as a result of entering information into an EHR. *See, e.g.*, California HealthCare Foundation, *supra* note 26.

EHRs are designed to communicate with insurers and are not good tools for facilitating communications across providers.[190] Further, some providers do not want to take what is perceived as an expanded role as the reliability of such systems is not well understood, and the sustainability of specific products has not been well documented.[191] Without solid evidence, providers may not want to take an active role in pioneering technology that may have quirks and need refinement.[192]

Technology considerations aside, providers may not have the information, tools, expertise or desire necessary to help patients navigate a series of decisions related to information management. One particular issue is whether providers, as agents acting on behalf of their patients, could reasonably be expected to record privacy preferences in a consistent fashion and in appropriate health record fields. Absent such consistency, providers documenting a patient's privacy preferences could categorize information differently, allowing references to sensitive information to remain in the general record.[193]

In efforts to avoid the aforementioned concerns, some systems have developed approaches to aid patients in making decisions regarding privacy preferences without depending on the sole guidance of providers. The VA, for example, implemented the use of privacy advocates and / or security administrators to aid patients in creating appropriate privacy constraints for sensitive information.[194] Such personnel take the direct responsibility away from the provider, and ensures that patient questions and concerns are addressed in order to better satisfy privacy preferences.

Ability to Accommodate Patient Expectations

Many providers (in addition to technology vendors and others) have expressed significant reservations about the ability of their information systems and internal data management processes to accommodate individual segmentation preferences reliably, accurately and completely. One factor referred to above is that, in recording clinical observations and notes as part of a clinical encounter, providers do not always enter data in the intended or usual fields. The concern here is that patients might express a desire to segment from view "all of the data related to their history of depression," but likely would not appreciate how challenging that task may be. To achieve complete success in this example would require the identification of every data point in the record that is related to the information considered sensitive—in this case, a history of depression. On the same note, patients might also be unsympathetic to any failures of a provider's system to accommodate their requests.

Rather than risking the possibility of failing to catch every instance of a data element deemed by the patient as sensitive, many provider organizations and HIOs have expressed reluctance to assume this responsibility. As such, few entities offer much granular patient choice in the area of information management. Some organizations allow for segmentation based on provider type or

---

[190] White, J.A. "A Doctor's Problem With Electronic Records," *Wall Street Journal Health Blog*, February 16, 2010. Available at: http://blogs.wsj.com/health/2010/02/16/a-doctors-problem-with-electronic-records/.
[191] Phone call with Dr. David Winn, *supra* note 134.
[192] Baldwin, G. "EMR Pushback." *HealthLeaders Media*, September 14, 2007. Available at: http://www.healthleadersmedia.com/content/TEC-92119/EMR-Pushback.html.
[193] Phone call with Dr. John Mattison, *supra* note 142.
[194] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57.

name, but very few are willing to hold themselves accountable for ensuring that the more granular preferences of patients are enabled. In general, either segmentation preferences of this nature are not allowed, or certain types of data (those related to sensitive conditions) are excluded altogether from exchange.

Liability Concerns

In addition to the accountability issue, and related also to the safety and care quality points discussed above, providers also have expressed concern about the extent to which they may be held responsible or liable for a patient's experience in situations where, despite access to an EHR, the provider did not have all of the information at his / her disposal that would be clinically relevant for that patient's situation.[195] As EHRs are viewed increasingly as a tool to help alleviate important information gaps (such as providing a complete medication list), providers have little interest in minimizing their utility by enabling segmentation. Their concern lies in the idea that, if the standard of practice in the future is for providers to consult their information systems (*e.g.*, EHRs) to support clinical decision making, then they do not want to be held responsible for actions taken based on imperfect information. However, to date efforts to evaluate the impact of electronic exchange of health information on providers' medical malpractice liability have not found sufficient legal basis on which to make conclusions.[196]

Finally, concerns regarding interpretation of and compliance with legal requirements may also create reluctance to pursue electronic exchange. For example, developers of the Clinical Management for Behavioral Health Services (CMBHS) system, which enables the electronic exchange of behavioral health records within the state of Texas, have cited interpretation of laws regarding consent as a challenge to their faster pursuit of greater interoperability.[197]

Legal Considerations

As outlined earlier, a complex network of state and federal laws has been developed to protect the privacy of personal health information. Where specific information within an individual's health record falls within the purview of these laws, data segmentation could serve as a useful tool in facilitating compliance that still allows for meaningful electronic exchange. However, the wide variety in these laws can pose challenges for entities whose goal is to exchange health information on a regional, or even national, basis.[198] Examples of such laws are addressed below.

HITECH out-of-pocket provision

The HITECH provision requiring that providers honor a patient's request to restrict disclosure of PHI related to treatment or services for which the patient has paid out-of-pocket in full presents a

---

[195] NCVHS, *supra* note 51.

[196] Shay, E. et al. "Medical Malpractice and Other Potential Liability," in Rosati, K. and M. Lamar (eds.), *The Quest for Interoperable Electronic Health Records: A Guide to Legal Issues in Establishing Health Information Networks* (American Health Lawyers Association, July 2005): pp. 88-95, at 88.

[197] Mitra, D. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010, at 1. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913478_0_0_18/Criticial_Management_for_Behavioral_Health_Sciences_Testimony.pdf.

[198] Consumer Partnership for eHealth, *supra* note 5.

challenge to providers and, more broadly, electronic exchange that advances in data segmentation could help alleviate. The provision places such requirements on the provider only where the purpose of the disclosure is for payment or health care operations purposes and is not otherwise required by law—disclosures made for treatment purposes are allowed regardless of a patient's payment method.[199] The provision therefore seems to require that a system separate information on the basis of both purpose of use and the identity of the recipient. For example, some analysts have highlighted the tremendous segmentation challenge related to preventing insurance companies from accessing information related to procedures paid for out-of-pocket.[200]

Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2)
Part 2 has been perceived as presenting challenges to the development of policies and practices for electronic exchange, particularly in the area of data segmentation. As described above, the regulations strictly limit disclosure and use of information about individuals seeking or obtaining diagnosis, referral or treatment in federally assisted alcohol or drug abuse treatment programs.[201] Because Part 2 generally requires written patient consent for the disclosure of patient-identifying information that specifies, among other things, the purpose of the disclosure, who is to receive the information, and a date or condition upon which the consent expires, data systems that include such information would be required to develop a means of ensuring and documenting such consent, as well as the capability of segmenting the information in order to comply with the law. These challenges might only be amplified in the case of treatment programs that fall under the umbrella of larger organizations with multiple departments that all generate data for the same patient. As a result, it is possible that, despite the continuity of care, quality improvement, and public health benefits that could result from its inclusion, data covered by Part 2 will be excluded from some exchange operations altogether.

Mental Health Information
In a similar manner, laws that protect information specifically related to mental health treatment often prevent disclosure without consent, thus presenting challenges to electronic exchange that advances in data segmentation could help alleviate. Developers themselves are particularly challenged by the prospect of segmenting mental health information that is scattered throughout the health record, for example in primary care records.[202]

As noted previously, larger institutions may face particular difficulties with respect to maintaining the privacy of any information within a patient's health record that could possibly fall within the purview of laws related to mental health treatment. Due to legal concerns, for

[199] HITECH § 13405, 123 Stat. at 264-265 (2009) (to be codified at 42 U.S.C. § 17935); see also Modifications to the HIPAA Privacy, Security and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40867, 40899 - 40901 (proposed July 14, 2010) (to be codified at 42 C.F.R. Parts 160 and 164).
[200] Phone call with Dixie Baker, *supra* note 116.
[201] 42 C.F.R. § 2.3(a) (2009).
[202] HITECH § 13405, 123 Stat. at 264-265 (to be codified at 42 U.S.C. § 17935); *See also* Modifications to the HIPAA Privacy, Security and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40867 (proposed July 14, 2010) (to be codified at 42 C.F.R. Parts 160 and 164). As discussed earlier, CORHIO chose to exclude from exchange any records originating from mental health clinics due to the perceived difficulty of separating out references to mental health that may appear in an individual's record and that may require consent for disclosure.

example, Vanderbilt Medical Center – a large treatment center where patients may receive care from many different departments – created an EHR system that strictly sequesters all information related to mental health treatment, including appointments, psychiatric notes and telephone communications, in a separate database accessible only by psychiatric providers.[203] The Vanderbilt system prevents other providers, such as surgeons or internists, from viewing any information that could indicate that a patient is receiving psychiatric treatment at the institution.[204] It is worth noting, however, that laboratory results, medications, diagnoses and problem lists are listed in the EHR and made available to all providers in the system.[205]

Despite the perceived difficulties associated with the segmentation of information related to both Part 2 and mental health treatment, technology developers have been working on solutions to the various challenges. For example, CMBHS created a technical solution specifically designed to accommodate state and federal regulations regarding medical records related to substance abuse treatment programs and behavioral health. Although CMBHS is currently operating as a closed system, and thus is not exchanging records with outside providers, the system does enable compliance with the consent documentation requirements of Part 2 and other relevant laws. More specifically, CMBHS documents the consent preferences of patients, including allowing for an expiration of consent, and where consent has not been provided for the disclosure of particular information, such information will not be released.[206]

Minors

Segmentation policies and practices with respect to the health information of minors are also viewed as challenging, in part due to the multiple factors and perspectives that must be considered. These include laws related to the rights of minors to consent to procedures, the rights of parents to access related records, the sometimes-conflicting needs and interests of both parents and minors, and factors related to the unique qualities of minors themselves, such as vulnerability to coercion or abuse. For example, developers of electronic exchange efforts in New York determined that compliance with New York minor consent laws would require a system to tag all data related to a procedure to which a minor has consented, record the related minor consent status in a structured field, and then transmit minor consent status and information tags within the exchange.[207] In the face of these complications, the New York Statewide Collaboration Process (SCP), in its recommendations for policies and procedures for HIOs in the State of New York, suggested excluding the exchange of health records of minors above a minimum age, but allowing the exchange of health records of younger children.[208] The SCP has yet to recommend a minimum age, but concluded that the harm of blocking young children's

---

[203] Salomon, *supra* note 138.
[204] *Id.*
[205] *Id.*
[206] Phone call with Debabrata Mitra, Senior Architect, Substance Abuse and Mental Health Application Development, Texas Clinical Management for Behavioral Health Services, April 28, 2010.
[207] New York eHealth Collaborative. "EHR Functional Requirements, Version 2.2," November 10, 2009, at 221. Available at: http://www.nyehealth.org/images/files/File_Repository16/pdf/Version_2_2_EHR_Functional_Requirements-16_Nov_09.pdf.
[208] New York Statewide Collaborative Process, New York Health Information Security and Privacy Collaboration. "Recommendatins for Standardized Consumer Consent Policies and Procedures for RHIOs in New York," November, 2008, at 35. Available at: http://www.nyehealth.org/images/files/File_Repository16/pdf/Consent_White_Paper_20081125.pdf.

records from an exchange was considerable and outweighed the privacy concerns regarding the small number of minor consent procedures that would likely occur among children in that age range.[209]

As mentioned earlier, Kaiser's Mid-Atlantic region likewise has recognized the challenges of respecting a minor's privacy rights and has chosen to limit the information included in the health records of 13 – 18 year olds to allergies and immunizations.[210] By doing so, Kaiser hoped to avoid violating the varied and conflicting laws related to minor access that would apply in the Mid-Atlantic region. These include, for example, a Washington, DC law that allows a minor of any age to consent to a limited amount of outpatient treatment for mental health and protects the related records, and a Maryland law that only allows minors age 16 and over to consent to behavioral health treatment, but gives the health care provider discretion regarding disclosing the related records to the parent.[211]

Finally, Indivo's solution for protecting a minor's privacy in a way that complies with the many different Massachusetts state laws related to minor consent involves granting different levels of parental access to the record according to the minor's age.[212] Under Massachusetts law, a drug-dependent minor age 12 and older may consent to substance abuse treatment, while a minor must be at least 16 in order to consent to outpatient mental health treatment.[213] A minor of any age may consent to treatment for HIV or an STI.[214] In the Indivo system, a parent is granted full access to the health record if the minor is under 13, while the parent of a minor between the ages of 13 and 18 is granted access to non-sensitive information in the record and the adolescent is granted control of all sensitive information.[215]

EXAMPLES OF SYSTEMS ENGAGING IN DATA SEGMENTATION

Data Segmentation in the Health Care Sector

As discussed above, several core components, including the level at which information is segmented (*i.e.*, capture, access, or view); the party that decides what information will be blocked; the person or entity that holds the authority and ability to apply segmentation preferences; the data that are eligible for exchange; and the part(ies) allowed access to the data for what purpose and what amount of time all affect the performance of data segmentation and, therefore, information sharing in general. This section explores the concept of data segmentation by analyzing examples of approaches that have been developed within the health care sector. After an introductory discussion of general developments within the field, the section is organized first by categorizing the person or entity that holds the authority and ability to apply segmentation preferences, followed by a more detailed discussion of particular examples. The

---

[209] *Id.*
[210] Phone call with Dr. Mark Snyder and Lori Potter, *supra* note 155.
[211] D.C. CODE § 7-1231.14(b) (2008); D.C. MUN. REGS. tit. 22, § 600.7 (2008); D.C. CODE §§ 7-1202.01 (2008) and MD. CODE ANN., Health-Gen § 20-104(a)(1)(2008); MD. CODE ANN., Health-Gen. §§ 4-301(k)(4)(ii); 20-102(f) (2008).
[212] NCVHS, *supra* note 53.
[213] MASS. GEN. LAWS ch. 112, § 12E (2008); MASS.GEN.LAWS ch. 112, § 117 and 105 MASS. CODE REGS. 300.001 and 300.180 (2008).
[214] Mass. Gen. Laws ch. 123, § 10 (2008); 104 Mass. Code res. 25.04 (2008).
[215] NCVHS, *supra* note 53.

featured systems are intended to reflect the various stages of development and diversity within the field, but are not exhaustive or fully representative of the data segmentation landscape. In addition, most systems do not fall neatly within one particular category, as their methods and processes (and, indeed the categories themselves) are constantly evolving.

As discussed at the recent Consumer Choice Technology Hearing sponsored by the Tiger Team,[216] and later in the Tiger Team's initial set of draft recommendations,[217] the prevailing view is that technologies capable of enabling granular segmentation are promising in general but still in the early stages of development.[218] For example, as the Tiger Team noted, many EHR systems can suppress narrative psychotherapy notes and some vendors offer the ability to suppress specific codes,[219] but the communication of those rules or protocols across systems still poses a challenge.

Commercial applications can also apply filtering to aggregate information pursuant to contractual or legal requirements, but most commercial EHR systems do not yet offer that capacity on an individual patient basis. Some allow a user to set access controls according to episode of care / encounter / location of encounter, but may not include all of the information generated in a particular episode (*e.g.*, prescription information). Further, prevention of downstream clinical inferences remains a challenge—that is, it does not yet seem possible to prevent inferences that might be made from, for example, the inclusion of lab test results in a record that indicate a particular malady, even though the diagnosis notation itself has been blocked from view. Finally, as the Tiger Team noted, the possibility of "tagging" or applying patient consent notations to data so that they follow the data as it is shared across entities has not been implemented successfully on a large-scale basis within health care or any other sector.[220] While there are currently several examples of EHRs that allow a practitioner to label data that should not be passed on without consent,[221] this technology has been implemented only "locally" within a hospital, hospital network, provider network or physician group. Although work is being done in the area, developers have not yet created a method to propagate segmentation preferences seamlessly across multiple institutions or systems electronically.[222]

Patient-controlled segmentation

As previously discussed, data segmentation policies have been captured in law and institutional governance at least in part to accommodate individual preferences with respect to health information sharing. However, it is not common at this point for individuals to apply these preferences to their data directly. Currently, the most dominant model is for patient preferences

---

[216] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57.
[217] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25.
[218] *Id.* at 15.
[219] *Id.* at 14.
[220] *Id.* at 14-15.
[221] *See, e.g.*, Stearns, M. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010, at 2. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913480_0_0_18/eMDs_Testimony.pdf; Texas Department of State Health Services. *Clinical Management for Behavioral Health Services*, June 7, 2010. Available at: http://www.dshs.state.tx.us/cmbhs/.
[222] Phone call with Ioana Singureanu, *supra* note 129.

to be put in place by a provider (possibly via use of an EHR or other application) or by an institution or organization acting on the individual's behalf.

At the present time, only PCHR / PHR systems offer patients the ability to apply segmentation preferences directly to their data. As the Tiger Team recently noted, however, even the most sophisticated of these systems currently provide individuals with control over only copies of their information. That is, patients are not able to control the provider's documentation or the flow of information once the patient releases it to another entity.[223] Firms within this industry argue that PHRs nevertheless present the most achievable privacy solution – particularly with respect to segmentation – because they allow data from multiple providers to accumulate in one place and give patients control over how that copy of the information is then shared (or not) with providers and other entities.[224]

PHRs allow patients to share data with specified providers.[225] That is, patients can direct the health information contained in their PHR to their GP, psychiatrist, cardiologist, or all / none of the above. In addition, some PHR systems function as electronic document repositories for medical documents received from different providers, giving patients control over which documents are shared with new providers.[226] This method of information sharing, however, still does not give the patient control over the original provider record.[227] Even within systems in which the PHR is "tethered" to a hospital or provider network, the patient cannot exercise complete control over the provider's documentation from within the PHR. Systems with "untethered" PHRs allow the patient to control access and grant privileges to others to use information within the PHR, but are not connected to a provider's electronic system.[228] Patients have the responsibility to manage and maintain all information, including entering it into the PHR or, alternatively, arranging for the information to be transferred from a specific source.[229]

Microsoft HealthVault

Microsoft HealthVault is a PHR that enables a user to share information either directly with other users or with third party programs. When sharing a health record directly with other users, which could include an individual provider, HealthVault allows the user to filter out parts of the record.[230] However, when a user shares information with a third-party "network," which could include allowing a hospital to view and / or contribute information to the PHR, the user has more limited ability to filter out portions of the record. In these cases, the user must grant the third party entity access to any parts of the record the entity has determined are necessary.[231] These

---

[223] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25, at 15.
[224] Phone call with Dr. Ben Adida, *supra* note 75.
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] The Children's Partnership. *Technology Profile: Personal Health Records*, 2009, at 1. Available at: http://www.childrenspartnership.org/AM/Template.cfm?Section=Technology_Enabled_Innovations&Template=/CM/ContentDisplay.cfm&ContentID=13566.
[229] *Id.*
[230] Phone call with Kathleen Connor, *supra* note 175.
[231] Sujansky and Associates, LLC. "Meeting the Requirements of Project HealthDesign: Comparative Analysis with Respect to Existing and Emerging Clinical Data Standards and Commercial PHR Data Repositories." Prepared for: *Project HealthDesign*, August, 2008, at 20. Available at: http://www.projecthealthdesign.org/media/file/Meeting_the_PHD_Req_Comp_Analysis_8-15.pdf.

designations will vary and must be described fully in the privacy policy of the third party program and agreed to by the HealthVault user.[232] Where the third-party program considers information in the user's health record to be optional for its needs, the user may have the ability to limit access to such information, depending on the policies of the third party program.[233] HealthVault does flag records when information has been filtered in response to a query, alerting the recipient of the information that information is missing from the record.[234] In addition, HealthVault allows consumers to alter professional-sourced information, but does flag such information as altered.[235]

Google Health

Google Health is a PHR that allows consumers to manage their health records in partnership with various institutions and EHR platforms.[236] Users can link their profile to Google Health partners' websites, giving the partners authority to read or automatically send and / or update information in the profile.[237] Partners who have been given permission to view a user's profile will be able to view the entire profile, even though they may only need information from a specific category, for example medications.[238] Google Health users can also share their profiles with individuals, such as family members, friends, or providers, by issuing an invitation via email granting access to view the profile.[239] However, Google Health currently does not offer consumers the opportunity to restrict access electronically to specific portions of their profile.[240]

If users choose not to import their medical records through Google Health partners, they have the ability to enter their medical history manually. Unlike Microsoft HealthVault, Google Health does not allow users to alter professional sourced information.[241] Google Health was built to CCR standards but plans to embrace CCD standards as well.[242]

Tolven, Inc.

Tolven, Inc. (Tolven) has developed an open source system for enabling patient control over the electronic sharing of personal health information.[243] Key elements of Tolven's solution include acting as a secure repository for copies of a patient's health records and enabling patients to control both the importation of information into the patient's PHR and the disclosure of

---

[232] *Id.*
[233] *Id.*
[234] Phone call with Kathleen Connor, *supra* note 175.
[235] Simborg, D.W. "Limits of Free Speech: The PHR Problem," *Journal of the American Medical Informatics Association*, Vol. 16, No. 3, May/June 2009, pp. 282-83, at 283.
[236] Google Health. *Personal Health Services*. Available at: https://health.google.com/health/directory?cat=importrecords.
[237] Google Health, *supra* note 176.
[238] Phone call with Kathleen Connor, *supra* note 175.
[239] Google Health, *supra* note 176.
[240] Phone call with Dr. Ben Adida, *supra* note 75.
[241] Simborg, *supra* note 235.
[242] Impact Advisors, LLC. *eHealth Strategies with Microsoft and Google in the Game*, September 30, 2008, at 9. Available at: http://www.impact-advisors.com/UserFiles/file/IA%20Whitepaper%20-%20%20eHealth-PHR-%20ala%20Google%20and%20MS%20%2020090510.pdf.
[243] Health Record Banking Alliance. *Principles and Fact Sheet*, 2008. Available at: http://www.healthbanking.org/docs/HRBA%20Principles%20&%20Fact%20Sheet%202008%20FINAL.pdf.

information from the PHR.[244] As described in more detail in the International Examples section, this solution is currently being implemented in the Stichting RijnmondNet (RijnmondNet) pilot project in the Netherlands, where Dutch law requires that a patient have complete control over the distribution of his / her personal health information.[245]

The Tolven platform provides each participating patient with a PHR and each participating clinician with a general EHR and a specialty EHR if the clinician is part of a participating specialty group.[246] In Tolven's solution, a patient first consents to have health records sent from a provider to a secure aggregation area, which can accept documents in any format, extract information, and record it in a format on which rules can be run to enable segmentation.[247] Once the patient has set up the PHR, the patient can request that specific information from the aggregation area be copied, encrypted and distributed to the PHR.[248] In this way, the patient can control exactly what information is transferred into his / her PHR. In addition, when the patient initially establishes this connection with the aggregation area, the patient can choose to have all records related to that patient automatically copied and sent to the PHR from that time forward.[249]

Once the patient's health information has populated the PHR, Tolven's system allows the patient to create and distribute encrypted copies of the PHR to providers within the health record bank environment that contain only the information the patient wants to share, again down to the clinical element level.[250] When a copy of a PHR is missing information, Tolven's technology can be configured to flag the record in a way that will indicate to the recipient that the record is not complete.[251] Additionally, Tolven's technology enables a patient to send a copy of his / her PHR to providers or any other individual outside of the health record bank environment in a variety of formats and is able to include a consent directive with the PHR indicating the patient's privacy preferences.[252] Once a record is sent to a provider or individual outside of the health record bank environment, however, there is no means of enforcing those consent preferences.[253]

Private Access, Inc.

Private Access, Inc. differs from the applications discussed above in that it currently enables patient control over access to personal health information only within the context of clinical research trials. The company does, however, envision extending the applications of their technology to other areas of health information sharing, including EHRs, bio-banks and health information exchange.[254]

---

[244] Jones, T. "Security by Design," *Comment on Public Notice #29*, at 3. Available at: http://fjallfoss.fcc.gov/ecfs/document/view.action?id=7020383780.
[245] 2 ch. 8 art. Wet Bescherming Persoonsgegvens (Personal Data Protection Act 2000) (NETH.).
[246] Jones, *supra* note 244, at 2.
[247] Jones, T. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913484_0_0_18/Tolven_Institute_Testimony.pdf
[248] Jones, *supra* note 244, at 2.
[249] *Id.*
[250] Jones, *supra* note 247.
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] Shelton, *supra* note 169.

The Private Access software platform offers patients the use of centrally-maintained consent directives and some granular privacy settings. The company obtains patients' consent and releases their health information in an "environment of trust"[255] where they can establish and manage their consent regarding health or other confidential information.[256] The pilot production of the platform in the clinical trial context allows researchers to recruit subjects who have characteristics that make them eligible for a particular trial.[257] Patients have the ability to allow particular researchers access to some or all (or none) of their personal health information based on their personal choice and prevailing law.[258] Additionally, the Private Access platform addresses issues related to consent preferences over time by requiring that such preferences be reviewed at any point that data moves or is proposed to move.[259]

Private Access stores and manages patients' consent directives through a technology platform called "PrivacyLayer,"[260] which has the capability of combining federal and state laws, institutional policies and patient preferences into a single filter or adjudicator.[261] Data seekers can be individuals (such as a primary care doctor or a single researcher), an entity (such as a hospital or pharmacy chain) or a group of entities (such as all doctors) that wish to access patients' records.[262] Data holders (*i.e.*, patients) create consent directives through the use of a series of guides or trusted intermediaries, which educate patients through interactive tutorials.[263] A data seeker will search Private Access's database for patients with particular characteristics[264] and, based upon a data holder's privacy settings, some of a patient's information may be visible.[265] If data seekers would like to see more information than allowed through the PrivacyLayer platform, a message can be sent to the patient requesting access. Patients then have the ability to grant access, ask for clarifying information (*e.g.*, about the data seeker) or deny access.[266]

Private Access is developing new applications that will allow for the sharing of health records and provide patients with the ability to redact information from a record and control with great specificity what information is shared.[267] In addition, the company is developing Application Programming Interfaces (APIs) that will allow software developers to build upon or modify their health applications in order to access the PrivacyLayer platform, including the Private Access database of consents and privacy adjudication engine, and use the Private Access technology to enable sharing of data on the basis of patient preferences.[268] However this capability is

[255] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 241-42.
[256] Shelton, *supra* note 169, at 5.
[257] Private Access, Inc. *About Us*. Available at https://www.privateaccess.info/about-us/.
[258] *Id.*
[259] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 380.
[260] Shelton, *supra* note 169, at 2.
[261] Phone call with Robert Shelton, *supra* note 154.
[262] Shelton, *supra* note 169, at 2.
[263] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 234.
[264] *Id.* at 241.
[265] *Id.*
[266] *Id.*
[267] *Id*. at 242.
[268] Shelton, *supra* note 169, at 2.

conditioned on the ability of the systems using the platform to remove or redact data that is meant to be segmented.[269]

Individual Provider-controlled segmentation
As noted above, PCHR / PHR systems allow patients to apply their segmentation preferences directly only to copies of their data—they have no ability to control a provider's documentation.[270] Segmentation systems have also been developed, however, that allow individual providers to act as the patient's proxy in recording data sharing preferences, typically through the use of an EHR or other application. The systems described below provide examples of technology solutions for use by the individual provider in implementing segmentation preferences—either those of the patient or those based upon the provider's own judgment.

<u>e-MDs</u>
e-MDs provides EHR solutions that currently work off of local servers as opposed to central or regional servers. The platform automatically defines certain categories of information as "sensitive" or "private" based on state and federal law, typically including information related to mental health, substance abuse, STIs and HIV.[271] However, e-MDs also offers providers an option to mark additional information as "private" in order to accommodate patient preferences.[272] Through the use of "meta tags," the provider can mark information as confidential in several areas of the EHR.[273]

In the health summary section of the EHR, for example, a provider can select a customizable template that will automatically tag predefined information, such as HIV status, as confidential.[274] Alternatively, or in addition to the default set of privacy tags, providers can mark individual data elements as confidential at the time the information is entered into the record; this allows providers to engage in a dialogue with patients regarding their preferences during the course of a clinical encounter. All information marked as private in the health summary is blacked out when viewed by someone without the required access privilege, thus indicating that confidential information exists in the record.[275] If a medication has been marked as private in the medications section of the summary, a note will indicate that the patient has been prescribed a medication, but will divulge no further information.[276]

In the progress notes section of the EHR, where free text is entered, e-MDs enables meta tags to be attached to any text the patient wishes to keep private. The software has insertion points at every sentence, allowing the provider to tag individual sentences as confidential.[277] As in the case of the health summary section, an individual without necessary privileges who attempts to view the document will see blacked out text where sentences have been marked private.[278]

---

[269] Phone call with Robert Shelton, *supra* note 154.
[270] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25.
[271] Phone call with Dr. David Winn, *supra* note 134.
[272] *Id.*
[273] Stearns, *supra* note 221.
[274] *Id.*
[275] *Id.*
[276] *Id.*
[277] Phone call with Dr. David Winn, *supra* note 134.
[278] Stearns, *supra* note 221, at 4.

Although information marked private in e-MDs appears as blacked out text when viewed in the summary record, providers have options regarding redacted information when exporting or printing. The provider can print or export a version of the EHR with the private information blacked out, thus indicating that information has been redacted, or the provider can choose to print or export a version in which the confidential information is missing completely, thus providing no indication that the record is incomplete.[279] Additionally, providers who choose to export the document as a CCR can export the document with or without the confidential information. This functionality will soon be expanded to the exporting of documents as a CCD as well.[280]

While e-MDs has not implemented its privacy system across other EHRs (it is a user-driven feature built in to this particular technology), the data transferred via CCR and CCD conform to standards that are readable and interpretable by other systems. Until the receiving systems are able to recognize the privacy tags applied by e-MDs, however, they will not be able to identify the information as confidential and treat it appropriately.[281]

According to recent testimony, the software's privacy-enabling technology, in particular the provider's ability to mark data as sensitive, has not been widely utilized.[282] However, one exception to this may be instances where employees of a facility also happen to be patients at the same facility. In these cases, the function enabling restriction of access by particular users has been employed more frequently.[283]

Texas Department of State Health Services Clinical Management for Behavioral Health Services (CMBHS)

CMBHS is an EHR system developed to serve behavioral health and substance abuse providers in the state of Texas.[284] The system implements role-based security that allows the sharing of health information based on a patient's consent preferences.[285] Data segmentation with significant granularity is enabled by the system, although it is not interoperable: electronic exchange occurs only among providers using the same system.

The data in a patient's record are separated by category, such as intake assessment or substance abuse assessment, and each type of data is stored as a separate document on a central database.[286] This system enables access controls to be applied to each data type, allowing the patient to release the entire record or segment categories in order to exchange only specific data.[287] For example, a patient could completely hide progress notes or a substance abuse assessment.[288] During a patient encounter, the provider works with the patient to complete an

[279] *Id.* at 3.
[280] *Id*. at 2.
[281] Phone call with Dr. David Winn, *supra* note 134.
[282] Stearns, *supra* note 221, at 7.
[283] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 70.
[284] Texas Department of State Health Services, *supra* note 221.
[285] *Id.*
[286] Phone call with Debabrata Mitra, *supra* note 206.
[287] *Id.*
[288] *Id.*

electronic consent form that indicates which types of clinical documents may be released, which providers may have access to those documents, a date range for access and an expiration date of the consent.[289] Hard copies of the consent form are completed, printed, and signed by the patient before being saved in the CMBHS system.[290] Once the consent form is saved in the system, specified providers have access to the information until the expiration date of the consent unless it is revoked prior to the expiration date.[291] In addition, once information is shared with one provider in the system, other providers within that provider's organization can access the information.[292]

Currently, the CMBHS system does not allow for interoperable electronic exchange—its developers explain that, because the systems reside on a central database and have utilized a significant amount of customized coding, interoperability has not yet been possible.[293] At present, each system can only connect to primary health care providers, for example, via fax.[294] However, CMBHS is moving toward more standard coding and is planning to enable electronic exchange in the future.[295]

Other Systems

In addition to PHCR / PHR models that allow patients to apply their information sharing preferences directly to copies of their data and systems where individual providers segment patient data based either on patient preferences or their own judgment, a number of systems have been developed that operationalize data segmentation instead at the organizational level, although they vary widely in both design and application. Whereas an EHR such as e-MDs might incorporate functionality that allows a practitioner to segment data as part of his / her interaction with an EHR, other systems might, for example, utilize a layer of software in addition to an EHR that executes segmentation rules on data within the system. That is, an organization might design its policies and infrastructure to allow for standard data segmentation and patient consent options across all users, and might execute those policies through the use of overarching technology applied to data within the system. Some systems do so through the use of a Service Oriented Architecture (SOA) solution,[296] while others might utilize third-party applications such as consent management systems that act as an outside rules or intelligence engine. In both cases, the system itself articulates the rules and policies to be implemented by the technology. The systems discussed briefly below provide examples of a few of these types of "collaborative" or "hybrid" systems—organizations that allow for data segmentation with some degree of granularity through the system-wide implementation of policies and rules. Following a discussion of the organizations themselves, we provide a few examples of the third-party systems

---

[289] Mitra, *supra* note 197.
[290] Texas Department of State Health Services. *BHIPS Functionality Definition*, March 7, 2010. Available at: http://www.dshs.state.tx.us/sa/BHIPS/functionality.shtm.
[291] *Id.*
[292] Phone call with Debabrata Mitra, *supra* note 206.
[293] *Id.*
[294] *Id.*
[295] *Id.*
[296] Service-oriented architectures are web-based, third party services that offer data routing and management services. These systems can also act as intermediaries between different computer languages. *See* Sprott, D. and L. Wilkes. "Understanding Service-Oriented Architecture," *MSDN Library*, January 2004. Available at: http://msdn.microsoft.com/en-us/library/aa480021.aspx.

that organizations might choose to utilize in addition to their own technology infrastructure for data segmentation and consent management purposes.

Users

The Massachusetts eHealth Collaborative

MAeHC's pilot electronic exchange program provides an example of data segmentation enabled at the organizational level. That is, the rules and protocols for the sharing of information within the system are determined by the HIO (as opposed to individual providers, provider groups, or patients). The HIO's policies, however, were developed with the input of key stakeholders, including consumer-focused organizations, and the help of steering committees in each of the participating communities.[297]

MAeHC gives participating providers access to a community repository of clinical summaries, including data on patient problems, procedures, allergies, medications, demographics, smoking status, diagnosis, lab results, and radiology reports.[298] The HIO itself predefined information that it considered sensitive, including HIV status, genetic information and mental health information, and created access controls to segment that data at the exchange level, preventing the sensitive information from being part of the repository to which providers had access.[299] If the participating provider's EHR system had a rules engine, the filtering of the sensitive information, as defined by MAeHC, would occur at the EHR level before the record was sent to the exchange. However, if the EHR involved did not have such a rules engine, filtering occurred at the exchange level. Data coming into the exchange would be processed by a rules engine capable of stripping out data types defined as sensitive by the exchange.[300]

MAeHC therefore has the infrastructure with which to segment patient data, but has determined at the outset what types of information will be segmented by the system. The patient has no input at the point of segmentation regarding what data should be segmented and what should not; nor, for that matter, does the provider—at least not directly.

Kaiser Permanente

In 2002, Kaiser Permanente partnered with Epic Systems Corporation to create and implement a program-wide integrated EHR—KP HealthConnect. The system combines an EHR system with a tethered PHR system,[301] through which patients have web-based access to portions of their health record and can send secure messages to clinicians as well as schedule appointments. The data collected by the EHR system includes both coded and free text information related to patient demographics; appointments; encounters (including diagnosis and procedure codes); prescriptions; lab tests; and longitudinal records of vital signs.[302] The system maintains control over the categories of information contained in the EHR.

---

[297] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.
[298] Tripathi, M. *Massachusetts e-Health Collaborative Powerpoint Presentation*, December 2008. Available at: http://www.mendocinohre.org/rhic/200812/rhic_tripathi_20081217.ppt.
[299] Phone call with Nael Hafez and Barbara Lund, *supra* note 118.
[300] *Id.*
[301] Academy Health, *supra* note 177.
[302] *Id.*

Although HealthConnect has a common national governance, each region of Kaiser Permanente may implement it somewhat differently according to local needs.[303] Uniform data definitions and semantic interoperability are maintained through the use of an internally-developed terminology solution.[304] However, policy decisions regarding segmentation of information in the health record may vary depending on the laws in each area. For example, HealthConnect in the Mid-Atlantic region restricts access to behavioral health records only to behavioral health providers due to state laws prohibiting the exchange of such information without patient consent.[305] Additionally, developers of this policy felt that segmenting on the basis of department, such as behavioral health, made it easier for providers to understand what information they were and were not receiving in a record.[306]

Veterans Health Administration

The VHA within the VA operates one of the first electronic health information systems in the U.S., the Veterans Health Information Systems and Technology Architecture (VistA).[307] Components of VistA are operational in all of the VHA's 1,400 clinical centers; clinical data are stored at 129 local data centers and is gradually being migrated to four regional data processing centers.[308]

VistA's primary clinician access software provides a single interface for physicians and other health care providers to use in reviewing and updating a patient's medical record.[309] The patient data collected and organized includes an active problem list, allergies, current medications, lab results, vital signs, hospitalization records and outpatient clinic history.[310] Providers search for a patient and, after finding the patient in the system, can request the patient's health record.[311] Information will be returned to the provider on the basis of access controls enforced by security and privacy policies.[312] Within the VHA, personnel have access to all or part of a patient's record depending on their clinical role, with the exception of information on drug and alcohol abuse, HIV status, and sickle cell anemia, all of which require written consent for disclosure pursuant to a statutory mandate.[313] Additionally, personnel have the ability to "declare

---

[303] *Id.* at 1.
[304] *Id.*
[305] Phone call with Dr. Mark Snyder and Lori Potter, *supra* note 155.
[306] *Id.*
[307] American Council for Technology. *VistA Modernization Report*, May 4, 2010, at 8. Available at: http://www.actgov.org/knowledgebank/studies/Documents/VistA%20Modernization%20Report%20-%20Legacy%20to%20Leadership,%20May%204,%202010.pdf
[308] Academy Health. "Partner Description: Veterans Health Administration." *HIT and HSR for Actionable Knowledge*, at 1. Available at: http://www.academyhealth.org/files/HIT/VHA%20Academy%20Health.pdf.
[309] Department of Veterans Affairs, Office of Enterprise Development. *VistA HealtheVet Monograph*, July 2008, at 6. Available at: http://www4.va.gov/vista_monograph/.
[310] *Id.*
[311] Davis, J. and D. Staggs. "Presentation to Health Information Technology Policy and Standards Committees: Implementing Advanced Security and Privacy in the Nationwide Health Information Network," *Department of Veterans Affairs*, June 17, 2010, at 41. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11988_912248_0_0_18/Privacy-Security-WG-061710.pdf.
[312] *Id.*
[313] Department of Veterans Affairs. *HIV/AIDS: Confidentiality in the VA System*, January 2002. Available at: http://www.hiv.va.gov/vahiv?page=prtop03-ov-01**;** 38 U.S.C. 7332(b)(2)(A).

emergency" to gain full access to a patient's record in the case of emergency.[314] Patients can also access their record online through "My HealtheVet," which functions much like a PHR.[315]

Currently, VHA's pilot with Kaiser Permanente in San Diego (described above) is in limited production, with fewer than 300 participating patients out of 1,200 in the population base.[316] The San Diego pilot enforces general opt-in or opt-out preferences,[317] collected using paper-based consent directives, but does not allow more granular consent options at this time.[318] Utilizing a federated consent model, the pilot requires patients to sign a consent agreement with each organization that may produce or share their information, which in the case of the pilot includes only Kaiser Permanente.[319] Thus, as currently implemented, patients must negotiate their consent preferences and choices with each provider.[320] The pilot's default organizational policy then allows providers from each of those organizations to assert the role of medical doctor and obtain access to patient information. At the time of exchange, a policy engine applies the patient's preferences to the patient's data and redacts any information that should not be exchanged.[321]

Expansion of the pilot to Hampton, Virginia is planned for early 2011 and will include additional features, such as an electronic consent directive that identifies veterans' preferences using standard-based semantics, roles, and concept codes,[322] and possibly more granular consent.[323] The use cases for the project, which include allowing a patient to hide medications from specific providers; allowing an emergency access override; and allowing protection of a patient's genomic data, would all support potential utilization of data segmentation with significant granularity.[324]

The VA's newest pilot project will take place in Indianapolis in partnership with the Indiana Health Information Exchange.[325] The Indiana pilot will use the same technology as that in development in San Diego, but will use a face-to-face consent process between patients and a VA representative (as opposed to a provider).

---

[314] Davis, *supra* note 311.
[315] Department of Veterans Affairs. *About My Healthevet*, July 2009. Available at: https://www.myhealth.va.gov/mhv-portal-web/anonymous.portal?_nfpb=true&_nfto=false&_pageLabel=aboutMHVHome.
[316] DeCouteau, D. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010, at 2. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913479_0_0_18/Department_of_Veterans_Affairs_Testimony.pdf.
[317] *See* Goldstein, *supra* note 15 for an analysis of consent options for electronic exchange.
[318] Phone call with Mike Davis, Senior Analyst, Department of Veterans Affairs, July 21, 2010.
[319] DeCouteau, *supra* note 316.
[320] *Id.* at 3.
[321] *Id.* at 2.
[322] *Id*. at 3.
[323] Phone call with Mike Davis, *supra* note 318.
[324] DeCouteau, *supra* note 316.
[325] Conn, J. "VA brings stricter info-sharing controls to Ind.," *Modern HealthCare*, August 30, 2010. Available at: http://www.modernhealthcare.com/article/20100830/NEWS/100829923/1029.

Tools

Indivo

Indivo is a "tethered" PHR system that was developed and released by the Children's Hospital Informatics Program at Harvard. As implemented at Children's Hospital Boston (CHB), Indivo offers some segmentation capabilities.[326] The patient's PHR can be populated with data from patients themselves as well as from electronic data feeds and manual entry from CHB clinical records.[327] Indivo's design excludes sensitive data, such as HIV status, from the record.[328] While in the future Indivo plans to allow electronic data feeds from primary care providers and others outside of the CHB system, at this time clinical data is sourced from CHB systems only.[329] Thus, patients can add information such as blood sugar measurements to their Indivo PHR, but cannot load data from providers outside the hospital system into the record. The patient, however, does have the ability to share information with outside entities, including other providers, by e-mailing a copy of the record.[330] Additionally, patients may share information with those outside the CHB system by inviting providers, schools or others to create an Indivo account and access the patient's information through Indivo.[331] The patient has the ability to hide medications, problems, documents or results from any individual given access to their PHR via this means.[332]

Indivo is an open source solution, developed to be extended and customized. The latest version of the software, Indivo X Alpha 3, is in alpha release for developers only[333] and has the capability for simple role-based access control.[334] That is, patients can create groups, and documents within the record can be shared or withheld from individuals granted access to the record based on the individual's relationship with the patient. For example, settings could be created to give all doctors full access to the record while entities such as schools are only given access to immunization records.[335] Indivo X may also increase the granularity of data within the system by using a data processing pipeline to segment data elements from documents in the record and enable sharing of more relevant data with third-party applications such as wellness programs.[336] They have pre-selected a group of basic fields to segment, including allergies, encounters, immunizations and problem lists, among others.[337]

---

[326] Bourgeois, F.C. et al. "MyChildren's: Integration of a Personally Controlled Health Record with a Tethered Patient Portal for a Pediatric and Adolescent Population," *American Medical Informatics Association Annual Symposium Proceedings*, November 14, 2009, pp 65-69.
[327] *Id.*
[328] Phone call with Dr. Ben Adida, *supra* note 75.
[329] Bourgeois, *supra* note 326.
[330] Phone call with Dr. Ben Adida, *supra* note 75.
[331] Bourgeois, *supra* note 326.
[332] *Id.*
[333] Indiovo Health Wiki. *Releases*. Available at: http://wiki.chip.org/indivo/index.php/Releases (last accessed September 17, 2010).
[334] Phone call with Dr. Ben Adida, *supra* note 75.
[335] *Id.*
[336] *Id.*
[337] *Id.*

InterSystems

InterSystems' HealthShare product implements a consent mechanism within a centralized health exchange system that maintains an index of patients but allows facilities and institutions to maintain control of the information they collect. The HealthShare consent service is capable of merging consent policies, or rules regarding what / to what extent information sharing is allowed, from several entities, including the community or jurisdiction, the facility and the patient, and then applying the proper policy rules to the data in question.[338] Providers who request a patient's record can query the system and, based on the preferences of the patient, facility and jurisdiction, the system returns an aggregated health record with data pulled from each facility or provider that has a record for the same patient. Currently, InterSystems does not offer a patient portal to capture consent preferences; consent typically is collected either via a paper form or verbally in a facility where the patient visits, and then is entered electronically by authorized facility staff.[339] InterSystems has also developed a web-based application that allows a provider to connect to the system and input records and that is adjustable based on user preferences.[340]

HealthShare approaches consent management in two ways—patient matching and clinical data. A first-phase consent filter is applied when a search is made for a particular patient.[341] When the centralized system receives a request for patient matching data, the database only returns information if the patient has agreed to be listed in the system. Patients can select a date range for which the filter is active, and can define which groups or users can receive their patient matching data.[342]

A second-phase consent filter is applied after the patient is identified and returns only portions of the records that the patient has agreed to share. For example, patients can restrict access to certain data types, such as lab results or allergies, or to certain classes of information, such as HIV status or genomic test results. Patients can also restrict access to information by date range, or to specific groups or users.[343] In all cases regarding segmentation of clinical data, however, providers viewing a record are able to see whether information has been filtered and / or information is missing.[344] A provider will receive a note with the record stating that information is missing due to the patient's consent policies.[345] An additional filtering feature enables a provider to "break the glass" and access masked data, although a facility may choose to take away this function if it conflicts with its or the jurisdiction's privacy policies.[346] Also, InterSystems is capable of embedding a patient's consent policy with the data if the data flows outside of the exchange community; however, there is currently no means available to communicate an update or change in the patient's consent preferences.[347]

---

[338] LaRocca, M. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010, at 3-4. Available at: http://www.bhix.org/Downloads/BHIX_ONC_Consumer%20Choice%20Technology%20Hearing_20100629.pdf.
[339] *Id*. at 6.
[340] InterSystems. *Creating Regional and National Electronic Health Records with InterSystems HealthShare*, December 19, 2008. Available at: http://www.InterSystems.com/healthshare/whitepapers/creating_nehr_wp.html.
[341] LaRocca, *supra* note 338, at 4.
[342] *Id.*
[343] *Id.* at 5.
[344] Phone call with Michael LaRocca, Product Manager for HealthShare, InterSystems, June 14, 2010.
[345] LaRocca, *supra* note 338, at 4.
[346] *Id.* at 3.
[347] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 175.

InterSystems has focused on compatibility with a wide range of data standards in order to make a variety of systems interoperable. It has created a software solution to translate standardized data received from other clinical systems, as well as that received from regional and national health information systems. In addition, although not available publicly at this time, InterSystems is pursuing an approach that would allow intelligent parsing of free text for the purpose of tagging relevant information with clinical codes so that consent filters can be applied.[348] Although InterSystems cannot support every standard, it has the ability to customize data transformation and enable compatibility with various data standards.[349] Still, a key technical challenge for InterSystems is the variation among vendor systems that often requires customization to enable integration.[350] Currently, the software is being used for electronic exchange only among organizations within the same HIO.[351]

InterSystems has been a part of developing health exchanges that include privacy policies with data segmentation in both Sweden and the Netherlands. As explained further in the *International Examples* section below, Sweden has implemented HealthShare, using its technology to translate medical records found in existing local formats into a common standard for the national patient record exchange. The exchange distributes patient information only to providers who have patient approval, and providers only receive information pertinent to their area of medicine (which, in turn, is defined by municipalities). In the Netherlands, the National IT Institute for Healthcare (NICTIZ) uses the InterSystems Ensemble product to handle authentication and authorization of system users and logging health information transactions for auditing.

HIPAAT

HIPAAT's SOA provides a "consent engine" that allows providers to implement privacy policies within their existing EHR systems.[352] HIPAAT offers providers a computerized interface, Privacy eSuite, to create consent preferences on behalf of patients. Additionally, Privacy eSuite acts as a decision engine and adjudicates requests to access personal health information.[353] HIPAAT also offers a PHR or patient portal, myConsentMinder, that enables patients to input their own consent preferences.[354] myConsentMinder utilizes simple web-based consent forms that are similar to the HIPAA privacy notices typically filled out by patients in a provider's office.[355] The patient input system gives detailed instructions and provides many of the same features found on paper forms, such as check boxes and explanations for information sharing options.[356]

---

[348] Phone call with Michael LaRocca, *supra* note 344.
[349] *Id.*
[350] LaRocca, *supra* note 338, at 6.
[351] *Id.*
[352] HIPAAT. *Consent Management: Implementing Consumer Privacy Preferences in Health Information Exchange (HIE) Using Service-Oriented Architecture (SOA)*, March 2009. Available at: http://www.hipaat.com/external_com/wpaper0309.html.
[353] Callahan, K. *Written Testimony Before the HIT Policy Committee Privacy and Security Tiger Team*, June 29, 2010, at 1. Available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_913481_0_0_18/HIPAAT_Testimony.pdf.
[354] *Id.*
[355] Phone call with Terry Callahan, President, and Kelly Callahan, Vice-President, HIPAAT, March 24, 2010.
[356] *Id.*

HIPAAT implements privacy policies in three categories—consumer, organizational, and jurisdictional.[357] Thus, in addition to allowing patients to create consent directives, HIPAAT's software tools can allow administrators to create organizational privacy policies, such as "allow all providers to access all patients' PHI," as well as jurisdictional policies, for example "restrict disclosure of mental health records."[358] A critical component is that, in all of its applications so far, HIPAAT defaults to the policies of the organization and jurisdiction; consumer preferences can only be accommodated to the extent that they do not conflict.

Once privacy policies are recorded in the consent engine, consent preferences are translated into an access control policy language so that HIPAAT's Consent Validation Service can allow or deny access to the relevant information, or deny access but allow an override. Additionally, HIPAAT's technology can be configured to inform a provider that information has been filtered out of the record.[359]

HIPAAT's consent management system allows patients to restrict access based on any combination of the following: purpose of use, type of data, who is accessing the data (which can include an individual provider, a type of provider, a department or an entire facility) and date range.[360] In order to enable the actual segmentation of the data, however, HIPAAT depends on the EHR or PHR to provide data that is structured enough to implement the policy.[361] For example, if a system intends to give patients the option of excluding a particular provider from receiving information concerning a diagnosis of diabetes, HIPAAT needs data in the EHR to be structured in a way that provides an identifier for data associated with a diagnosis of diabetes.

HIPAAT works in a similar way as the InterSystems software in that it coordinates data sharing across different systems with certain criteria. As long as an EHR's data can be structured in a way that includes "information identifiers," HIPAAT's consent management operates across systems.[362] The system, however, does not segment data itself and relies on a compatible sharing network when sharing the data.

HIPAAT's capabilities will not be ready for full implementation until late 2011.[363] The company is currently in the testing phase for use in an HIO that includes a group of hospitals and providers. HIPAAT also participated with the VA in an interoperability test and was able to share consent policies with the VA.[364]

International Examples

International efforts to accommodate patient consent preferences through the use of data segmentation have faced challenges similar to those existing in the United States, including legal issues, incompatible local systems and a lack of common standards and terminologies. Approaches to addressing these issues have varied and this section presents a few illustrative

[357] *Id.*
[358] Callahan, *supra* note 353.
[359] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 277.
[360] *Id.* at 279.
[361] Phone call with Terry Callahan and Kelly Callahan, *supra* note 355.
[362] *Id.*
[363] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 57, at 321.
[364] *Id.* at 340.

examples of those efforts. For example, Sweden has taken a top-down approach by rewriting laws thought to hinder electronic exchange and creating mandates that require participation by county councils and the use of particular standards by hospitals.[365] Another approach has been taken in Canada, where a not-for-profit organization was created to work with regional authorities to create a privacy baseline for the exchange of health information and a conceptual privacy and security architecture that allows segmentation ("masking") of sensitive information.

Sweden

Sweden is in the process of designing and deploying the National Patient Summary (NPÖ)[366] to allow for the sharing of information across hospitals and practitioners throughout the country.[367] Particular challenges identified with regard to establishing the NPÖ included a lack of common terminology and information models, legislation that impeded the sharing of information across counties and a long tradition of local autonomy.[368] In Sweden, health care is a responsibility of each local county council, and the law originally barred counties from exchanging patient health information.[369] After the national legislative body changed the law, however, counties studied possible solutions for sharing information while protecting patient privacy.[370] Creators of the NPÖ decided that a full-scale national solution should be based on existing systems, which meant separating the information into volumes that were compatible with the existing technology.[371] Information volumes in the NPÖ now include patient demographics, symptoms, diagnosis, resolutions, medicines, care contacts, treatment documents, patient status, care planning, and examination results.

As described briefly above, Sweden hired InterSystems to implement HealthShare so that the NPÖ could transform data from many different local formats into a centralized format for each of the volumes within the index.[372] Although 100 percent of primary care services and between 80 and 90 percent of hospital care services in Sweden are digitized, the systems are not interoperable.[373] HealthShare is capable of translating between a variety of different medical vocabularies; however, the Swedish county governments, which have developed EHR systems within their hospitals, must develop translation map tables in order for HealthShare to convert the data for use in the centralized system.[374] The project is moving forward on an incremental

---

[365] Phone call with Michael LaRocca, *supra* note 344; S*ee also* Ministry of Health and Social Affairs. *Swedish Strategy for eHealth: 2008 Status Report*, 2008, at 13. Available at: http://www.regeringen.se/content/1/c6/11/48/73/bc8a2ecc.pdf.

[366] Elfgren, E.L. "Prevention progression," *Public Service Review: Science and Technology* 4, September 14, 2009. Available at: http://www.publicservice.co.uk/article.asp?publication=Science%20and%20Technology&id=397&content_name=Health%20technology&article=12698.

[367] "Summary Record Starts in Sweden," *eHealthEurope*, July 1, 2009. Available at: http://www.ehealtheurope.net/comment_and_analysis/481/summary_record_starts_in_sweden.

[368] Ståhl, I. "National Patient Summary: Development and Introduction," February 2, 2006, at 6. Available at: http://www.srdc.metu.edu.tr/stakeholders_group/public_docs/NationalPatientSummaryProjectInSweden.pdf.

[369] "Summary Record starts in Sweden," *supra* note 367; Datainspekitonen (Patient Data Act 2008) (Swed.).

[370] "Summary Record starts in Sweden," *supra* note 367.

[371] National Patientöversikt. "Focus on Delivery." Available at: http://www.xn--np-gka.nu/index.php?s=english.

[372] Intersystems Press Release. "Tieto and InterSystems Create Swedish National Electronic Health Record," June 3, 2009. Available at: http://www.intersystems.com/press/2009/sweden.html.

[373] Elfgren, *supra* note 366.

[374] Intersystems. "The Requirements of Health Information Exchange and how HealthShare Addresses Them." Available at: http://www.intersystems.com/healthshare/requirements-of-hie.html.

basis, linking one county to the system at a time.[375] To date, of the 21 Swedish counties, only Örebro and Östergötland have been linked to the exchange.[376]

Once the data has been standardized, the Swedish system will be able to control access based on patient / provider relationships and consent using a rules database attached to the index to regulate access to patient records. First, a provider will swipe a personal card to access the system. The rules database will filter clinical information based on the provider's role in the hospital and the information from each of the volumes that the county council has determined that doctor should be able to see. Next, the system will verify that the patient has consented for that doctor to obtain the information and whether that consent is still within the period of validity. Finally, the system will establish a "patient relation" between the doctor and the patient within the record for future requests.[377] The system is designed to segment data based on individual county determinations of who should be able to see each specific type of data in the record; individual patients do not have the ability to segment specific information by data element.[378]

Within the two Swedish counties currently participating in the NPÖ there are 300 active clinical users and more than 1,000,000 patients using the system.[379] The NPÖ planned to add three additional county councils during the first half of 2010, and all 21 counties by 2012.[380]

The United Kingdom

The United Kingdom's National Health Service (NHS) is in the process of rolling out a nationwide EHR that allows for a limited degree of data granularity and segmentation. The NHS Care Record Service (CRS) is built around the Summary Care Record (SCR), also referred to as the "spine," a centralized database that is structured to house patient demographic information, medication reactions, allergy information, information on chronic health conditions, test and x-ray results, and contextual information on the patient (*e.g.*, medically relevant home and work information).[381] Future functionalities are planned to include the ability to upload discharge summaries from in-patient and outpatient clinics, "out of hours" encounters, and information input by patients themselves via the NHS HealthSpace website, which currently only allows patients to view their SCR.[382]

Participation in the SCR is based on an opt-out with restrictions consent model.[383] In January 2009, the NHS, through ten Strategic Health Authorities, began sending out informational packets informing all citizens over the age of sixteen of the SCR and their options for

---

[375] National Patientöversikt, *supra* note 371.
[376] *Id. See also*: "Swedish National Patient Summary Gains Wide Acceptance," *HospitMedica International*, April 2010. Available at: http://mydigitalpublication.com/display_article.php?id=391323.
[377] National Patientöversikt, *supra* note 371.
[378] Elfgren, *supra* note 366.
[379] LaRocca, *supra* note 338, at 7.
[380] "Swedish National Patient Summary Gains Wide Acceptance," *supra* note 376.
[381] NHS. "Your Health Information, Confidentiality and the NHS Care Records Service," at 3-4, 7. Available at: http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/confidentiality.pdf.
[382] NHS. "Summary Care Record: Implied Consent and Permission to View," November 2, 2009, at 6-7. Available at: http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrcmodelptv.pdf.
[383] *See* Goldstein, *supra* note 15.

participation. In order to opt out of the system, patients (or their legal guardian) must return a form to their GP. If this form is not received within twelve weeks, the patient's GP may send the record to the central SCR database.[384] Once in the database, a given SCR may be accessed by any practitioner with a compliant SCR system and a clinical relationship with the patient. Within practices, access is mediated by role-based access control, which restricts some personnel from accessing the entire record (*e.g.*, non-clinical personnel may be restricted only to demographic information).[385] Further, at each clinical encounter, patients must give "permission to view" to the clinician before their record can be accessed (the patient also has the option of waiving this step by granting permission to view for all subsequent visits, or until permission is revoked).[386]

Beyond opting out and granting or denying permission to view one's SCR to individual practitioners, patients may also request that a clinician not input a given data element into their record. This request may be made for any data element except information relating to medications, allergies, or adverse drug reactions.[387] An additional functionality is planned that will allow patients to "seal" information in their record.[388] Sealed portions of the record will not be able to be accessed without express consent, but their existence is indicated within the SCR. An additional function, "seal and lock," will allow the patient to hide the presence of selected information entirely.[389] There is no timeline for implementation of this feature, however, and patients who currently wish to mask information relating to medications, allergies, or adverse drug reactions are advised to opt out of the SCR (as these data cannot be excluded from the record by patient request).[390]

Canada

Canada Health Infoway, Inc. (Infoway) is a not-for-profit organization working in collaboration with Canada's 14 provinces and territories to establish the framework and standards for an interoperable, nationwide EHR based on interconnected regional systems.[391] While differences exist in the provinces' privacy statutes, all individuals have the option of limiting the disclosure of their health information for treatment through "lockbox" provisions. These provisions vary by province and territory, affording individuals the option of restricting disclosure of some or all of their electronic health information, depending on the jurisdiction.[392] The Pan-Canadian Health Information Privacy and Confidentiality Framework grew out of an attempt to harmonize the various privacy provisions and serves as a baseline for provincial consent rules.[393] Among other provisions, the framework states that the individual has the right to withdraw consent to share information; however, that withdrawal of consent can be overridden in an emergency. A provider sharing segmented information must inform the recipient that masked information exists.[394]

---

[384] NHS, *supra* note 382, at 6.
[385] Pritts, J. and K. Connor. "The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands (the ability to mask or limit access to health data)." Prepared for: *Substance Abuse and Mental Health Services Administration, HHS*, February 16, 2007, at 34.
[386] NHS, *supra* note 382, at 11.
[387] *Id.* at 9.
[388] NHS, *supra* note 381.
[389] *Id.* at 16.
[390] NHS, *supra* note 382, at 9.
[391] Pritts, *supra* note 385, at 14.
[392] *Id.* at 17.
[393] *Id.*
[394] *Id.* at 18.

Furthermore, it is incumbent upon the health provider to notify the patient of any consequences of withholding certain data.[395]

Infoway has also developed a conceptual privacy and security architecture for use in building EHRs across Canada that incorporates the framework provisions described above. In particular, the architecture includes the ability to mask health data at the data element level; to mask health data from specific providers; to override masking; and to create repositories storing patient consent directives.[396] This conceptual architecture is designed to be flexible enough to enable different jurisdictions to implement privacy and consent features consistent with their local requirements, including masking or segmentation features. To date, masking functions are being used in several e-health projects in Canada.[397] For example, British Columbia's PharmaNet e-health project allows patients to limit access to information by asking the pharmacist to attach a keyword to the file. In this way, only pharmacists with whom the patient shares the keyword will have access to the file. An emergency override is available, however, if considered necessary for treatment.[398]

The Netherlands

The Dutch National Healthcare Information Hub (LSP) is built around remote information hubs connected to a national database. The system maintains records at the practitioner or regional level that are available through a searchable database accessible to eligible practitioners throughout the country (*i.e.*, those who meet a set of minimum security and functionality requirements).[399] While consent to share medical information is implied for treatment purposes, patients have the option of segmenting data based on provider, care delivery setting, and data type, and may also opt out of the exchange entirely.[400]

The Stichting RijnmondNet (RijnmondNet) pilot project in the Netherlands is an electronic exchange serving hospitals, clinicians and patients in an area of the Netherlands near Rotterdam.[401] As mentioned above, the project utilizes the open source system developed by Tolven, Inc. to enable patient control over the electronic sharing of personal health information.[402] In keeping with Dutch law, RijnmondNet is patient-focused, enabling the patient to control the distribution of his / her personal health information with considerable granularity.[403] For example, a patient can control access to particular sections of personal health information and can grant or deny access to either individuals or to groups.[404] The system accomplishes this goal by making and distributing encrypted copies of the information on the

---

[395] *Id.*
[396] *Id.*
[397] *Id.*
[398] British Columbia Ministry of Health Services. *Frequently Asked Questions about eHealth and Disclosure Directives*, at 3. Available at: http://www.health.gov.bc.ca/ehealth/pdf/dd_faq.pdf.
[399] Pritts, *supra* note 385, at 3.
[400] *Id.* at 42-45.
[401] Jones, T. "Leveraging Open Source Software to Assure Privacy of Health Information," *OSCON Open Source Convention*, July 21, 2010.
[402] Health Record Banking Alliance, *supra* note 243.
[403] Jones, *supra* note 244.
[404] *Id.*

basis of the patient's preferences and at the patient's request, rather than controlling access by denying or granting particular users the ability to view information in the health record. In the RijnmondNet pilot, a patient first must opt in to participate in the exchange, providing consent for his / her records to be transferred from the clinical environment to a secure aggregation area. Although patient records are transferred in one format only, Tolven's technology is capable of receiving documents in the aggregation area in any format.[405] The aggregation area is a secure environment where neither patients nor clinicians are able to view or access documents. Documents coming into the aggregation area are organized by patient and are processed by Tolven's rules engine, which applies syntax-based rules to create semantically interoperable and computable documents that can support granular segmentation of the patient's health record.[406]

In addition to accommodating Dutch law requiring consent for the exchange of a patient's health records, Tolven's implementation for the RijnmondNet exchange must accommodate complex Dutch laws regarding the health records of minors. In the Netherlands there is a gradation of parental access to minors' electronic health records on the basis of the minor's age.[407] As a minor ages and is granted expanded control over his / her health record, and as parental rights diminish, Tolven's system automatically computes and enforces the necessary changes in access.

Segmentation in Contexts Other than Health Care

Use of data segmentation in industries and contexts other than health care provides an opportunity for comparison with its use in the health care sector. Moreover, analysis of its uses in other industries provides data on how the public views privacy and the amount of control people generally desire over their personal information in other areas of their lives. Industries other than health care must also balance consumer privacy rights with beneficial reasons for collecting their personal information—many of which stem from consumers' own desires. Facebook and TiVo in particular have implemented data segmentation methods that offer various granular options for consumers.

Industries other than health care also provide examples of the various barriers (both perceived and actual) the health care industry faces when implementing data segmentation. For example, the extent of granular control over personal data in other industries has seemingly fluctuated along with consumer demand. As described in more detail below, Facebook recently implemented the option of using simplistic controls over the sharing of data after a short period of time when the platform essentially offered only very detailed individual control (or none).

Facebook

The evolution of Facebook's privacy policies and practices provides a useful case study of the complexity of meeting consumer privacy demands in the context of granular data segmentation. Facebook, a social networking site, requires consumers to create a "profile" and connect with people identified as "friends." Information is entered into the application from the outset into established data type fields, such as "Name," "Hometown," "E-mail," "Hobbies," "Political Views," *etc*. Members can also add photographs individually or divided into albums. The

[405] Jones, *supra* note 247, at 1.
[406] *Id.*
[407] Wet op de Geneeskundige Behandelingsovereenkomst (Dutch Medical Contract Act 1995) (NETH.).

platform is built on the idea of transparency and sharing of an individual's information, which has occasionally sparked public controversy[408] in response to the company's request for progressively more user information.[409]

In response to user criticism that its privacy policy allowed too much unwanted sharing, Facebook changed the policy in December 2009 to allow users to indicate who could have access to the information within each data set, as well as each photo or album. The company sent a message to all users upon login that alerted them to the change, encouraged them to review / update their privacy preferences, and provided them with a link for doing so. The default settings, however, allowed all internet users to view members' general profile information, including picture, gender and age—thereby allowing users' information to be more exposed rather than less.[410] Status updates, photos, and other information were defaulted to the "friends of friends" setting.[411] Additionally, profile pictures, names, gender, current city, networks, and lists of friends were permanently public information, with no option for consumers to opt out.[412] As a result, third party "facebook-enhanced" applications could access this information regardless of user-chosen privacy settings.

The December 2009 privacy policy was criticized for being too complicated and not providing its members adequate instruction on how to use the available privacy tools. In response, the company quickly launched a "privacy guide" that can be accessed on the Facebook homepage or from a person's profile.[413] The guide is intended to explain the privacy policy and basic terms and walk users step-by-step through setting up preferences. The onus is still on the user, however, to seek out the guide in order to implement stricter controls than Facebook's default sharing policy.

The company also issued a revised policy in May 2010 that offers simplistic controls in addition to offering the same detailed level of granularity. Users can now determine how much basic information is shared with the exception of name, profile picture, gender and networks, which are still permanently public information.[414] Specifically, users can grant access to other users of Facebook that they have organized into broad categories of people (*e.g.*, "friends" or "friends of friends") by selecting the particular category or can customize their sharing on an individual level by granting a specific individual user access, which allows them to decide exactly who can view which pieces of information. The May 2010 policy also allows users to choose whether to share their information with applications or websites.[415] In line with the company's philosophy

---

[408] Kirkpatrick, D. *The Facebook Effect: The Inside Story of the Company that is Connecting the World* (New York: Simon and Schuster, 2010), at 207.
[409] Helft, M. and J. Wortham. "Facebook Bows to Pressure Over Privacy," *The New York Times*, May 26, 2010. Available at: http://www.nytimes.com/2010/05/27/technology/27facebook.html.
[410] Kirkpatrick, *supra* note 408, at 209.
[411] Bankston, K. "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly." *Electronic Frontier Foundation: Deeplinks blog*, December 9, 2009. Available at: http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.
[412] Facebook Help Page. *Update to Privacy Settings*. Available at: http://www.facebook.com/help/?page=927.
[413] Facebook Privacy Page. *Controlling How you Share*. Available at: http://www.facebook.com/privacy/explanation.php.
[414] Zuckerberg, M. "Making Control Simple," *The Facebook Blog*, May 26, 2010. Available at: http://blog.facebook.com/blog.php?post=391922327130.
[415] *Id.*

that encourages information sharing, the default setting recommends that users share information in all of the broad categories Facebook offers, including the availability of members' profile information, status updates, and photos, to all internet users. The default policy would also allow the "friends of friends" category to view members' birthdays, religious and political views, and photos and videos that a member has been "tagged" in (*i.e.*, identified by another member). The "friends only" category would be able to view this information, in addition to members' email addresses, phone numbers and address.

Facebook provides an example of an electronic platform that allows users to exercise highly granular control over personal information. The program, however, requires users to enter data into strictly-defined categories, thereby avoiding the problem of separating commingled data. In addition, Facebook's categories apply across all profiles and users of the program. Within health care, however, different organizations utilize different EHRs, which do not consistently define categories of data or use the same technical interfaces. Just as a Facebook privacy setting could not apply to information shared on Twitter (a social networking program with similar uses but completely different data categories), different EHRs and PHRs categorize medical information in different ways. As a result, a Facebook-style privacy policy could only work within health care if all EHRs and PHRs adopted consistently-defined categories of information in addition to the same technical interface.

Facebook's experience also illustrates the issues raised by providing a great degree of user control over granularity in data types without instruction—the company's new privacy guide is an acknowledgment of this gap. As noted recently by the Tiger Team, the ability of individuals to exercise this capability remains unclear.[416] HIOs could face similar concerns when implementing a privacy policy that allows consumers to express preferences with regard to segmenting data (or to segment the data themselves) within, for example, PHR or PCHR models. They will need to ensure that patients are aware of default settings up front and are given clear instructions on what options are available and how to make changes. As the scope of an electronic exchange grows, entities will need to evaluate privacy policies on a continual basis to ensure that they align with and enable the breadth of sharing made available by the exchange. Consumers will also need a user-friendly system to be able to select which data should be shared with which users.

Finally, as also noted by the Tiger Team, the most notable difference between Facebook's data segmentation design and those under development in the health care sector is that Facebook users maintain unilateral access and control over their own data. Personal information within the health care sector, however, is (and likely will always be to some extent) generated and stored by a variety of entities in addition to the individual.[417]

TiVo

TiVo, Inc. (TiVo), which produces digital video recording (DVR) devices and provides related services connecting consumers to digital media, uses data segmentation to extract information about its customers' viewing habits. TiVo places protections on "personally identifiable viewing information," which refers to information about a customer's viewing habits that can be used to

[416] Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25, at 15.
[417] *Id.*

identify the customer.[418] Unless a customer gives prior consent, TiVo does not collect or access the personally identifiable viewing information of that customer except as necessary for servicing.[419] According to its privacy policy, TiVo does use its recording devices to gather anonymous data about a customer's viewing habits, which includes the customer's viewing choices, but does not identify the customer's household or include any demographic or personal information.[420] Customers can, however, elect to block TiVo from collecting anonymous viewing information.[421]

TiVo "boxes" connect to large servers and have the capability both to receive and send information.[422] The company gives customers three options for information sharing via a TiVo box. The default option is considered "opt neutral" which allows the collection of viewing information but separates the information from an account and detaches it from the specific TiVo box. Viewers can opt out of sharing even this information by selecting an option through the box's software. Finally, viewers can opt in to sharing their viewing information as tied to their personal account information.[423]

TiVo has an elaborate method of segmenting the data for the "opt-neutral" option. If a viewer does not specifically opt in, viewing information received by TiVo servers is automatically separated from any information that could be used to match it to individual receivers or subscribers. Account information and anonymous viewing data are stored in separate systems.[424] Viewing data is then randomly transferred to one of a number of different servers for storage. File transfer logs are turned off and timestamps are erased from the data every three hours. These measures were implemented to enable the use of anonymous viewing data for customers who do not opt in specifically to sharing their viewing information.[425]

TiVo provides an example of a company's ability to separate data at the consumer's direction for purposes of limiting identifiability. When information is first transferred from a TiVo box to a server, it is identifiable and can be associated with a specific household. TiVo's hardware / software combination then removes the identifiable information in accordance with the default option or the preference expressed by the TiVo subscriber. Notably, TiVo's system separates very specific data from every TiVo box as opposed to enabling a granular set of choices. That is, TiVo itself establishes the criteria for segmentation and does not adjust those criteria according to the preference of the consumer. As previously discussed, within health care, patients may want to segment different data depending on their personal circumstances and the entities with which they are sharing their health information. In addition, since TiVo customers purchase their DVR boxes from the company, the information being transmitted by each individual box uses the same format and terminology. In the health care industry, different EHRs use different data formats

---

[418] TiVo. *TiVo Privacy Policy*, January 2010. Available at: http://www.tivo.com/abouttivo/policies/tivoprivacypolicy.html.
[419] *Id.*
[420] *Id.*
[421] *Id.*
[422] Spangler, W.E. et al. "Exploring the Privacy Implications of Addressable Advertising and Viewer Profiling." *Communications of the ACM*, Vol. 49, No. 5, May 2006, pp. 119-123, at 121.
[423] TiVo, *supra* note 418.
[424] Spangler, *surpa* note 422.
[425] *Id.*

and terminologies, creating an additional barrier to implementing similar data segmentation methods.

Web Spiders

The term "web spiders" refers broadly to programs developed to search websites and retrieve web documents from the internet, either by following hypertext links or other methods.[426] Web spiders are used in various applications for the purpose of personal searching (finding web documents of interest to an individual user), as well as for building collections of web pages, archiving particular websites or providing statistics.[427] The web analysis conducted by spiders can include content-based analysis, which examines the body of the text to determine its relevance, or link-based approaches.[428]

Search engines, such as Google, Yahoo, and Bing index web content to make it searchable by sending web spiders around the internet to copy information from websites and update the index. Web designers can prevent spiders from copying information from their website in two standard ways. The first method, known as the Robots Exclusion Protocol, involves creating a "robots.txt" file in the website's root directory.[429] This file contains rules that explain which sections of the website are open for indexing and which parts of the website are off limits. Web designers have highly granular options in creating a "robots.txt" file. First, the designer can limit access to areas by specific spider-type ("who"). Also, designers can limit what content from the website each spider can access ("what"). Finally, for major spiders, the designer can place a time limit between successive requests on the server ("how"). Additionally, there is a proposed new standard under development that would allow designers to limit spider access by time of day and rate of request ("when").[430]

The second standard method of blocking web spider access is typically referred to as the Robots META tag. This method differs from robots.txt in that it does not require access to the web server and can enable even more fine-grained control over access to individual pages of a website.[431] It should be noted, however, that these standards are not strictly enforced and rely on voluntary compliance by web spiders.[432] Also, neither the Robots Exclusion Protocol nor the use Robots META tags allows an author to express preferences as to how the data should be indexed or used once it is made available to the search engine via the web spider. Some analysts argue that search engines should adapt to a new standard that would allow web developers to pass on tagging information that expresses who recorded the web content and with what devices, and what the author is comfortable having others do with it.[433] The benefit of such a protocol would

---

[426] Chau, M. and H. Chen. "Personalized and Focused Web Spiders," in *Web Intelligence*, N. Zhong et al., eds. (New York: Springer-Verlag, February 2003), pp. 197-217, at 197.
[427] *Id.* at 199.
[428] *Id.*
[429] *Id.* at 198.
[430] Yang, C. and H-J. Liao, "Using the Robots.txt and Robots Meta Tags to Implement Online Copyright and a Related Amendment," *Library Hi Tech*, Vol. 28, No. 1, 2010, pp. 94-106, at 103.
[431] Chau, *supra* note 426, at 198.
[432] *Id.*
[433] *See, e.g.,* The proposed Automated Content Access Protocol (ACAP). Paul, R. "A Skeptical Look at the Automated Content Access Protocol," *ars technica*, January 13, 2008. Available at: http://arstechnica.com/business/news/2008/01/skeptical-look-at-acap.ars.

be to allow those who place information on the web the opportunity to keep track of who is using their information and for what purposes, while allowing those accessing information to know when they must ask the original author for permission before re-using the information.

This debate is relevant to data segmentation in health care in that it shows how web designers can allow access to some information while limiting access to other information. Web spiders act as information requesters to all web sites on the World Wide Web—they pull information from each web site for indexing. Robots.txt and Robots META tags provide examples of the technological capability to communicate what information should be pulled and what should not.

As the internet has grown and content has become more dynamic, web spiders have evolved into intelligent, adaptive tools that are being used to perform complex tasks for a variety of purposes.[434] For example, sophisticated Dark Web-focused spiders are being used in counter-terrorism efforts to explore forums and other websites in the hidden web to seek and acquire very specific content.[435] These intelligent spiders not only use special means of searching through multimedia files and attachments, but also are capable of identifying and retrieving content based on the sentiment and affect of the resource.[436]

Additionally, web spiders have evolved to work within the semantic web, where web content is being linked through the use of metadata—machine-readable data that describes other data and enables a standardized way of annotating information.[437] One commonly used type of metadata is the Resource Description Framework (RDF), which uses "triples" to indicate subject, property and object with respect to data. Specially designed web spiders called "scutters" have been developed in order to search RDF files. By attaching metadata to web content through the use of RDF, computers are able to interpret web content or web documents in a more useful way. Additionally, RDF enables compatibility with many vocabularies—it is not necessary for applications to know in advance which vocabulary will be encountered in order for inferences to be made.[438] Some experts have identified potential benefits of using RDF tags in EHRs due to the interoperability of RDF tags and their ability to describe more complex relationships and concepts, as well as enable more intelligent, relevant searching.[439]

RECOMMENDATIONS AND CONCLUSIONS

As the quality and quantity of health information expands through the use of EHRs and other technology platforms, and as electronic exchange vehicles facilitate the free flow of that information, our current strategies (technical, legal and otherwise) for protecting personal health information struggle to keep pace. Data segmentation has been identified as a promising approach that can be employed to help allay concerns about health information privacy and to

[434] Chau, *supra* note 426, at 211-12.
[435] Chen, H. "Discovery of Improvised Explosive Device Content in the Dark Web," *Intelligence and Security Informatics*, June 2008, pp. 88-93, at 88.
[436] *Id.* at 93.
[437] Paolillo, J.C. and E. Wright. "Social Network Analysis on the Semantic Web: Techniques and Challenges for Visualizing FOAF," in *Visualizing the Semantic Web*, Geroimenko, V. and C. Chen, eds. (London: Springer, 2003), pp. 229-42, at 239.
[438] *Id.* at 230-32.
[439] Phone call with Dr. Ben Adida, *supra* note 75.

foster greater consumer involvement. As we have discussed, segmentation has value in many other contexts as well; it can provide a mechanism for increasing consumer protections, insulate against the harms of hindsight or outcome bias, and enhance the utility of medical records for research, quality improvement, and other public health advances.

We should continue to develop policies, methods and technologies that support segmentation of health information for at least three basic reasons: (1) our current legal environment requires the protection of certain types of personal health information more than others; (2) enabling granular patient control over the use and disclosure of their health information honors fundamental principles of patient autonomy and builds patient trust and participation in the health care system; and (3) failure to make advances in this capacity could hamper the quantity and quality of information available to support a more rapid learning cycle in health care.

Recognition of its potential and many benefits, however, does not eliminate the complexities and challenges surrounding data segmentation. As we have described, electronic exchange supporting some level of data segmentation has succeeded to varying degrees, although the solutions developed up to this point frequently are in preliminary stages and tend to enable segmentation only in contained environments. Moreover, issues ranging from how data are structured and coded, to the level of sensitivity assigned to certain information (and who defines it), challenge our ability to maintain forward momentum and commitment to the endeavor.

Articulated below are some observations that could help decision makers explore possible policy, technology and other means of enabling granular patient control of their health information through segmentation.

Build a Bridge to Greater Autonomy

Institutional stewards of patient information tend to rely primarily on federal and state definitions of what constitutes sensitive information, which in turn are mostly based in law. Given that these laws often vary among states, organizations working to provide technology solutions to support segmentation often must develop highly-customized products and services. This process is neither efficient for the data stewards involved nor for the vendors attempting to serve their client base. Further, this system is entirely opaque to the individual patient. From a consumer perspective, no proactive, subjective, or individual context considerations factor into the determination of what constitutes sensitive information.

In addressing the limitations of this system, one potential approach would be to establish – through legal or other means – a definition of sensitive data that could attempt to weigh the interests and concerns of various stakeholders as well as reflect the environment in which information exchange now occurs. However appealing this goal may be, though, its potential drawbacks warrant consideration. Changing law in response to technology and / or societal developments can be a very slow process and can yield inflexible results. This last issue is particularly important given the challenge of predicting how the electronic exchange environment is going to evolve—even in the near term. Finally, this approach fails to prioritize individual choice with respect to health information management.

Perhaps a more flexible and forward-looking option would be to stipulate via some method of policy implementation[440] that people's preferences regarding information sharing should be accommodated, and that the health care sector should strive to achieve this capacity within a specified period of time. Recognizing that this vision likely would take years to achieve, this solution represents a move beyond simple default to state and federal legal requirements and would require data stewards to engage in direct dialogue with the patient and consumer communities they serve.

This second option would move us closer to the goal of supporting individual, subjective preferences and, though we are not yet able to fully operationalize this goal, could provide an important stepping stone in that direction. Given the hurdles that this transition would pose to many stakeholders in the health care arena, the idea also would necessitate the provision of significant support to help overcome the challenges associated with achieving granular and individualized data segmentation.

Provide Direct Financial and Other Support to Stimulate Change

While it is likely that many of the provisions in HITECH related to meaningful use will stimulate broader use of EHR technologies and result in the generation of more structured data, additional mechanisms specifically intended to encourage the development of segmentation-enabling processes and technologies should be considered. Some of these methods might be more technical in nature, whereas others might help to mitigate provider workflow concerns or address gaps in flagging / tagging standards, for example. In short, if progress on this front is a policy priority, then commensurate support should be provided to aid its development.

For example, while a handful of technical solutions support granular choice, all currently have limitations. Several of these approaches are evolving, however, and should be encouraged to expand, both in terms of their functionality and in the number and type of exchange they serve. As such, the provision of incentives for developers to test ways to better accommodate patient choice in a variety of exchange models and contexts should be considered. Policy makers should seek ways to encourage such development and testing in applied environments, perhaps through the establishment of pilot projects or, though already under way, as part of future Beacon Community enhancements.

Generate Evidence

As referenced above, we are currently straddling two information-sharing paradigms in the health care sector: one that is primarily paper based, with a corresponding set of policies and processes, and another that is facilitated by technical advances that allow the sharing of information more freely between a greater number and more diverse set of stakeholders. As we move through this transition, decision makers could be tempted to rely on evidence from prior experience in the paper environment to support the development of future policies. Given the significance of this transformation, however, we suggest an alternative approach: each of the challenges described in this paper represents an opportunity to establish updated research priorities—the results of which could point to possible policy solutions or best practices.

[440] *See* Goldstein, *supra* note 15.

One key area that would benefit significantly from additional research relates to the means by which patients are educated about and informed of their information management options. Specifically, as the landscape of information, applications, and tools available to consumers rapidly evolves, it would be worthwhile to explore the most effective mechanisms for facilitating patient decision making regarding segmentation. Further research on who, if anyone, should assume the role of helping patients in this regard is needed. This analysis would include evaluations of whether, and if so what type, of health care providers are best suited to the task of assisting patients in making these decisions, and via what mechanisms. The goal of this research would be to identify promising approaches to supporting consumers in their determination of how to establish their health information sharing preferences.

These ideas represent only a few of the possible options available to policy makers in advancing our capacity for granular segmentation of health information. We support the Tiger Team's recent recommendation to cast a wide net in searching for appropriate means to provide patients more granular control over the exchange and use of their identifiable health information,[441] and point to the efforts underway in other countries as evidence that this is a worthwhile endeavor. While still a challenge, data segmentation indeed holds promise for accomplishing the ultimate goal of accommodating the needs and desires of the multiple stakeholders engaged in the electronic exchange of health information.

[441] *See* Health IT Policy Committee, Privacy and Security Tiger Team, *supra* note 25, at 15.