CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS

March 23, 2010

Prepared for:

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Planning
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by:

Melissa M. Goldstein, JD
Associate Research 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:

Penelope P. Hughes, JD
Julie K. Lappas, JD
Scott A. Weinstein
Benjamin Williams

TABLE OF CONTENTS

CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS

EXECUTIVE SUMMARY

The issue of whether, to what extent, and how individuals should have the ability to exercise control over their health information represents one of the foremost policy challenges related to the electronic exchange of health information. The current landscape of possible consent models is varied, and the factors involved in choosing among them are complex. States and other entities engaged in facilitating the exchange of electronic health information are struggling with a host of challenges, chief among them the establishment of policies and procedures for patient participation in their exchange efforts. While some have adopted policies enabling patients to exercise individual choice, others have prioritized the needs and concerns of other key stakeholders, such as providers and payers. The purpose of this paper is to discuss in detail the issues, nuanced considerations, and possible tradeoffs associated with the various consent options to help facilitate informed decision making.

Core consent options (abbreviated) for electronic exchange include the following:

- *No consent*. Health information of patients is automatically included—patients cannot opt out;
- *Opt-out*. Default is for health information of patients to be included automatically, but the patient can opt out completely;
- *Opt-out with exceptions*. Default is for health information of patients to be included, but the patient can opt out completely or allow only select data to be included;
- *Opt-in*. Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out; and
- *Opt-in with restrictions*. Default is that no patient health information is made available, but the patient may allow a subset of select data to be included.

As these definitions illustrate, a range of consent models can be applied in different contexts of electronic exchange in the U.S., and it is possible for there to be further permutations depending on the level of choice granularity allowed. There is also considerable variation in the type of information exchanged, ranging from the more basic (*e.g.*, lab results) to the more mature and complex (*e.g.*, a wide array of health information).

The consent model selected for electronic exchange, as well as the determination of which types of health information to exchange, affects many stakeholders (*e.g.*, patients, providers, and payers). These decisions also have consequences for national policy goals, such as improving the quality of healthcare, promoting public health, engaging patients in their health care, and ensuring the privacy and security of personal health information. This discussion requires not only an appreciation of the sometimes competing interests of various stakeholders, but also consideration of the interests of the individual relative to those of society as a whole.

Provider and patient participation in electronic exchange have been identified as key challenges—both patient and provider participation are desired to facilitate better care delivery and advance other societal goals (*e.g.*, improved public health), as well as to ensure the viability and utility of the exchange. To enhance patient participation, numerous electronic exchanges have employed one or more of the following tactics:

- Active engagement of patients in the development of the exchange entity;
- Vigorous marketing of exchange efforts through effective channels;
- Initial and ongoing education (largely from providers) about the effort; and
- Adoption of an *opt-out* or *no-consent* model, in concert with tight restrictions on data access and / or use, including stringent penalties for misuse.

In addition, these electronic exchanges have employed the following methods of ensuring adequate provider participation:

- Minimization of administrative burdens, sometimes coupled with financial or other incentives;
- Maximization of value (*i.e.*, access to as much useful information as possible, as often as is needed); and
- Provision of key infrastructure and service components (*e.g.*, a record locator service or consent management tool).

Other issues of particular significance with regard to progress (or lack thereof) toward the greater proliferation of electronic exchange include:

- Numerous and sometimes inconsistent federal and state laws regarding patient consent generally, and disclosure of sensitive information specifically;
- Provider workflow challenges associated with obtaining and managing consent;
- The lack of (or difficulty in achieving) technical and procedural capacity to segment and manage data in the manners desired by various constituents;
- The concern that existing security and privacy provisions are inadequate; and
- The need to balance multiple and often conflicting stakeholder interests to ensure adequate participation.

At present, the evidence from emerging electronic exchanges is insufficient to determine the consequences associated with policy decisions that allow for greater or lesser levels of patient choice with regard to the electronic exchange of their data. There are early signs that consent models at both ends of the spectrum can generate sufficient patient and provider participation to achieve the critical mass necessary for system function and the realization of key goals. However, in any consent model the role of other factors, such as the accompanying level of dedicated human and financial resources, policy development, and other necessary supports, must also be considered. Due to the complexity of issues involved in selecting and applying a particular consent model, appropriate guidance in the form of higher-level principles or recommendations is critical to moving forward. While this document represents a starting point for discussion related to consent, it is imperative that future deliberations are informed by further research regarding the effectiveness and impact of various consent options, consideration of the

broader policy landscape, and assessment of the needs of those most affected by the consent decision. Until the time when we are confident that we can protect health information in a systematic and thorough way, prudent use of the mechanism of consent appears to be one of the most reliable ways to pursue that goal.

CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS

INTRODUCTION

Background and Rationale

The Health Information Technology for Economic and Clinical Health (HITECH) Act (Division A, Title XIII of the American Recovery and Reinvestment Act (ARRA))[1] directs the Office of the National Coordinator for Health Information Technology (ONC) to oversee the development of a health information technology (HIT) infrastructure that "improves health care quality, reduces medical errors, reduces health disparities, and advances the delivery of patient-centered medical care."[2] This charge sets a course for the U.S. health care system to transform the way it operates fundamentally by leveraging twenty-first century technologies. It is widely recognized that this is no small task—in part because legal, technical, cultural, economic and policy considerations must be addressed before HIT can be fully leveraged to achieve anticipated quality and efficiency gains.

One immediate challenge for policy makers is the daunting task of urging health care providers to adopt and demonstrate "meaningful use"[3] of HIT systems. It is for this reason that incentives for the acquisition and use of such technologies were built into the HITECH Act.[4] However, technology acquisition is clearly not the ultimate goal. It is widely believed that the vision of better patient care will not be achieved unless these systems are used to support the delivery of patient-centered care, which requires that relevant information about patients can be accessed and used whenever, wherever, and by whomever it is needed. This vision calls for true data liquidity and means that information exchange must overcome entrenched institutional, legal, cultural, and business boundaries as well as some technical obstacles.

It is also widely acknowledged that, if we are to reap the benefits of information exchange, patients must be assured that appropriate technology solutions, business practices, and policy protections will be employed to prevent their information from being used in undesirable ways or to generally impinge upon their rights and civil liberties. As communicated in a recent message from Dr. David Blumenthal, National Coordinator for Health Information Technology, "*We must have comprehensive, clear, and sustainable policies that strengthen existing protections, fill gaps as they emerge, fortify new opportunities for patients' access to and control of their information, and align with evolving technologies*." [5]

---

[1] American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, §§ 13101-13424, 123 Stat. 115, 228-279 (2009).
[2] § 13101, 123 Stat. at 230 (codified at 42 U.S.C.A. 300jj-11 (West 2009)).
[3] § 4101(a), 123 Stat. at 467-477 (codified at 42 U.S.C.A. § 1395w-4 (West 2009)).
[4] §§ 4101-4201, 123 Stat. at 467-494.
[5] Blumenthal, D. "Coordinator's Corner: Updates from Dr. Blumenthal," November 12, 2009. Available at: http://www.healthit.hhs.gov/portal/server.pt?open=512&objID=1406&parentname=CommunityPage&parentid=0&mode=2&in_hi_userid=10741&cached=true.

To accomplish the goals envisioned by Congress, and fully leverage the benefits of an HIT-enabled health care system, we face several fundamental policy challenges. This whitepaper presents a discussion of the issues associated with whether, and if so how, to obtain individual consent[6] for the purposes of electronic health information exchange. Years of policy deliberations at the state and federal level have proven that this is a difficult issue to resolve—in part because of economic, technical, cultural, and legal considerations, but also because the various stakeholders involved disagree, often strenuously, on the best approach. Determining when and how an individual's consent should be obtained for electronic health information exchange is a complicated policy decision that requires consideration of a number of complex issues and a determination of how to balance the needs of the participants in the exchange along with desired societal outcomes.

The Existing Electronic Health Information Exchange Landscape

Broadly speaking, the goal of electronic health information exchange (from here on simply referred to as electronic exchange) is to facilitate the sharing and use of health-related information in order to enable safe, timely, efficient, effective, equitable, and patient-centered care. At present, most electronic exchange efforts focus primarily on use of information for clinical care purposes. This focus partly reflects the immediate and high-priority goal of improving patient care through wide availability of relevant clinical information. It also is likely a function of the fact that, as discussed later in this paper, the privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and many state laws allow for the exchange of most health information for specified purposes (treatment foremost among them) without patient[7] consent. However, organizations that engage in electronic exchange do not always exercise this option—even when the states' legal framework would permit the exchange of clinical information for treatment purposes without first obtaining patient consent. This practice is largely due to an acknowledgement that, in order to achieve any level of systemic durability and success, electronic exchange efforts must establish trust relationships with all participants, including patients.

At present, a number of technical, legal, policy, cultural, and business challenges are impeding progress toward these goals. Despite – or perhaps because of – these challenges, numerous and often differing examples of electronic exchange are evident across the country. The level of complexity associated with electronic exchange can vary depending on a host of factors, including but not limited to: 1) the number of parties involved in electronic exchange and their relationships with one another; 2) the purposes for which the information is being exchanged; 3)

[6] 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. The HIPAA Privacy Rule (discussed later in this paper) requires an "authorization" for uses and disclosures of protected health information that are not otherwise permitted or required. An "authorization" is a detailed written document defined by the Rule that gives covered entities permission to use or disclose protected health information (PHI) for specified purposes. We use the term "authorization" in this paper when referring to the requirements of the Privacy Rule or other specific laws (*e.g.*, the New York Public Health Law, Rhode Island Health Information Exchange Act of 2008).

[7] 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 or 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."

the nature of the information being exchanged and the existence of technical standards to support its exchange; 4) the maturity of the exchange system; and (5) the rules and policies applied to the organizations involved and information being exchanged. For these and other reasons, some electronic exchange efforts can be characterized as more basic (*e.g.*, very limited data are electronically exchanged between few entities in a small geographic region) or more sophisticated (*e.g.*, many types of data are electronically exchanged between multiple providers in more than one state).

The U.S. electronic exchange landscape also reflects great diversity in the governance and architectural models applied. Some electronic exchange efforts lack a formal, centralized governance structure – preferring instead to distribute responsibilities among participating organizations without designating a central authority. Others establish formal public-private collaboratives that direct and coordinate efforts for one or more electronic exchanges. The former tend to be associated with smaller-scale efforts, and the latter with larger and more complicated structures, such as those undertaken at the state level.

Toward the more "basic" end of the spectrum are exchange efforts that leverage their existing relationships to send or "push" information from one point to another, often adding new technology components (*e.g.*, Electronic Health Records (EHRs)) to do so. Generally speaking, this "push" approach makes electronic exchange (versus paper) the dominant model of point-to-point information sharing from one provider or other partnering entity to another (*i.e.*, Dr. Smith sends clinical data on patient Sue electronically (versus via fax) to Dr. Jones). At present, these point-to-point approaches to electronic exchange are more common, as they typically can facilitate early exchange efforts without significant infrastructure investment and the key elements are more readily available and culturally more similar to the current information flow paradigm. It has also been suggested that perhaps even the policy considerations involved in these types of electronic exchange might be less complicated to implement than alternative methods.

On the other end of the spectrum is the "pull" approach to electronic exchange (which is typically associated with larger, networked, and more structured exchange efforts, such as those undertaken at the state level). These often involve the creation of a shared architecture and supporting services that enable a more sophisticated capacity to search for and extract - or "pull" - electronic data from one or more networked sources using a query system, and may or may not require the presence of an existing relationship between the requesting entity and the data holder.

Regardless of where a particular electronic exchange effort falls on the governance and / or architecture spectrum, certain key functions need to be undertaken by participating organizations. These include the establishment of a policy framework, development and management of contractual conventions and terms, determination of the means of exchange and data to be exchanged, and development and maintenance of exchange standards. Typically, the participating organizations reflect some combination of providers, payers, and health agencies.

While many entities engaging in "push" versions of electronic exchange are able to share responsibility for these functions across the participating organizations, larger and / or more sophisticated efforts tend to require the establishment of an external, coordinating entity. The

entities most commonly associated with this function are Health Information Organizations (HIOs),[8] which have emerged as technical, governance, and oversight structures that facilitate the exchange of health-related information among participating organizations. Sometimes these entities focus primarily on administrative data exchange but, for the purposes of this work, we have considered only those that enable electronic exchange of clinical data.

HIOs can operate at the state or other geographically defined level, but often reflect collaboration based on service orientation, patient population, or strategic business interest. A number of other factors may influence the scale and scope of an HIO, as well as its likelihood of achieving success. These include:

1. The number and types of entities participating (or committed to participating) in electronic exchange of clinical data;
2. The variety of types of data being exchanged;
3. Whether electronic exchange is focused on exchanging data for a specific population (*e.g.*, just Medicaid patients);
4. Whether the participants have a history of prior collaboration; and / or
5. The level and sources of revenue available to the HIO (both in the formative phases and ongoing).[9]

At any given time, varying numbers of HIOs are reported to be active in the U.S., and many other less formalized exchange efforts exist across the country. Given the multiple and diverse examples in the U.S., it is not surprising that approaches for managing patient consent are equally so. In a later section, we provide several examples of how different states (and some differently defined HIOs) have approached this issue and what is unique about each approach.

Other vehicles for electronic exchange are continuing to emerge, including some that do not require the creation of a new governance entity and / or a reliance on underlying HIT systems from which to extract the data intended for electronic exchange. For the purposes of this whitepaper, we focus primarily on the common challenge of how to deal with the issue of consent, and less on the specific context or environment in which this and related decisions are made. A number of the specific examples of electronic exchange referenced throughout this paper are based on our review of state-led efforts, but this is primarily a function of there being more information available and transparency surrounding the decisions made at this level. Undoubtedly, there are lessons to be gleaned from smaller and / or less formalized exchange endeavors, but these examples were not as evident or readily accessible.

While there is relatively little quantifiable information available as to whether and to what extent patients involved in electronic exchange would differentiate between more or less complex efforts (as referenced above), it is reasonable to assume that several factors might influence that

[8] 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.

[9] Adler-Milstein, J. et al. "Characteristics Associated with Regional Health Information Organization Viability. *Journal of the American Medical Informatics Association*, Vol. 17, No. 1, January 2010, pp. 61-65.

perspective. For example, a reasonable hypothesis might be that electronic exchanges that are fairly limited in scope or scale (*e.g.*, exchange of lab information between a hospital and large group practice) might present less of a threat or reason for concern among participating patients than would electronic exchanges that integrate numerous types of patient information from multiple sources and make it broadly available for care and / or other purposes. Specific factors would likely include:

1. The types of information included in the exchange;
2. The nature and number of entities granted access to that information;
3. The purpose(s) for which the exchanged information could be used;
4. The perceived value of the electronic exchange to the patient; and
5. The extent of protections and remedies in place should one of the above conditions be compromised.

These and other issues often require decisions that take into account the particular laws that govern the use and disclosure of health information in the state in which they are chartered or operating.

CONSENT MODELS: DEFINITION AND DISCUSSION

This whitepaper is intended both to frame and describe some of the major policy, legal, cultural, practical, and other challenges associated with selecting consent models for electronic exchange, and also to serve as a decision aid for policy makers and stakeholders alike. Based on our review of various forms of electronic exchange in the U.S., as well as other sources in the public domain, we have determined that there are five core consent models. Provided below is a definition of each, along with some additional contextual information. These consent models are presented in order from "lowest" to "highest" in terms of reflecting the extent to which consumer preferences are integrated and accommodated.

It is important to note that the models are intended to apply to participation in a networked electronic exchange effort and are not intended to imply constraints to the usual transmission – paper or electronic – of information for treatment, payment, or health care operations purposes as permitted under HIPAA and other relevant federal and state laws. Also relevant is the fact that these models may be combined within the same exchange environment. An example of this is the situation where one consent model applies to the inclusion of information in a network and another model applies to the ability of the provider and other allowed participants to gain access to that information via the exchange.

The Five Consent Models

No consent

This model provides no opportunity for accommodation of individual preference with respect to participation in electronic exchange, so the health information of patients under the care of a participating provider organization is automatically included in and available (often according to certain rules) through the exchange. This model is typically found in states that require no additional provisions for the electronic exchange of health information beyond the federal floor

set by the HIPAA privacy regulations. In these states, electronic exchange can take place irrespective of and without obtaining patient preferences for participation (within the bounds of applicable federal and state laws). Not all HIOs with this authority exercise it, but *no consent* should be considered as an option in the spectrum.

One interesting permutation of this approach is the possible requirement that patients be notified of their participation in the exchange and educated as to what the exchange does, how the information is used, and what purpose(s) it serves. Another possible version of this model provides no opportunity for accommodation of individual preference with respect to participation in electronic exchange (meaning that all data flow into the exchange), but does require that patients be afforded the opportunity to exercise consent for making the information available for any purpose not already permitted by law (*e.g.*, public health surveillance). This means that while patients would have no ability to constrain the flow of their information into the system, they would have some authority to determine how (*e.g.*, by whom, under what circumstances) it can be used. It should be noted that this concept may also be applied to the *opt-in* model described later in this section.

Opt-out

In an *opt-out* model, the default is for all or some pre-defined set of data (*e.g.*, labs, summary record information) to be eligible automatically for exchange, with a provision that patients must be given the opportunity to opt out in full. In a typical *opt-out* scenario, this could mean either that the information of the patient who opts out is collected through the exchange (and used only for legally permitted purposes, such as public health reporting), but never shared with other providers for clinical care, or that the patient's preferences are captured and propagated such that his / her clinical information never even enters the exchange. Regardless of where in the system the information exchange is blocked, this option allows for no granularity of patient preference, meaning that a patient's information is either all in or all out. Many electronic exchange models with the legal authority to adopt the *no consent* approach ultimately end up using an *opt-out* approach instead.

Opt-out with exceptions

In an *opt-out with exceptions* model, the default is that all or some pre-defined set of data types are eligible for exchange, but patients can either opt out in full (as described above), or: 1) selectively exclude categories of data / specific data elements from the exchange; 2) limit exchange of their information to specific providers / provider organizations; and / or 3) limit exchange of their information for specific purposes. The trade-off with this level of patient accommodation is that it is technically and procedurally more complex to administer and manage. Very few electronic exchange models have allowed for full granularity in the choice of data type exchanged, but some have allowed patient choice as to which provider types may gain access to their data via the exchange. Granularity of exchange at the individual provider level is procedurally more complicated and could pose additional management challenges. For these and other reasons, it has rarely been implemented. Most entities engaging in electronic exchange have not yet attempted to allow granularity with regard to purpose specification, as very few are currently using the information for purposes other than clinical care delivery and public health.

Opt-in

In an *opt-in* model, the default is that no patient data are automatically made available for electronic exchange. Patients wishing to make all, or a pre-defined set, of their information available must actively express their desire to participate. This option allows for no granularity of patient preference—meaning that a patient's information is either all in or all out. Once participating, patients who opt in have no control over what information is shared, how, with whom, or for what purpose. The only exceptions here are: 1) permission is later revoked by the patient; or 2) other protections extend to the data (*e.g.*, marketing provisions in the HIPAA privacy regulations).

Opt-in with restrictions

In an *opt-in with restrictions* model, the default is that no patient data are automatically made available for electronic exchange. Patients wishing to make all, or a pre-defined set, of their information available for exchange must actively grant their consent to participate. They then have the option to make all of their information eligible for exchange or: 1) include only specific categories of data or / data elements; 2) enable information to flow only to specific providers; and / or 3) allow their information to be exchanged only for specific purposes.

In theory, each of these discrete consent models represents a cleanly-delineated option for how patient consent could be approached for electronic exchange. In practice, however, there are as many choice model permutations as entities that participate in electronic exchange. Each entity (regardless of scale) encounters who, what, why, and when decisions, and resolves them based on its own unique set of legal, cultural, political, and other contextual circumstances. This variability forces us to consider a more nuanced picture. Additionally, even though the above consent categories appear to be mutually exclusive, some electronic exchange systems have flexible enough policy frameworks such that they can permit multiple consent models to co-exist. One example of this occurs in those utilizing *opt-out* models that, in order to accommodate an array of provider preferences, have permitted provider entities to make their own determinations as to whether the patients under their care are required to give affirmative consent (*i.e.*, opt in) even when not dictated by the general policies for participation in electronic exchange.

GRANULARITY AND CHOICE

In numerous ways, and for a variety of reasons, patients participating in electronic exchange may prefer to:

1. Exert some control over the type and level of information that can be shared;
2. Restrict information accessed via electronic exchange to a limited (and potentially specified) set of individuals or entities;
3. Establish preferences for the time frame and / or duration for which their information could be accessed via electronic exchange; and / or
4. Specify – either broadly or specifically – the various purposes for which their information accessed via electronic exchange could be used.

A person's rationale for desiring this level of control may stem from concern or fear for how the information available through electronic exchange could be perceived or used, a personal preference for privacy, or his / her individual values. Whatever the reason, it is important to acknowledge and respect those concerns upfront so appropriate steps can be taken to advance the goal of health information exchange while still respecting fundamental autonomy and values. In the health care context, however, it is important to acknowledge the consequences associated both with enabling and choosing not to prioritize individual autonomy—many of them undesirable or unintended, or both.

Granularity by Data Type

One of the most commonly discussed issues in the context of electronic exchange is whether patients should be able to block specific data elements (*e.g.*, a recent lab test),[10] or categories of data (*e.g.*, all medications) from being exchanged electronically. This idea is referred to as granularity by data type. The advantages of this approach are relative, and depend considerably on one's perspective. Patient and consumer advocates, and very often consumers themselves (when asked), indicate a preference for having some choice in this matter and suggest that such a provision would increase their trust / willingness to participate in electronic exchange.[11]

However, providers and those responsible for implementing electronic exchange tend to view this level of control in a less positive light, partly for reasons related to the perceived difficulty of administering and then incorporating processes for accommodating this level of control into their workflow. In addition, most providers have expressed a strong preference to have complete (or as complete as possible) clinical information available to facilitate the provision of high quality care, and also to mitigate liability issues. They also argue that enabling patients to segregate potentially important data from other clinical information inhibits the provision of coordinated care and perpetuates the lack of integration between mental and physical health. One possible exception to this trend is seen in the case of psychiatrists and other behavioral and mental health providers, who may be more reluctant to share clinical data because they are sympathetic to the concerns of their patients about how such information could be used (*e.g.*, to discriminate, deny insurance coverage, etc.).[12]

In seeking a compromise solution for this challenge, it has been suggested that it should be possible to pre-define (for the purpose of sequestering from electronic exchange) specific categories of information that are likely to be considered as sensitive by individual patients. What we know from experience, however, is that sensitivity is subjective. For example, while some patients may have very few reservations about making their imaging results available to all of their providers, a victim of domestic violence may not want that same type of information to be shared beyond the system of the treating facility.

---

[10] *See* Purington, K. et al. *Electronic Release of Clinical Laboratory Results: A Review of State and Federal Policy*. Prepared for: California HealthCare Foundation, January 2010 at 2. Available at: http://www.chcf.org/topics/view.cfm?itemid=134157.

[11] Peel, D.C. *Written Testimony Before the HIT Policy Committee*, September 18, 2009, at 2-3. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_889203_0_0_18/Peel_PPR%20Written%20testimony%20HIT%20Policy%20Committee.pdf.

[12] Salomon, R.M. "Openness of Patients' Reporting with use of Electronic Records: Psychiatric Clinicians' Views," *Journal of the American Medical Informatics Association*, Vol. 17, Issue 1, October 2009, pp. 54-60.

Despite the reluctance to define specific categories of data for the purpose of restricting electronic exchange, this is exactly what has resulted from both federal and state laws that govern the flow of sensitive information,[13] such as substance abuse, mental health, and HIV diagnoses. In this case, however, it is the presence / interpretation of the law, and not the individual patient, that has restricted the flow of such information. Most electronic exchange models expressly exclude the exchange of sensitive information, and do so because they: 1) do not know how to interpret the various federal and state policies and regulations that apply to sensitive information; 2) have not yet determined how best to handle the technical and procedural challenges associated with data segmentation; and / or 3) wish to establish a basic level of trust before exchanging information considered "sensitive."

Given this environment, the question has been posed as to whether it is possible to define a set of eligible data for near-term exchange (*i.e.*, low hanging fruit) that would enable incremental progress. What most have settled on is: 1) a conservative (*i.e.*, more limited) interpretation of the federal and state laws related to the exchange of sensitive health information; and 2) a determination of what is reasonable and procedurally and technically feasible to implement. This process has led many entities to a "next best" granularity approach that allows patients to exert some control, not over which data are shared via the exchange, but with whom.

Granularity by Provider

One way of addressing consumer concern about electronic exchange is to restrict information access to only those providers approved by the patient. This method is referred to as granularity of consent by provider. There are three main approaches for how this can be handled:

1. The patient is given the option to permit access to only specific individual providers;
2. The patient is given the option to permit access to only specific provider or staff types (*e.g.*, all MDs and RNs could be granted access, but not office staff); or
3. The patient is given the option to restrict access at the provider entity level (*e.g.*, primary care and cardiology practices are granted access, but the allergist is not).

As with granularity by data type, the benefit of provider granularity is not perceived equally across stakeholders. While patients may view the option as a way both to retain some level of control and ensure that only those providers they deem appropriate are eligible, many of the provider and governance entity concerns mentioned above would apply. From a provider perspective, coordination of care may be compromised by their inability to get "the full picture" of a given patient. This holds true both for those providers with and those without access to a patient's information via electronic exchange—the former because they have only part of the picture, and the latter because they only have access to the information that resides within their own record.

[13] *See, e.g.*, Confidentiality of Alcohol and Drug Abuse Patient Records ("Part 2"), 42 C.F.R. pt. 2 (2009); New York laws governing disclosure of HIV-related information, N.Y. PUB. HEALTH LAW § 2782 (McKinney 2010); N.Y. COMP. CODES R. & REGS. tit. 10,§ 63.5(a) (2009).

Granularity by Time Range
Another possible, though rarely applied, granularity option involves the inclusion or exclusion of information based on the time / date associated with an element of clinical data. Theoretically, this method could be handled in a number of different ways, and used for a variety of reasons. Possible examples include:

1. An entity engaging in electronic exchange could make the determination that it is only necessary to have the most recent clinical information available to providers and other partners via electronic exchange. In this case, provider access could be restricted to only the most recent year (or two or three) of clinical data, and perhaps more direct patient consent could be required to release "older" information;
2. An entity engaging in electronic exchange could allow patients to apply a time range restriction that corresponds to specific episodes of care that may be particularly "sensitive' in nature (*e.g.*, a month spent in a rehabilitation clinic). In this case, provider access to all other clinical information on the patient could be allowed, but any clinical information recorded between X and Y dates would be blocked out; and / or
3. An entity engaging in electronic exchange could institute specific time-sensitive "use cases" that enable information access only for a certain period of time. A specific example that has been widely discussed and implemented by more than one entity is the "break the glass" provision, which is intended to enable access to clinical information only for a brief time (typically 24 hours) in order for providers to treat patients in emergency situations. This method also requires definition of a "purpose specification," and would therefore involve applying multiple layers of granularity in practice.

Each of the examples above might reflect an attempt to address the needs of multiple stakeholders. They also require consideration of the potential drawbacks associated with granularity of this type. Patients with a long medical history and / or chronic conditions, for example, may not be well served by limiting electronic exchange to only the most recent year of data, and the value of the data would be diminished from a public health and research perspective as well. Conversely, a failure to offer individuals some level of choice may lead certain patients to stop seeking care altogether, or to seek care only if they can pay out-of-pocket. It should also be noted that any of these time stamp permutations can be – and often are – combined with other granularity provisions.

Granularity by Purpose
A fourth granularity category involves segmentation according to the intended use or specified purpose for which data can be accessed via electronic exchange. With this type of consent, patients would have the option to consider all possible uses of their information that is available via electronic exchange (*e.g.*, care delivery, quality improvement, clinical research, health services research), and then determine which uses would be acceptable to them (*i.e.*, consent to use of information for specified purposes only). Of course, the latitude that any particular patient would have to deny use of his / her information for treatment purposes would be subject to the laws of the relevant state and consent model policies established for the particular electronic exchange. The same would hold true for other purposes that may not require a patient's consent, such as public health surveillance.

The primary appeal of granularity by purpose is that, assuming patients choose to consent to allow their information to be used for treatment purposes, and unless this choice is coupled with other granularity options, it enables all relevant clinical information to be made available via electronic exchange. From a provider perspective, as well as that of the patient who prioritizes highly-coordinated care, this method could alleviate concerns about incomplete or missing data that can jeopardize the goal of improving patient care. This approach, standing alone, also diminishes the technical and procedural concerns that arise with some of the other granularity options (*e.g.*, granularity by data type).

From the patient perspective, one advantage of this approach is that it affords some level of choice and perhaps the ability to help support (through allowance of data use) certain activities that are highly valued by that individual. For example, patients with a family history of cancer may be particularly inclined to make their data available for clinical research purposes in that field. Conversely, patients with significant privacy concerns could choose to deny access to their information for any or a particular purpose, and could also require more information or explanation for proposed uses on a case-by-case basis. To the extent that this method presents an opportunity for patients to gain a better understanding of how and why their information might be used, the process of participating in such discussions regarding consent could also help to foster greater understanding and engagement.

That said, this option does little to address the needs of patients who would prefer to have most of their information available for treatment or other purposes, but wish to deny access to a specified subset of providers or reduce availability of any information they deem too sensitive. Furthermore, granting patients the ability to restrict access in this manner potentially reduces the total volume of information available for a variety of possible purposes, particularly those that are less understood and / or less likely to gain patient approval.

General public perception may also be a factor in selecting choice options. Implementing nationwide electronic exchange of health information, particularly for uses other than treatment, may be perceived by segments of the population as inappropriate corporate or governmental intrusion. It has been suggested that these concerns may be somewhat mitigated by permitting some degree of patient choice as to whether to participate in such a system.

One final but critically important consideration regarding this option is that the process of defining and describing possible uses of information in electronic exchange may pose a significant challenge. This issue is evident in the difficulty that various stakeholders have had interpreting the purview of the HIPAA privacy regulations, which generally permit the exchange of protected health information for treatment, payment, and health care operations.[14] The first two domains are fairly straightforward and are generally supported by patients and providers, who rely on them for care delivery and payment reasons. Numerous polls have found that patients either already presume that their clinical information is shared with their health care

[14] 45 C.F.R. § 164.506(a) (2009). Please see the Legal Framework section for a fuller discussion of the HIPAA privacy regulations.

providers as needed, or overwhelmingly support such information sharing to support their care.[15] It therefore seems unlikely that many patients would choose to restrict access to their clinical information for such purposes. Further, though patients likely do not fully appreciate the extent to which or reasons why their information must be shared for payment purposes, most (except perhaps those who either do or would wish to pay out-of-pocket for select products and services) understand that such information sharing is a pre-condition of reimbursement. The health care operations element, however, is very open ended, and has been more difficult for stakeholders to interpret in an evolving health care landscape.[16] Any future efforts to define categories of use should try to incorporate lessons learned from this experience.

Each of these granularity options presents certain advantages and drawbacks. A common theme, however, is that the provision of patient choice comes at a cost —sometimes borne by providers, sometimes by electronic exchange governance entities, and sometimes by third parties who wish to use the information for research or other purposes. Conversely, a failure to offer individuals some level of choice may lead certain patients to seek care only if they can pay out-of-pocket or to stop seeking care altogether, and could have serious consequences for patient engagement in health and health care more generally.

U.S. AND INTERNATIONAL EXPERIENCES

Because health care improvement and efficiency gains are needed in many countries, and given that HIT and electronic exchange are widely believed to support these goals, a variety of models for electronic exchange exist throughout the world. As this section will highlight, the U.S. is not the only country to have struggled with the issue of patient consent in the context of electronic exchange. Countries that have implemented HIT systems have experienced varying degrees of success in leveraging them for the purpose of sharing health information electronically among relevant stakeholders. By examining examples of individual choice models currently used in the U.S. and other countries, the relative benefits of various approaches as well as their critical issues and challenges can be considered. While the sections that follow offer some important illustrative examples, they are not intended to be exhaustive or fully representative of the electronic exchange landscape.

State-Led Examples of Exchange in the U.S. – (See Appendix A)
In their efforts to maximize the benefits of HIT, numerous states and state-designated entities (SDEs) have worked to establish mechanisms for electronic exchange, many of them formalized as HIOs. An analysis of the various approaches to consent at the state level reveals great similarity in the awareness of core challenges, but vast differences in how these issues are addressed and resolved by each exchange effort. Through numerous conversations with individuals working at the state level, and additional research on individual exchange efforts, we have gained insight into the possible reasons for selecting one consent model over another.

---

[15] Schneider, S. et al. "Consumer Engagement in Developing Electronic Health Information System." Prepared for: *Agency for Healthcare Research and Quality*, July 2009, at 4-5. 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.

[16] McGraw, D. "Privacy and Health Information Technology," *O'Neill Institute: Legal Solutions in Health Reform*, April 27, 2009, at 21.

Based on a variety of factors (*e.g.*, state laws, funding availability, and leadership capacity), the technical architecture, governance structure, and policy decisions vary significantly from one exchange effort to the next. Not surprisingly, approaches to handling patient consent also vary significantly.

Some state laws, for example, do not require patient consent for the exchange of health information beyond that required by federal law, enabling HIOs in those states to implement a *no consent* model. Other states' laws, such as those in New York, contain explicit patient privacy protections,[17] and have led to implementation of an *opt-in* model of exchange. State exchanges also vary in their accommodation of various stakeholders. Some state HIOs, such as Delaware's Health Information Exchange (DHIN), have designed their exchanges primarily to support the needs and interests of the provider community. Other states, such as Washington, afford patients a more active role in determining what, how, and with whom their health information can be shared by designing their exchange programs with consumer choice as a more pronounced goal.

Drawing from the experiences of HIOs in eight states, this section provides an overview of the range of choice models in operation at the state level today, along with examples of how they define core elements of their exchange efforts. The section includes comparisons of the types of information exchanged, the purposes for which information can be used, the processes by which consent is obtained and managed (who and how), and the durability of consent. In reviewing the activities in these states, we have identified examples of: *No consent, Opt-out, Opt-in,* and *Opt-in with restrictions,* many of which co-exist within the same exchange but are applied differently depending on specific conditions. We also have included some discussion of a health record bank approach underway in the State of Washington.

Consent Models Implemented at the State Level

No Consent

The legal landscape in Indiana and Delaware has enabled HIOs in both states to apply *no consent* policies to their electronic exchange efforts—the Indiana Health Information Exchange (IHIE) and the DHIN, respectively. In Indiana, no patient consent is needed for the exchange of health information under state law. IHIE has therefore chosen not to require express patient consent for participation in the exchange.[18] However, federally-funded substance abuse treatment programs covered by the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (Part 2)[19] do not provide data to IHIE.[20] In Delaware, the results delivery function[21]

[17] New York laws governing disclosure of HIV-related information, N.Y. PUB. HEALTH LAW § 2782 (McKinney 2010); N.Y. COMP. CODES R. & REGS. tit. 10, § 63.5(a) (2009).

[18] Email from Victoria Prescott, CEO of McBroom Consulting, December 23, 2009.

[19] 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). For more information on Part 2 in the context of electronic exchange, see Legal Framework section.

[20] Email from Victoria Prescott, *supra* note 18.

[21] DHIN's results delivery function allows physicians to receive electronically a patient's clinical lab and radiology results, medication history, and discharge summaries. See Matthews, T. *Health Bridge: Transforming Health Care Through Connectivity and Collaboration PowerPoint Presentation,* February 19, 2010. Available at: http://www.nga.org/Files/pdf/1002ehealthmatthews.pdf.

of DHIN also operates under a *no consent* model, meaning that a variety of patient data are included in the exchange without the provision of express consent.[22]

In selecting its individual choice model for the results delivery function, Delaware policy makers prioritized the needs and concerns of the provider community, essentially minimizing the likelihood that patient information would be "missing" from the exchange in the event that consent was not granted. As a result, provider participation in the DHIN is high, and a significant portion of eligible records are available through the exchange. Since going live in 2007, DHIN's results delivery function automatically uploads a patient's laboratory data, radiology reports, and hospital admissions, discharge, and transfer data to the DHIN system at the point of care without patient consent.[23] As of December 2009, over 85 percent of all laboratory transactions in the state were available through DHIN, and more than 80 percent of hospitalizations were captured.[24]

Full Opt-Out

By contrast, the patient query function of DHIN's system operates as an *opt-out* model. This function allows providers to query the system to obtain specific data on a particular patient.[25] While they have no choice in the matter of whether their information is available through the exchange, patients can choose to opt out of the query function, thus barring any provider seeking to access their information via the exchange from doing so without first obtaining the patient's consent.[26] Again, however, DHIN has chosen to maximize the availability of health information to the provider community by making it somewhat difficult for patients to exercise this *opt-out* option. To opt out of the DHIN system, a patient must have an approval form signed by his or her provider or a notary public (to validate identity), and then return the form to DHIN.[27] Although DHIN makes it the provider's responsibility to educate a patient about the policies, practices, and rationale for the exchange, including the procedure for opting out, no one in the State of Delaware has yet exercised the right to deny access to their information via the exchange.[28] DHIN's approach raises questions as to whether patients in Delaware are truly aware of the exchange and, if so, how well they understand the purpose of the exchange, the actors involved, the potential uses of their information, and their rights.

---

[22] The Commonwealth Fund. *Delaware: First State, First Statewide Health Information Exchange* in "States in Action: October/November 2009." Available at: http://www.commonwealthfund.org/Content/Newsletters/States-in-Action/2009/November/October-November-2009/Snapshots/Delaware.aspx; Phone call with Sarah Matthews, Vice President of Client Services, Advances in Management, Inc., December 3, 2009. Delaware does not have a general health information law, meaning that most information may be disclosed in accordance with HIPAA, but does statutorily require providers to obtain patient permission to disclose the results of an HIV test. Del. Code Ann. tit. 16 § 1203(a)(2),(3),(4) (2008); 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, at 4-3, n. 72. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_910326_0_0_18/DisclosureReport.pdf.

[23] Phone call with Sarah Matthews, Vice President of Client Services, Advances in Management, Inc., December 3, 2009.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

Another example of an *opt-out* exchange is the Chesapeake Regional Information System for Our Patients (CRISP) in Maryland. CRISP currently has two operational pilot programs: 1) an exchange of medication history between select hospitals in Baltimore County; and 2) an exchange of certain clinical data between select hospitals in Montgomery County.[29] The default policy in Maryland has been that patients are notified at the point of care about the existence of CRISP and about their ability to opt out of all exchange participation.[30] Compared to DHIN, CRISP affords patients greater opportunity to exercise their consent options. Patients can opt out of the exchange by calling a toll-free phone number and requesting to have their information excluded.[31] Alternatively, if they wish to participate, they can affirmatively enroll in CRISP via phone or by completing a form available from their provider's office.[32] Depending on the particular anticipated use of the information, additional patient consent may be required.[33] These permutations have not yet been fully explored, as Maryland's electronic exchange, like many other states', is still evolving.

As in Indiana, state laws in Virginia and Tennessee do not require express consent from patients to share their general clinical information electronically for treatment purposes or for other purposes expressly permitted under law.[34] The CareSpark organization, which spans areas of both Virginia and Tennessee, therefore has chosen an *opt-out* model. However, the CareSpark Board of Directors felt strongly that community members involved in the exchange should be well educated about the process.[35] As a result, CareSpark established an *opt-out with notice* policy, meaning that no data are included in the system until the patient has received at least minimal education about the exchange.[36] At present, this education occurs largely in provider settings. CareSpark leaves the question of whether more strenuous consent policies should be used to the discretion of individual provider organizations.[37] If provider organizations prefer, they can require express consent (or denial thereof) from their patients.[38]

Opt-in

The legal environment, stakeholder orientation, and governance structures in some other states have resulted in the development of consent models that allow for more patient choice. Exchanges in Rhode Island, New York, and Massachusetts all use variations of *opt-in* approaches. The Rhode Island Quality Institute (RIQI), for example, uses an *opt-in with restrictions* model. To participate in the Rhode Island exchange, patients must actively enroll in RIQI (opt in) and can then exercise one of three options for participation:

1. Allow all provider organizations involved in their care to access information;

[29] Phone call with David Sharp, Director of the Maryland Center for Health Information Technology, Maryland Health Care Commission, November 19, 2009.
[30] *Id.*
[31] *Id.* Even if a patient opts out, a certain amount of basic patient demographic information will still reside in the exchange (in a separate data repository used for the master patient index), but providers won't be able to access it.
[32] *Id.*
[33] *Id.*
[34] Phone call with Liesa Jenkins, CareSpark Executive Director, and Randy Sermons, CareSpark technology committee, November 30, 2009.
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*

2. Authorize only certain provider organizations to access information; or
3. Authorize the "default" setting, which provides temporary access to information by a licensed practitioner only in the case of an emergency or unanticipated event.[39]

New York's exchanges also have adopted *opt-in* models. The models vary depending on the entity involved, and generally take one of two forms: 1) the provider obtains patient consent at the point of care; or 2) the exchange obtains patient consent using a multi-provider consent form that can be accessed either at the point of service or online via the entity's website.[40]

Similarly, the three pilot programs launched by the Massachusetts eHealth Collaborative (MAeHC) operate using an *opt-in* model. Patient consent for participation in MAeHC is also obtained at the point of care.[41] At a patient's first visit to a given clinical entity, he or she is given the option to have all clinical data from that entity included in the exchange.[42] Similar to Rhode Island's model, patients can identify which provider entities can and cannot contribute their information to the exchange.[43]

A final and unique model of electronic exchange is the health record bank, with which patients create personal accounts using web-based tools such as Microsoft HealthVault, Google Health to store their personal health information in one location. With a patient's consent, copies of his or her health information can then be transferred from the point of care into the health record bank account.[44] Patients can then allow release of this information to providers and other entities of their choosing.[45] In part because it places a high value on consumer control, the State of Washington has recently implemented four health record bank pilot programs in communities across the state.[46] It should be noted, however, that this is not the only exchange model underway in Washington, and the preferences that patients express through use of this model do not – at least at present – affect the flow of information directly among providers and other organizations subject to HIPAA.

Type of Information Exchanged

An examination of exchange efforts across the country reveals that, while most entities start by sharing the same types of information, the practice evolves over time as the exchange matures. Largely due to the fact that many of these data are readily available in standard electronic

[39] Phone call with Amy Zimmerman, Chief of Health Information Technology, Rhode Island Department of Health, November 23, 2009.
[40] Phone call with Ellen Flink, Director of Research in Patient Safety and Quality Initiatives, New York State Department of Health Office of Health Systems Management, Lara Rosas, Director of Policy and Compliance, New York State Department of Health and Mental Hygiene Primary Care Information Project, and Katie O'Neill, Senior V.P., Legal Action Center, November 12, 2009.
[41] Tripathi, M. *Massachusetts e-Health Collaborative Powerpoint Presentation*, December 2008. Available at: http://www.mendocinohre.org/rhic/200812/rhic_tripathi_20081217.ppt.
[42] *Id.*
[43] Tripathi, M. et al. "Engaging Patients for Health Information Exchange," *Health Affairs*, Vol. 28, No. 2, March 2009, pp. 435-43.
[44] Phone call with Juan Alaniz, Jr., Deputy State Health Information Technology Coordinator, and Kelly Llewellyn, Assistant Deputy State Health Information Technology Coordinator, Washington State Health Care Authority, December 9, 2009.
[45] *Id.*
[46] *Id.*

formats, exchanges typically begin with laboratory data and radiology reports, and then advance to highly codified data elements, such as hospital admissions, discharge, and transfer summaries. We identified no examples of clinical notes exchange, and few examples of problem lists and other categories of information for which there has been little harmonization in either definitional or technical standards.

In sum, we have found that some exchanges are more mature in this respect than others. Since beginning its operations in 2007, DHIN's results delivery function automatically uploads a patient's laboratory data, radiology reports, and hospital admissions, discharge, and transfer data to the DHIN system at the point of care without patient consent.[47] DHIN plans to expand this list by adding PACS data[48] to the system in January 2011, which would allow a provider to view a patient's radiology images through a link in the radiology reports.[49] DHIN also expects to include a patient's 90-day medication history in the near future.[50] Similarly, laboratory data, medication data, and x-rays are currently eligible for transfer into patient health record banks in Washington.[51] Presently in test mode, Rhode Island's RIQI does not currently exchange any type of health information; however, RIQI has short-term plans to exchange laboratory data and medication history, with longer-term plans to exchange radiology reports and summary discharge reports.[52]

The MAeHC and the IHIE are examples of more sophisticated HIOs, and exchange a wide array of health information. The MAeHC gives 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.[53] Similarly, several types of data are available for exchange in the IHIE, including labs, pathology, radiology, emergency department reports, electrocardiogram reports, medication history, discharge summaries, allergies / immunizations, ambulatory appointment data, claims processing, and prescription data.[54] IHIE also offers several business models and electronic exchange services through its system, including a clinical messaging service that delivers test results from labs to the doctor's office, a patient look-up service, and a quality metrics and reporting service.[55]

How Information is Used

In addition to variation in the type of information exchanged, differences exist across state-level exchanges with respect to the ways in which health information can be used. Some, such as the

[47] Phone call with Sarah Matthews, *supra* note 23.
[48] "PACS" is an acronym for picture archiving and communication systems. PACS are computers dedicated to the storage, retrieval, distribution and presentation of images. *See*, Hood, N.H. "Introduction to Picture Archive and Communication Systems," *Journal of Radiology Nursing,* Vol. 25, Issue 3, September 2006, pp. 69-74.
[49] Phone call with Sarah Matthews, *supra* note 23.
[50] *Id.*
[51] Phone call with Juan Alaniz, Jr., *supra* note 44. At present, patients participating in the Washington health record banks don't have the ability to input or alter their health information in the bank; they can only view the information on a computer screen and print it out to share with providers in hard copy form.
[52] Phone call with Amy Zimmerman, *supra* note 39.
[53] Tripathi, *supra* note 41.
[54] University of Massachusetts Medical School Center for Health Policy and Research. *Public Governance Models for a Sustainable Health Information Exchange Industry: Appendices*, February 17, 2009, at 5.
[55] Email from Victoria Prescott, *supra* note 18.

IHIE, augment their choice of consent model by limiting data exchange to particular use cases.[56] In the IHIE, which uses a *no consent* model, a patient's data are maintained in separate vaults, or clinical repositories, by the generating institution until a provider triggers an allowed use.[57] At that time, the patient's data becomes available to the provider, but only for a limited time window that depends on the specific use case.[58] Emergency departments, for example, have limited access to health information data for only 24 hours.[59] DHIN, which uses an *opt-out* model for its patient query function, uses a similar "break the glass" system to access information in emergency and / or unanticipated circumstances. Emergency department physicians in Delaware who work within the DHIN are designated as "superusers" and may access a patient's data at any time. Physicians and specified staff may access a patient's record in non-emergencies if there is no previously established clinical relationship, but must specify a time frame and purpose (*e.g.*, for a new patient who has made an appointment for a given day). All such access events are subject to audit by the DHIN, both routinely and at the request of the patient. However, this type of access is not available at all (for any type of provider) for patients who have chosen to opt out of the query function.

Most state exchanges currently allow patient information to be used for treatment purposes only.[60] While some indicate a preference to continue in this vein, others have plans to expand their uses of collected health information. For example, data presently exchanged through CareSpark is used for treatment purposes only, but the entity's goal is to expand to public health reporting and eventually to other research applications.[61] The type of information exchanged in the CareSpark system is also influenced by state law. Currently, CareSpark only exchanges general clinical information, which expressly excludes any type of information deemed sensitive under state laws in Virginia and Tennessee.[62] However, this policy is presently under review and could change in the future.[63]

Although data exchanged in Maryland's CRISP is primarily used for treatment purposes, CRISP's secondary use cases include public health reporting, research, and biosurveillance.[64] CRISP policy makers have also recognized that great potential exists for using the exchange for early identification of communicable diseases, chronic disease management, data mining, and identification of potential research participants.[65] CRISP leadership also recognizes, however, that sound policy development and consumer education will be necessary to enable these secondary uses.[66]

---

[56] *Id.*
[57] Email from Marc Overhage, President and CEO of the IHIE November 23, 2009.
[58] *Id.*
[59] *Id.*
[60] Public health is an allowed and commonly applied exception. Phone call with David Sharp, *supra* note 29; CRISP Health. *Maryland Health Care Commission HIE Policy Board Meeting Slides*, December 8, 2009. Available at: http://www.mhcc.maryland.gov/electronichealth/hie_policy_board/crisp_policy_board_120809.pdf; *See, e.g.*, R.I. GEN. LAWS § 5-37.7-7 (2009).
[61] Phone call with Liesa Jenkins, *supra* note 34.
[62] *Id.*
[63] *Id.*
[64] Phone call with David Sharp, *supra* note 29; CRISP Health, *supra* note 60.
[65] CRISP Health, *supra* note 60.
[66] *Id.*

Granularity Options

Only one of the eight exchanges considered in this analysis, the Washington health record bank model, allows patients to segment information in the exchange by data type. Although Washington's health record banks allow patients to sequester certain types of data from view, a patient's ability to do so depends on the type of software used to manage his / her health record bank account.[67] The two types of software available for use in Washington's health record banks, currently Google Health and Microsoft HealthVault, have different capabilities. At present, Google Health does not provide the same level of granularity as Microsoft HealthVault, which offers patients the ability to control the type of information providers see.[68]

Although many state-level HIOs do not currently support segmentation of health information by data type, a few have established consent models that allow patients to segment data either by provider organization or by individual provider. Currently, both RIQI and Washington's health record banks allow segmentation by provider, meaning that a patient can select which specific providers can view his or her health data. Maryland's CRISP also has expressed intentions to enable this level of consumer control once health record bank efforts gain more traction in the state.[69] Enabling patients to provide some level of input as to who can view their health information, under what conditions, and for what purpose, represents a tremendous opportunity for growth among state-level exchange efforts, and one that would be strongly supported by consumer and patient advocacy groups seeking greater engagement in their health and health care.

How Consent Is Obtained

In each of the state models described above, the process for obtaining consent varies. In general, consent is obtained (or not) at the provider point of care level, with educational assistance regarding notification and consent options often facilitated by the relevant HIO. Other approaches include active outreach on the part of the HIO, with some providing consent tools via the web or over the phone. These approaches allow patients to complete relevant forms and specify provider access preferences directly through the HIO. Some models rely upon a one-time event for obtaining patient consent, while others call for multiple interactions. In addition, some HIOs apply a single form for all use cases, whereas others tailor the forms to specific uses of data.

The DHIN and CareSpark models exemplify a provider-centric approach to educating patients about consent options. DHIN places all responsibility for notifying patients of its *opt-out* procedures on providers, offering them talking points, sample privacy language, and confidentiality forms to assist them in their conversations with patients.[70] Similarly, in the CareSpark model, providers are responsible for educating patients and notifying them of the exchange policies. CareSpark has an employee who trains provider organizations on the consent process, and also supplies providers with written educational materials that can be used during

[67] Phone call with Juan Alaniz, Jr., *supra* note 44.
[68] *Id.*
[69] Phone call with David Sharp, *supra* note 29.
[70] Phone call with Sarah Matthews, *supra* note 23.

the notification process.[71] Most provider organizations affiliated with the CareSpark exchange use a paper notice or consent form when they first discuss the subject with a patient.[72]

Other state exchanges obtain patient consent using a combination of provider-based and other approaches. Patients can enroll in Maryland's CRISP via phone or through a form provided at the point of care.[73] At present, a CRISP policy board is determining whether one consent form should cover all (or most) use cases, or whether multiple consent forms should be used for various secondary uses of data, including biosurveillance and public health.[74] Exchanges in New York also have two approaches for obtaining patient consent: one that allows the provider organization to obtain consent at the point of service, and another that allows the specific exchange to obtain consent through a multi-provider consent form that can be accessed either at the point of service or online via the entity's website.[75] Finally, RIQI trains staff in participating provider organizations to walk patients through the consent process and assist them with completion of the enrollment and authorization forms.[76] Alternatively, patients seeking to enroll in RIQI can do so directly through Rhode Island's "Current Care" website,[77] though they must also call a hotline to indicate their provider preferences.[78]

Durability of Consent

Many state-level HIOs have made the determination that a patient's consent to participate in the exchange remains in effect until expressly revoked. In others, consent is valid only for a limited time, and depends on a set of pre-defined conditions. Exchanges that require consent for specific use cases include the IHIE, RIQI, and CRISP. IHIE gives providers access to patient data in the system for various lengths of time, depending on the specific use case.[79] Similarly, CRISP plans to require additional patient consent for some use cases, but has not yet established those parameters.[80] Furthermore, it is possible that general parameters might apply to all exchanges operating within the CRISP HIO umbrella, but vary from one to another in terms of specifics. Patients who select the default consent setting in RIQI, which provides temporary access to a patient's information only in the event of an emergency or unanticipated event, authorize access to their data for a period of 72 hours only.[81] In other state models, such as DHIN, the New York exchanges, and two of the consent options in RIQI, patient consent is durable until expressly revoked. Patients enrolled in these exchanges have the ability to revoke their participation at any time. If patients in the New York entities or RIQI revoke participation in the exchange, their existing data remains, but will be sequestered and denoted as inaccessible unless required by law.

---

[71] Phone call with Liesa Jenkins, *supra* note 34.
[72] *Id.*
[73] Phone call with David Sharp, *supra* note 29.
[74] *Id.*
[75] Phone call with Ellen Flink, *supra* note 40.
[76] Phone call with Amy Zimmerman, *supra* note 39.
[77] http://www.currentcareri.com.
[78] Phone call with Amy Zimmerman, *supra* note 39.
[79] Overhage, M.J. *Testimony to the HIT Policy Committee on Patient Choice, Control, and Segmentation of Health Information*, September 18, 2009. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_889187_0_0_18/Overhage_HIT%20Policy%20Committee%20September%202009%20v4.pdf (if the provider is an ER, for example, access is time limited to 24 hours).
[80] Phone call with David Sharp, *supra* note 29.
[81] Phone call with Amy Zimmerman, *supra* note 39.

Data Security Oversight and Accountability

To build consumer trust in electronic exchange and ensure that sensitive information is protected, systems of electronic exchange should contain built-in security protections, and have mechanisms of enforcement in place for when health information is misused or a security breach occurs. Currently, some safeguards in state-level exchanges are more vigorous than others, and states vary in the degree to which audit and enforcement penalties are built into state law.

As a baseline, all of the electronic exchanges reviewed for this project require some form of authentication in order for providers to gain access to information via the exchange. Many have also tried to limit vulnerability by proceeding with the exchange of data that do not qualify as sensitive, as contemplated in federal and state law. CareSpark, for example, attempts to ensure that sensitive information is not shared by restricting the participation of facilities that primarily serve patients with sensitive conditions.[82] While the representatives of CareSpark with whom we spoke acknowledge that this is a sub-optimal approach with potentially negative implications for both patients and providers, they have settled on this approach as an interim solution.

In part to offset the fact that patients in Delaware have limited opportunity to exclude themselves from the exchange, DHIN has put systemic protections in place to protect patient information. In the DHIN system, providers can only access health records of their current patients, and must "break glass" (*i.e.*, follow a specified protocol) to obtain data on a patient they have not yet treated.[83] In addition, providers can design system security so that only certain staff can access data through the exchange.[84] Patients also have the right to obtain an audit report of providers who have accessed their records.[85] DHIN routinely conducts audits to ensure compliance with these policies, and revokes the privileges of providers who misuse the exchange.[86] Washington's health record banks and the New York exchanges also contain audit functions, which allow patients to find out when and by whom their records have been accessed.[87]

Another security method employed by many state exchanges is the use of firewalls. The State of Rhode Island is currently supporting the development of a technology solution that will reside for the time being at each contributing provider site. The interface will contain a firewall, which will require the participation status of patients to be ascertained before information is shared outside the firewall.[88] The New York exchanges also include safeguards enabling a patient to lock certain data behind a firewall so that it can only be seen by a designated primary care physician.[89]

Many states rely upon state law to establish enforcement and penalty mechanisms for the use (and misuse) of health information in exchanges. The Rhode Island Health Information Exchange Act of 2008, for example, gives patients the right to obtain reports of the health

[82] Phone call with Liesa Jenkins, *supra* note 34.
[83] Phone call with Sarah Matthews, *supra* note 23.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] Phone call with Juan Alaniz, Jr., *supra* note 44; Phone call with Ellen Flink, *supra* note 40.
[88] Phone call with Amy Zimmerman, *supra* note 39.
[89] Phone call with Ellen Flink, *supra* note 40.

information that has been shared through RIQI and the identities of those who access the information, in addition to notices of security breaches.[90] New York's Education law makes it professional misconduct for a physician to reveal a patient's health information to a third party without patient consent.[91] Finally, legislation in Delaware specifies that any misuse of DHIN health information or data must be reported to the state Office of the Attorney General, and that violators will be subject to prosecution and penalties under either the Delaware Criminal Code or federal law.[92]

Each of these examples speaks to the notion that there are multiple, necessary dimensions to consumer protection, and that an entity's determination of which consent model to use in electronic exchange is an important – but still only one – consideration. Consent models that do not incorporate patient preferences as an initial matter can be augmented with legal, technical, security, and privacy policies designed to protect patient data. As discussed in depth below, while consent plays a critical role in protecting patient privacy and autonomy, it is not the only method by which patient interests can be protected in electronic exchange.

Examples of Exchange in Other Developed Countries (See Appendix C)

Canada

Canada is currently developing interoperable electronic exchange for its 32 million residents. The system is being developed and funded primarily through Canada Health Infoway, a not-for-profit corporation whose members are the 14 federal, provincial, and territorial Deputy Ministers of Health. Infoway supports HIT development by way of strategic investments in local and regional infrastructure projects. Specific consent policies are developed primarily at the provincial level and are largely *opt-out* systems with various degrees of granularity.[93] The federal government has created a set of guidelines to promote further harmonization and development of consent policies nationwide, the Pan-Canadian Health Information Privacy and Confidentiality Framework,[94] and is developing a nationwide system to track consent directives through the Consent Directive Management Service.[95] Infoway plans to have fully interoperable EHRs for its entire population by 2016.[96]

The Netherlands

The Dutch National Healthcare Information Hub (LSP), currently being implemented by the National Information and Communication Technology Institute for Healthcare (NICTIZ), is an *opt-out with exceptions* system built around remote information hubs connected to a national,

[90] R.I. GEN. LAWS § 5-37.7-10 (2009).
[91] N. Y. EDUC. LAW § 6530 (23) (McKinney 2010).
[92] DEL. CODE ANN. TIT. 16, § 9926 (2010).
[93] Canada Health Infoway. *White Paper on Information Governance of the Interoperable Electronic Health Record*, March 2007. Available at: http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf.
[94] Health Canada. *Pan-Canadian Health Information Privacy and Confidentiality Framework*, January 27, 2005. Available at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php.
[95] Canada Health Infoway, *supra* note 93, at 7-8.
[96] Canada Health Infoway. *2015: Advancing Canada's Next Generation of Health Care.* Available at: http://www.v1.theglobeandmail.com/partners/free/infoway/pdf/2015%20Health%20care%20full%20report%20EN.pdf.

searchable database. This system, referred to as the "health care Google," maintains patient records at the practitioner or regional level (where regional electronic exchange already exists), and makes them 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).[97] The country is currently debating whether to require all practices to connect to the LSP.[98] 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.[99]

Sweden

Sweden began trials on May 4, 2009 to implement a health information exchange starting with the Municipality and County Council of Örebro.[100] Sweden plans to place all digitized records on a central server, but to allow patients to authorize which physicians will be able to access their records in the database.[101] Patients must also restrict the time period in which the provider can continue to access their records after giving initial permission. Sweden's system will also restrict how much of the medical record providers can see. However, county councils and municipalities, not patients, designate which professionals can see which parts of the record. The system has a "break the glass" provision that allows health care professionals to access records in an emergency, but the access will be logged and providers will have to explain why they needed to view the information.[102]

ANALYSIS OF CHOICE MODELS

Having identified the five core consent models, potential granularity options, and examples of individual consent approaches in the U.S. and abroad, we now turn to an analysis of key factors that likely would influence the choice of one particular consent model over another. As a preamble, we provide an overview of the needs, concerns, and general perspectives associated with each of the major categories of stakeholders typically involved in electronic exchange. The analysis section itself is organized into three major parts. The first is a discussion of certain **ethical and cultural** considerations relevant to the determination of which choice model to apply. The second focuses on some of the critical **logistical, technical, and process** considerations (with respect to consent) that often emerge in the course of establishing an exchange, and the third describes the federal and state **legal framework** that shapes the environments in which consent decisions are made.

---

[97] Pritts, J. and K. Conner. "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 3.

[98] HIMSS Enterprise Systems Steering Committee. *Electronic Health Records: A Global Perspective*. August 2009, at 25. Available at: http://www.himss.org/content/files/200808_EHRGlobalPerspective_whitepaper.pdf.

[99] Pritts, *supra* note 97, at 42-45.

[100] National Patientöversikt. "Focus on Delivery." Available at: http://www.npö.nu.

[101] "Prevention Progression." *Public Service Review: Science and Technology*, Issue 4, July 2009, p. 2. Available at: http://www.publicservice.co.uk/article.asp?publication=Science%20and%20Technology&id=397&content_name=Health%20technology&article=12698.

[102] *Id.*

Stakeholder Perspectives

Nearly every stakeholder in health care has preferences for, and will be affected by, the consent model approach selected to support electronic exchange. Not surprisingly, these stakeholders differ in their emphasis on and prioritization of features associated with the various models, and will be affected in diverse ways by the selected approach. Sometimes the impact may be characterized as logistical in nature (*e.g.*, the imposition of administrative burden), and other times may present a financial strain or practice concern. Still others reflect the fears and concerns associated with the potential for misuse of information (*e.g.*, discrimination, social stigmatization). All of these perspectives are valid, and must be considered in the context of the core policy objectives and operating principles established by a given exchange. It should be noted that the stakeholder perspectives articulated below are intended to reflect the predominant view, and do not attempt to accommodate the natural variability and wide ranging spectrum of individual perspectives that likely exist.

Patients / Consumers

In numerous polls and focus groups, consumers have expressed strong support for the implementation and exchange of EHRs, believing that these technologies have the potential to improve care coordination, reduce paperwork, and reduce the number of unnecessary and repeated tests and procedures.[103] These same studies also reveal significant consumer concern over who has access to their health information and how it is used.[104] In a focus group study conducted by the Agency for Healthcare Research and Quality, participants voiced concern – both spontaneously and when prompted by a moderator – that electronic health data are more prone than paper to security breaches and misuse by entities such as employers and insurance companies.[105] When asked about the issue of consent, a large proportion of participants believed that their consent should be sought by a physician or staff member before their health information could be shared electronically, and also perceived this as an opportunity to specify who could access this data.[106]

Generally, consumers want to equip their health care providers with the information necessary to support the delivery of well-coordinated and high-quality care. Some have concerns, however, about the potential for intrusions on their privacy and, more importantly, how their information might be accessed and used in unanticipated and / or damaging ways.[107] Recent stories in the news concerning improper access to medical information by unauthorized staff, data breaches, and large-scale data losses may raise patients' concern that the wrong people will be able to access their health information. Consumers may be protective of their health information in part because disclosure of such information – whether deemed sensitive or not – can cause embarrassment and may be used as a basis for discrimination (*e.g.*, denial of health insurance and loans, denial / loss of a job, criminal liability). Absent the existence of an overarching set of policies that offer protections against discrimination and other negative consequences associated

[103] Schneider, *supra* note 15, at 16; Markle Foundation. *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*, November 2006, at 1. Available at: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.
[104] Schneider, *supra* note 15, at 2.
[105] *Id.* at 18-20.
[106] *Id.* at 36-37.
[107] Markle Foundation, *supra* note 103.

with unwanted information exposure, it is likely that many consumers would express a preference for systems that afford them a high level of control.

In focus group settings, consumers have indicated that controlling access to specific health data or categories of data would increase their trust and willingness to participate in electronic exchange.[108] For some, this goal might be accomplished through granularity of choice by provider, time stamp, or data use. For others, however, *opt-in* models with full granularity (*e.g.*, a health record bank model) might be the only consent option that sufficiently meets their concerns. In this scenario, consumers might also prefer to have choice beyond the categories established for what has been deemed sensitive information, and might desire the ability to define and then restrict specific information from electronic exchange.

While blanket *opt-in* and *opt-out* models allow patients to choose whether or not their information can be shared, these models force an all or nothing decision. Given this level of choice, patients with specific privacy concerns would likely opt out (or refuse to opt in) in order to prevent information that they consider to be too private to share from being disclosed via the exchange. This action could not only reduce the patient's access to high-quality / well-coordinated care, but might also, as described below, have negative consequences for other stakeholders as well.

Providers

Individual health care providers participating in electronic exchange want at least the following three basic elements from the experience: 1) consistent and comprehensive access to information that will improve their capacity to deliver high-quality, well-coordinated care; 2) assurance that their reliance on electronic exchange as an important information source will not increase their exposure to liability; and 3) minimization of technical, financial, and administrative burden associated with participation, including workflow modifications required for obtaining and managing consent).[109]

Given their preference for more rather than less patient information, many providers do not support consent models that potentially limit either the number of patients participating in electronic exchange, or the amount / types of information available for a specific patient. Generally speaking, providers worry that any treatment decision made without access to relevant information might impact negatively their ability to provide quality care, and could expose them to medical liability.[110] This concern is essentially a critical mass issue, which is to say that providers will only participate in electronic exchange to the extent that they perceive value in doing so. This issue is evident in other HIT-related areas as well. For example, a recent AHRQ-

[108] Peel, *supra* note 11.

[109] Hersh, W. "Health Care Information Technology: Progress and Barriers," *JAMA*, Vol. 292, No. 18, November 10, 2004, pp. 2273-4; Goldstein, M.M. and Blumenthal, D. "Building an Information Technology Infrastructure," *Journal of Law, Medicine and Ethics*, Vol. 36, Issue 4, December 2008, pp. 709-15, at 712. See also Texas Medical Association. "TMA Survey: Electronic Medical Records Report," Fall 2009, at 15. Available at: http://www.texmed.org/uploadedFiles/Practice_Management/Computers_And_Software/EMR%202009%20survey%20report.doc.

[110] Dolan, P.L. "Do EMRs cut liability risk? Insurers want evidence before offering more discounts," American Medical News, November 30, 2009. Available at: http://www.ama-assn.org/amednews/2009/11/30/bica1130.htm; Texas Medical Association, *supra* note 109, at 17.

supported survey of 228 outpatient primary care providers found that non-use among previous users of e-prescribing systems was associated with perceptions of poor usability and lack of complete information available through the system.[111]

Providers also have expressed concern about the increased financial and administrative burden associated with initiating and maintaining a consent management process.[112] In an environment where many providers already face challenges in adopting and using and, eventually, demonstrating "meaningful use"[113] of HIT systems, the need to educate patients about their consent options, integrate information regarding the administration of consent into their practice workflow, and adhere to that directive is perceived as being overly onerous.

Finally, timeliness of access to information via electronic exchange may be impacted by the choice of consent model, and certainly has implications for the provider community. For example, a consent model with protocols to restrict information access based on a specific set of use cases, and / or that requires express patient consent to access sensitive information, might be perceived as creating undue bureaucratic barriers to obtaining important clinical information. Many entities address this issue by instituting a "break the glass" provision, which typically allows providers to access any available medical information in unexpected and / or an emergency situation. However, these provisions do not guarantee rapid access, as some exchanges require special codes or processes to gain access to the information.

Provider Organizations

Like individual clinicians, provider organizations want to minimize the administrative, financial and technical burdens imposed by consent requirements and generally share the concerns outlined above. Their workflow concerns, however, are compounded, as any consent requirement would need to be applied consistently across the entire organization, not just by discrete providers or business units, and account for a larger patient population. Experience from HIPAA implementation shows that upfront capital costs for training staff, implementing new patient consent procedures, and changing workflow processes to ensure compliance can increase along with the size of the provider organization.[114] Likewise, estimates of the cost of implementing a national health information exchange are highest among the largest provider organizations.[115] Large provider organizations therefore hold a key position in both developing and implementing interoperable health information exchange.

Professional organizations such as the American Medical Association and the American College of Physicians generally have supported the adoption of HIT with strong privacy protections, and wish to see systems developed in such a way that preserves patient choice by encouraging active

[111] Wang, J.C. et al. "Perceptions of standards-based electronic prescribing systems as implemented in outpatient primary care: a physician survey," *Journal of the American Medical Informatics Association*, Vol. 16, No. 4, July/August 2009, pp. 493-502.
[112] Hersh, *supra* note 109.
[113] ARRA, Pub. L. No. 111-5, § 4101(a), 123 Stat. 115, 267-277 (2009) (codified at 42 U.S.C.A. § 1395w-4 (West 2009)).
[114] Kilbridge, P. "The Cost of HIPAA Compliance," *New England Journal of Medicine*, Vol. 348, No. 15, April 10, 2003, pp. 1423-24.
[115] Kaushal, R. et al. "The Costs of a National Health Information Network," *Annals of Internal Medicine*, Vol. 143, No. 3, August, 2005, pp. 165-173, at 170-72.

communication between providers and their patients. These groups also have expressed a preference for unencumbered physician access to all available patient medical data, with the noted exception of certain categories of sensitive data, such as psychiatric notes.[116] Because large provider organizations are often highly visible in the community and typically provide care to medically and culturally diverse populations, having access to accurate records and building patient confidence in the health care system are viewed as important goals, particularly given the high costs associated with implementation. Further, to the extent that electronic exchange itself might represent a revenue enhancement opportunity for a provider organization, bolster its reputation within the community, and / or help facilitate research or other partnerships, volume and completeness of data likely would be important elements. For these reasons, provider organizations might have an additional interest in implementing low-resistance consent models (*e.g.*, *opt-out*) to ensure the adequacy of the data for those purposes.

Payer Organizations

Payer organizations, as well as the employers that constitute their client base, are increasingly engaging in health care quality improvement efforts, and are appealing directly to members to use tools (*e.g.*, personal health records (PHRs)) and participate in disease management initiatives to support their overall health. In this context, it seems reasonable that payers generally want access to clinical and other information that could be of use in these efforts, and therefore would want to ensure maximum participation in and sharing of data. Ultimately, payers hope to realize the benefits of electronic exchange through reductions in their own expenditures. For these reasons, as discussed in the section on provider interests above, payers generally would prefer low-resistance consent models that yield high participation and data volume.[117]

A final consideration is that many payers are investing significantly in the development of electronic exchange, and often make claims data available to organizational participants.[118] It is therefore understandable that they would not want consent restrictions to prevent them from realizing any anticipated benefits of these ventures.

HIOs

Electronic exchange organization leaders want to ensure that any consent policies and procedures adopted permit the entities to provide valuable services, fulfill their mission to the community of participants, evolve over time, and remain financially viable. As such, HIOs share many of the same concerns as their provider participants regarding administrative burden, particularly to the extent that it could limit the use and utility of the enterprise as a whole.

An additional layer of complexity is that much of the infrastructure supporting the consent process is oftentimes the responsibility of the exchange entity itself. For example, most state-led exchanges rely on the HIO to build and maintain the intelligence infrastructure that manages and monitors consent, including data capture, the application of decision rules for appropriate access,

---

[116] American Medical Association. "Improving Communication-Improving Care," *The Ethical Force Program*, 2006, at 56-58. Available at: http://www.mihealthandsafety.org/pdfs/06-improving-communication1.pdf; American College of Physicians, *Health Information Technology and Privacy – Position Paper*, 2009, at 7-9. Available at: http://www.acponline.org/advocacy/where_we_stand/health_information_technology/acphit.pdf.

[117] HISPC. *Final Report of the Interstate Disclosure and Patient Consent Requirements Collaborative*, March 31, 2009, at ES1-ES2.

[118] *Id.*

the authentication of eligible providers to the system, etc. For this reason, less complicated consent policies and procedures are generally preferred. And, to the extent that an HIO may need to coordinate policies with others or comply with those of other organizations, there is also concern that they will be unable to accommodate downstream operations.

HIOs also may want to allow for flexibility, as they may need to accommodate a range of consent preferences as dictated by their participating provider organizations. Such flexibility is evidenced in many existing exchanges (*e.g.*, CareSpark and NY entities), in that participating provider organizations have the latitude to engage in consent procedures that exceed the baseline requirements of the HIO (*e.g.*, they can obtain express patient consent if that is preferred).[119]

Policy Makers

Finally, policy makers at all levels who are tasked with supporting the development of electronic exchange face the key challenge of making decisions despite the fact that they will not be able to address simultaneously the needs and concerns of all of the multiple and diverse stakeholders. Policy makers must envision the end goals of electronic exchange (*e.g.*, better health and health care quality, improved public health reporting, more engaged patients) and develop consent and other policy guidelines that are most likely to yield the desired results without compromising privacy or alienating key partners. In this respect, there is possibly no single consent model that is more likely to appeal to policy makers—all of the models require tradeoffs and depend on the particular interests and needs of the affected stakeholders.

Ethical and Cultural Considerations

Individual Choice and Public Good

Policy decisions regarding how and to what extent patients exercise control over the electronic exchange of their health information have been discussed at times as representing the degree to which patient privacy and autonomy are preserved in a networked health environment. Autonomy is the ethical principle underlying an individual's right to make and carry out informed decisions that arise from unbiased and thoughtful deliberation. Self-determination is the derivative of autonomy most commonly associated with informed consent and health care, pursuant to which an autonomous agent who understands the relevant facts and can engage in practical reasoning freely makes decisions.[120] As both clinical and research medicine traditionally have relied upon informed consent to further these ethical principles in practice, the proper role of informed consent in electronic information sharing has been widely discussed in recent years.

It has been suggested that an individual's participation in electronic exchange should be thought of as a type of medical intervention in which "one needs to balance the benefits of using the systems with the potential risks to the patient."[121] While a consent model that allows for greater patient control over his or her medical records (such as an *opt-in with restrictions* model) may

[119] Phone call with Liesa Jenkins, *supra* note 34; Phone call with Ellen Flink, *supra* note 40.
[120] King, J.S. and B.W. Moulton, "Rethinking Informed Consent: The Case for Shared Medical Decision-Making," *American Journal of Law and Medicine*, Vol. 32, No. 4, October, 2006, pp. 429-501, at 435.
[121] Berner, E.S. "Ethical and Legal Issues in the Use of Health Information Technology to Improve Patient Safety," *HEC Forum*, Vol. 20, No. 3, September 2008, pp. 243-58, at 244.

provide more choice to the individual patient, there is considerable uncertainty as to whether access to a range of choices ultimately satisfies the health interests of the individual patient and, more broadly, undermines the utility of the exchange for both the patient and society. In addition, it has been argued that over-reliance on consent could lead to "consent fatigue," where patients presented with too many complex consent forms unknowingly agree to uses and disclosures of their health information.[122] The concern is that a system that relies on consent alone to maintain patient choice and privacy paradoxically may subvert these goals by shifting the focus away from true autonomous choice and toward a legally binding, but ethically questionable, process that consists primarily of the mere signing of forms.

Many groups, including the Center for Democracy and Technology (CDT) and the Markle Foundation, instead have recommended integrating individual control and consent into a robust framework of legal, technical, and policy rules organized to protect the privacy and security of data within an electronic exchange.[123] Within this paradigm, they suggest that individuals should be informed about and agree with how their health information is being collected and used, but not rely on consent alone to bear the full weight of privacy protection.[124] Many of the HIOs reviewed in this paper, including DHIN, the New York exchanges, and RIQI, have built such frameworks into their exchange policies; relevant state laws that support such infrastructure have been developed as well. In the absence of well-defined infrastructure, however, an entity's choice of consent model may take on more importance for the individual as providing the sole or one of a few vehicles for ensuring adequate data controls and protections.

One important but confounding challenge in discussing consent's role in electronic exchange is taking into account the benefits that it promises on a societal scale. Encouraging individuals to seek care in the first instance by promising confidentiality helps fulfill the societal goal of having a healthy population. While electronic exchange has the potential to advance such societal goods as population health and clinical research, this effect diminishes as fewer patients participate and less data are available. These uses of health data promise benefits for both the individual and society, but their potential ultimately depends on the extent to which such data are made available for these purposes. Eike-Henner Kluge notes that, from an ethical perspective, those who wish to benefit from HIT (including any quality improvement within the health care system as a whole) but do not participate in the system constitute "free riders."[125] While it does not necessarily follow that participation in electronic exchange should be mandatory, the overall costs and benefits to all participants must be considered in deciding consent's proper role in electronic exchange. It has been noted that, at least in our current health care system, the

[122] Center for Democracy and Technology. "Rethinking the Role of Consent in Protected Health Information Privacy," January 2009, at 10. Available at: http://www.cdt.org/healthprivacy/20090126Consent.pdf.
[123] *Id.* at 21-22; Center for Democracy and Technology, "Beyond Consumer Consent: Why we Need a Comprehensive Approach to Privacy in a Networked World," *Markle Foundation*, February 2008 [hereinafter "Beyond Consumer Consent"]. Available at: http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.
[124] Center for Democracy and Technology. "Beyond Consumer Consent," *supra* note 123.
[125] Kluge, E.H. "Security and Privacy of EHR Systems-Ethical, Social and Legal Requirements," *Studies in Health Technology and Informatics*, Vol. 10, Issue 7, July 2008, pp. 495-99, at 497.

individual, as opposed to society as a whole, bears the primary risks associated with the improper use and disclosure of information, such as losing employment or insurance.[126]

Ultimately, striking a balance between enabling autonomy and patient choice and achieving socially fair and legally valid standards for medical data use and electronic exchange recalls the foundations of the doctrine of informed consent itself—meeting legal and professional standards of informed consent does not always fulfill the ethical obligation of maintaining patient autonomy. As health information becomes more complex and widely available, our societal challenge is to develop consent rules and procedures within HIT that honor the goal of autonomous choice while simultaneously acknowledging considerations of clinical efficacy, resource restrictions, and the greater social good.[127]

Consent in the Privacy Context

Many of the concerns surrounding patient choice and privacy in the HIT context are, in a sense, extensions of reservations patients currently have regarding their medical records. It is estimated that one in six Americans engage in "privacy-protective behavior" due to concerns over unwanted disclosures of their medical data, with higher rates among those who are in poor health and ethnic and racial minorities.[128] Surveys have also shown that the majority of Americans are "very concerned" about identity theft or fraud (80 percent), the use of their medical information for marketing purposes (77 percent), and that their data might become available to employers or insurance companies (56 and 55 percent, respectively).[129] At the same time, 89 percent of respondents say that they want their physicians to be able to communicate with one another,[130] while the majority support the development of HIT as a whole and believe that it will improve care and reduce costs.[131] Furthermore, while consumer opinion regarding unrestricted access to even de-identified health data for research purposes is not positive, the vast majority of respondents are supportive of such research provided that consent is sought beforehand.[132]

While there seems to be general agreement among the experts we interviewed that patients should have some control over their electronic data and its uses, the ideal reach of that control is less clear. *Opt-in* or *opt-out* consent frameworks could meet these goals, but within those broad areas, policy makers and system developers must design specific sets of choice options. A model that allows for individual control over each data element might compromise clinical efficiency. Many proposed and existing electronic exchange systems therefore choose granularity options based upon different parameters, such as provider type or time-stamp, or eliminate granularity altogether. Even the most ardent supporters of consent acknowledge that

---

[126] *See* Pritts, J. "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. Available at: http://www.iom.edu/Activities/Research /HIPAAandResearch.aspx.

[127] Goldstein, M.M. "Health Information Technology and the Idea of Informed Consent," *Journal of Law, Medicine, and Ethics*, Vol. 38, No. 1, pp. 27-35.

[128] McGraw, D., *supra* note 16, at 5.

[129] McGraw, D. et al. "Privacy as an enabler, Not an Impediment: Building Trust Into Health Information Exchange," *Health Affairs*, Vol. 28, No. 2, March 2009, at 417.

[130] *Id.*

[131] Schneider, *supra* note 15, at 5.

[132] 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, at 2. Available at: http://www.ncvhs.hhs.gov/080220lt.pdf.

policy makers legitimately may take account of what is fair and reasonable to require of health care professionals in protecting autonomy.[133]

Successful electronic exchange systems engage consumers, physicians and other stakeholders at an early stage to ensure that choice is integrated into the architecture of the systems. The MAeHC illustrates this approach. Using an *opt-in* system without granularity, MAeHC achieved an average of 90 percent participation in its three pilot communities (granularity was not an option, in part because only a limited set of data was included in the exchange). This high level of participation was attributed to several factors, including early and ongoing community participation in the formation of the Collaborative, the use of marketing materials that underscored the benefits of the exchange to both patients and providers, and a high level of support among physicians, which in turn fostered greater patient trust.[134] Conversely, as discussed in greater detail in Appendix C, the nationwide Dutch EHR system encountered significant difficulty in achieving wide participation despite the high level of choice allowed by the system, which was attributed to a lack of consumer understanding of both their privacy options and the quality improvement goals of the system as a whole.[135] Many privacy advocates point to these experiences to support their arguments that individual patient participation and control are key enablers for successful electronic exchange.[136]

Electronic exchange systems that utilize *opt-in* or *opt-out* choice models that allow for some level of granularity generally are considered more protective of patient choice and privacy than those that do not provide granularity of choice. What health information is included, how and to what degree patients can choose who sees their data, and how these standards are upheld in law are critical questions to be addressed by any entity in advance of engaging in electronic exchange. Early involvement of consumers in the planning of these systems will help to build trust as well as ensure that patients have a degree of choice that encourages participation and upholds privacy standards while meeting the clinical goals of improved quality and efficiency.

Human Factors

Particularly in the U.S., where individual freedom and choice are highly valued, a common perception is that more choice is always better than less. Studies have shown, however, that while people may prefer to choose from as many alternatives as possible, decision-making ability is compromised when too many choices are offered.[137] One prominent study that documented this effect involved an offer of free jam samples at a supermarket in California.[138] Researchers alternated between showing two different sample displays in the same store—one that included

[133] T. Beauchamp and J. F. Childress. *Principles of Biomedical Ethics*, 6th ed. (New York: Oxford University Press, 2008): at 107.
[134] Tripathi, *supra* note 43, at 443-43.
[135] Laurens J. van Baardewijk. "Electronic Health Record in the Netherlands: Afraid of the Unknown." *Amsterdam Law Forum*, August 2009, at 42.
[136] Peel, *supra* note 11, at 3.
[137] 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).
[138] Iyengar, *supra* note 137, at 996.

six samples of jam and another that included 24 samples of jam. Although a larger percentage of people walking past the display stopped when it contained 24 samples, only three percent of these people eventually purchased one of the jams. Conversely, 30 percent of people who sampled from the display with six choices eventually bought jam. The researchers 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.[139] They also concluded 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. People are more likely to avoid this perceived time and effort barrier in favor of entrusting the choice to someone else, choosing randomly, or avoiding the choice altogether.[140]

This body of evidence should be taken into account when considering the array of policy approaches that could be established to manage consent in an electronic exchange, particularly those involving greater granularity. 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.[141] In a "perfect" choice environment, patients would have the time, interest, and incentives to learn about and consider a variety of factors for each opt-in and opt-out choice placed on their "menu" of options. As discussed above, it is important for patients to understand the full context of their decisions, including the benefits of having their information in the electronic exchange as well as any associated risk to their privacy.[142]

The method used to obtain consent can also affect human decision making. If consent is obtained at a medical institution, for example, patients may limit their deliberations based on how much time they think they have before an appointment or how much time they think they will have with their physicians. This could result in a quick "checking of the boxes," or a complete opt in or opt out rather than the exercise of true choice.[143] Further, both the complexity of the information shared and the way in which a choice is framed may affect a patient's ability to make a decision.[144] Each factor increases the magnitude of the "too much choice" effect and has its own impact on the decision. People sometimes have trouble comprehending information regarding unfamiliar subjects.[145] Moreover, a choice can seem complicated for a number of reasons, including hard-to-follow explanations and elaborate presentations. As a result of the perceived complexity of decisions in the health care context, patients may become more inclined to trust their providers' judgments.[146] In the electronic exchange context in particular, patients

---

[139] *Id.* at 1004.
[140] *Id.*
[141] HISPC. *Guidance for Developing Consent Policies for Health IT*, March 31, 2009. Available at: http://www.oregon.gov/OHPPR/HISPC/Docs/CEE_OM_Consent_Policies.pdf.
[142] NCVHS, *supra* note 132.
[143] Ram, N. "Tiered Consent and the Tyranny of Choice," *Jurimetrics*, Vol. 48, No. 3, November 3, 2008, pp. 253-84.
[144] Lee, B. and W. Lee. "The Effect of Information Overload on Consumer Choice Quality in an On-Line Environment," *Psychology and Marketing*, Vol. 21, No. 3, March 2004, pp. 159-183, at 160; Tversky, A. and D. Kahneman. "The Framing of Decision and the Psychology of Choice," *Science*, Vol. 211, No. 4481, pp. 453-58.
[145] Faden, R.R. and T.L. Beauchamp. *A History and Theory of Informed Consent* (New York: Oxford University Press, 1986): at 323.
[146] *Id.* at 319-20.

presented with several information sharing options might feel pressure to defer to their providers' suggestions rather than completely evaluate the privacy and confidentiality risks of information exposure. If being given more choice adds to complexity, patients might also understand less about their options.

The provision of opt-out notices in the retail banking industry presents a good case study for examining the challenges associated with the presentation of complex choice information to consumers. In 1999, Congress passed the Gramm-Leech-Bliley Act, which mandated that financial institutions give consumers an opportunity to opt out of having their information disclosed to nonaffiliated third parties.[147] According to the statute, a financial institution must "clearly and conspicuously" explain its policies regarding disclosure to third parties, and inform consumers of the opportunity to opt out.[148] When the first notices were sent, however, consumer groups complained that they were hard to understand and sometimes misleading.[149] The American Bankers Association estimated that only five percent of consumers exercised their opt-out option in the years immediately following implementation of the Act.[150] This low participation could partially be explained by a tendency to throw out mail but, according to a telephone survey, two-thirds of consumers claimed to have read the disclosure notices.[151]

In response to consumer pressure, Congress modified the Gramm-Leech-Bliley Act in 2006 to mandate that the FTC create a model form for banks to use that would be "comprehensible to consumers, with a clear format and design."[152] The FTC has conducted several studies to determine the best way to disclose information practices and explain the opportunity to opt out. One of the problems these studies tackled was the reading level of the notices in response to analyses by privacy rights groups that estimated that the average notice was written at the level of a college junior or senior.[153] In response to this and other criticisms, the FTC developed a model notice that is only two to three pages in length and presents key information in a table format.[154] A study that compared the table format to the notice previously used found that people reading the table notice were more likely to identify correctly which banks share more information than others as well as both the substance and quality of their opt-out provisions.[155] The FTC, in conjunction with several other agencies, promulgated a final rule in November 2009 with model notice guidelines and a "safe harbor" provision for all financial institutions who decide to switch to the table format.[156]

This case study demonstrates some of the challenges (*e.g.*, clear and audience-appropriate presentation of information) associated with enabling consent. In the electronic exchange

---

[147] 15 U.S.C. § 6802 (2006).
[148] 15 U.S.C. § 6802(1)(A).
[149] Lee, W.A. "Opt-Out Notices Give No One a Thrill," *American Banker*, Vol. 166, No. 131, July 10, 2001.
[150] *Id.*
[151] *Id.*
[152] 15 U.S.C. § 6802(e)(2)(A).
[153] Lee, *supra* note 149.
[154] Levy, A. and M. Hastak. *Consumer Comprehension of Financial Privacy Notices*: *Submission to Interagency Notice Project*, December 15, 2008. Available at: http://www.ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf.
[155] *Id.* at 9.
[156] Federal Trade Commission Press Release. *Federal Regulators Issues Final Model Privacy Notice Form*, November 17, 2009. Available at: http://www.ftc.gov/opa/2009/11/glb.shtm.

context, a consent process that fails to convey benefits and risks as well as the terms and conditions of participation could have serious and / or undesirable consequences. Ideally, a consent process for electronic exchange would invite participants to make an informed decision by avoiding unnecessary complexity, clearly and concisely explaining the utility of the exchange, and making transparent the terms and conditions for participation.

Process, Logistical and Technical Considerations in Obtaining and Managing Consent

Any electronic exchange – regardless of scale or approach – needs to determine how and by what means it intends to execute its selected consent model. This plan involves consideration of numerous process, logistical and technical issues that affect, often differentially, the various stakeholders participating in the exchange. Approaches that are preferred by one group may impose additional process or workflow requirements on another (or have more significant financial implications) and there are some approaches that may seem reasonable from a policy perspective but are not always technically feasible. The following discussion highlights some of these challenges and tradeoffs by examining the process, logistical, and technical implications of the various choice models with respect to **who** participates in the consent discussion and **how** consent is obtained and managed.

Who Obtains and Manages Consent

Electronic exchanges vary greatly with respect to the actors they designate to assume the role of obtaining and managing patient consent. In general, consent can be obtained and managed by the individual practitioner or provider organization, or by the coordinating HIO or by all of the above. Most entities have distributed responsibility for obtaining and managing consent between these two groups. The entity coordinating exchange efforts in the State of New York, for example, allows for consent to be obtained either directly through the exchange entity, or by a health care provider at the point of care. The MAeHC in Massachusetts distributes responsibilities in a different fashion, making the provider responsible for informing the patient of the exchange and for obtaining express consent, but assigning responsibility for storage, management, and maintenance with the governance entity.[157]

It is also possible to place responsibility for both obtaining and managing consent on the HIO itself. One advantage of this approach is that it has the potential to ensure greater uniformity of implementation across participating providers in a more efficient manner. This approach has been implemented by the DHIN in Delaware, which, as a default, automatically includes all patients in the state as participants.

Regardless of how these roles are divided, models that require express patient consent for participation in electronic exchange tend to impose greater workflow burdens on whatever entity is designated as having either full or joint responsibility for obtaining and managing consent. Any model that provides a level of patient choice – either to opt in or out – requires planning and execution regarding some basic functions. In obtaining consent, these typically include tasks associated with:

1. Establishing policies and procedures to guide the consent process;

[157] Tripathi, *supra* note 43.

2. Educating both patients (about the exchange) and providers (about their responsibilities with respect to consent management);
3. Developing methods and materials to support the education process; and
4. Developing methods and materials to obtain actual consent.

An example on the less prescriptive end of the spectrum regarding these requirements is DHIN, which requires providers to make available (but not systematically present to patients) some level of education about both the exchange and the *opt-out* procedure. DHIN offers providers talking points, sample privacy language, and confidentiality forms to help them educate patients, but does not require the exercise as a condition of participation. Furthermore, the management infrastructure function is performed by DHIN directly, so the level of effort expended by providers on the consent process is minimal. Conversely, Rhode Island has engaged RIQI to train staff in participating provider and other organizations (including ambulatory and inpatient care settings, employers, community-based organizations, and long-term care facilities) on how to help patients through the consent process. This process involves helping patients to complete an enrollment and consent form and, if the patients wish to restrict access to only certain provider organizations, making available a telephone hotline through which patients can indicate their provider preferences.

If the responsibility of performing these tasks falls on individual providers or provider organizations, workflow and resource issues likely will emerge. Research has shown that, when providers are tasked with additional responsibilities absent training, incentives, and / or adequate time to adapt or modify their work processes, they either "work around" such impositions or quit.[158] Likewise, asking busy providers to devote additional time to the collection and / or tracking of myriad consent directives may call for resources that are not available, which could lead to complete noncompliance, or a failure to uphold consent policies and procedures adequately. Past experience with HIPAA implementation has shown that training providers and educating patients on new privacy policies can be costly and time-consuming.[159] This issue is more pronounced in *opt-in* or other "high touch" consent models, as the sheer volume of work required is greater. For this reason, the Department of Health and Human Services in Rhode Island has agreed to pay a one-time, three-dollar authentication[160] fee for every participant enrolled in that state's exchange.

If these tasks are largely delegated to HIOs, additional challenges emerge. Specifically, HIOs tasked with obtaining consent in an *opt-in* model, for example, likely would require significant resources (human and otherwise) to reach out to and secure participation of patients in their community. Given that these entities do not have an existing relationship or the opportunity to interface directly with patients, they would have to expend considerable time and effort to generate the level of patient participation necessary to make the exchange valuable to providers and other participating organizations. It is likely for this reason that every exchange evaluated as part of this review relies on the provider community to assume some role in the consent process.

---

[158] Berner, *supra* note 121, at 247-48.
[159] Arora, R. and M. Pimetel. "Cost of Privacy: A HIPAA Perspective." *Privacy Policy, Law and Technology*, December 9, 2005, at 9.
[160] This is referred to as an "authentication fee," as it is intended to cover the provider's effort associated with validating the identity of the patient for purposes of participation in the exchange.

An entirely distinct and often even more complicated and resource-intensive component of consent management is the "back end" work, which involves maintaining and enforcing the consent directives already obtained and applied. This process is rarely the responsibility of individual providers or even provider organizations unless they serve as coordinating entities for the exchange. Most often, an HIO develops functionality that enables it to:

1. Authenticate the identities of patients in the exchange;
2. Apply the consent directive appropriately to the identified patients;
3. Monitor / audit access to records via the exchange in order to validate appropriate management; and
4. Facilitate provider access (consistent with consent preferences) to information available through the exchange.

The technical complexity and resource implications of these tasks can vary substantially depending on the type of consent model in place. Again, those allowing for more patient choice are perceived as being more challenging to implement.

A complicating factor in this arena is that many of the HIT systems already in place or in the process of being adopted lack the technical capacity to support many of the consent model approaches fully—specifically those involving granularity of choice by data type or source. This fact reinforces the notion that provider organizations are not well positioned to serve as the managers of consent. The HIT systems used by most providers have been designed to organize information for care delivery and administrative functions. These systems typically do not offer users, for example, the option of organizing the information in the record by source (*e.g.*, mental health provider or obstetrician) or of easily sequestering information that is deemed by an individual patient to be inappropriate for sharing (particularly if it is acceptable to the patient to share the information with some participants, but not others). As such, providers likely would have to develop or alter existing (though not standardized or harmonized) systems of decision rules for identifying and segmenting information on multiple patients, and then manage that information accordingly. Individual providers might well perceive this process as complicated and a serious interference with practice workflow. Implementation across multiple parties involved in an exchange would present the additional challenge of requiring every participating organization first to use products that allow for the extraction of structured data, and then to apply a similar set of standards and definitions. However, as long as EHR data from different providers is structured, even if structured differently, the use of common terminology within the HIO could make sharing among different systems feasible. In this case, participating organizations would need to work collectively to map their systems' terminology to that of the HIO, which would require a fair amount of time and effort on the part of the organizations.[161]

Despite these workflow and resource issues identified with *opt-in* consent models, there remain some distinct advantages that may render such tasks worth the effort, at least at the front end of obtaining consent. The MAeHC noted in a review, for example, that their *opt-in* implementation

[150] Phone conversation with Ioana Singureanu, Eversolve, L.L.C., March 10, 2010.

strategy, which involved explicit communication between patients and providers, contributed significantly to the high level of participation and community trust.[162]

A potential alternative to either provider-based or exchange-based consent directives is the use of a third party as a type of "consent broker." This option is discussed in more depth below.

How Consent is Obtained and Managed

In addition to deciding who in the health care system should assume primary responsibility for the consent management process, electronic exchanges also need to address the issue of how, or by what means, consent will be obtained. At present, paper is the most common medium for recording consent preferences, but the process is usually precipitated by an in-person consultation or telephone interaction. This simple method of obtaining consent for exchange has several advantages. It is inexpensive in the short term and can also serve as physical evidence. As noted in Appendix A, Delaware, Maryland, Virginia and Tennessee all currently offer patients the option of opting out of the state's electronic exchange by submitting a paper form.[163] Though not yet operational, CRISP in the State of Maryland includes all patients in the exchange as a default, but intends to allow them to opt out by calling a toll-free phone number. As Maryland requires a second level of consent to enable information to be accessed via the exchange, CRISP has determined that patients also will be able to enroll at this level either via phone or direct contact with a provider at the point of care.

If an HIO applies a choice model that requires obtaining consent for electronic exchange, it will also need to record patient consent preferences to ensure that it continues to adhere to the patient's wishes. In order for the directive to be searchable and actionable for other parties, however, the information captured needs to be made available through a shared utility designed to support the needs and responsibilities of participating organizations. If a patient decides to opt out of an exchange, for example, and there is no electronic record of that preference, then other participating providers would not be able to act accordingly. In addition, paper forms can be lost easily and are more cumbersome to share. Although a paper form may be an appropriate method of obtaining consent when one provider wishes to transfer electronic information directly to another, or for a patient to use in opting out of an exchange system completely, it is less so when serving as a directive to all participants within an electronic exchange or beyond.

In response to concerns associated with maintaining patient consent preferences in paper form, technology companies and policy makers are beginning to support electronic methods of obtaining consent. This approach is already being applied by numerous providers when seeking informed consent for medical procedures. For example, providers at VA centers in Atlanta and Los Angeles have used computer software that helps to explain the risks and benefits of a particular procedure and captures the patient's consent within the system.[164] When accompanied by clear communication with the provider, the process could both facilitate patient understanding of the procedure and make it easier for the provider to keep track of the consent.[165]

---

[162] Tripathi, *supra* note 43, at 441.
[163] *See* Appendix A.
[164] Spotswood, S. "VA Patient Consent Goes Electronic," *U.S. Medicine Information Central*, February 2005.
[165] *Id.*

Similar technology has been proposed to allow patients to create an electronic file expressing their preferences concerning electronic exchange. Patients could create the file by using software that guides them through a series of consent preferences in fixed categories. The software could be associated either with the patient's EHR (for individual providers or a specific exchange entity) or the patient's PHR. Once recorded, the data could be used in at least three different ways: 1) the responsibility could be placed on the health care provider to adhere to the patient's consent preferences when using and sharing information; 2) the system could actively require health care providers to signify that they understood a patient's preferences prior to accessing the information, and / or 3) the system could act as a gatekeeper and permit only certain individuals to access information.[166] The first of these alternatives might not be suitable for electronic exchanges that apply a granular consent model because of the variety of transactions such an entity might need to undertake to comply with patient preferences. However, it could be more suitable to systems that call for simple electronic exchange between providers, as electronic consent records could guide the provider in deciding what information to share. E-consent systems that require provider certifications of understanding and that act as gatekeepers might be suitable for an electronic exchange employing granular consent, but likely would require the use of software to keep track of and enforce a patient's consent preferences.

E-consent systems might also employ the use of "consent directives," which are records "of a health care consumer's privacy policy, which is in accordance with governing jurisdictional and organization privacy policies that grant or withhold consent [to one or more defined entities based on consumer preferences]."[167] The Healthcare Information Technology Standards Panel (HITSP), for example, has created standards for a "manage consent directives transaction package" for HIT developers to follow in creating individual software applications. In order to meet the HITSP standards, the consent directive package may allow users to create, store, amend, and replace a consumer preference; transmit the preference electronically; allow for individual providers and other exchange participants to view the preference; apply the preference to an individual health record; transmit an update of the preference; reconcile conflicting preferences; maintain an audit log of the preference; and classify data.[168]

HITSP has also described the components necessary to create such a system and how they would interact. First, a "content creator" would allow the patient or the designated entity to input the consent directive electronically. The patient could provide his / her directive in paper form, as long as designated staff could then input the form into a "content creator"—a user-friendly computer program designed to ask for and accept data. Alternatively, the patient could be instructed to use the "content creator" form as a form of e-consent.[169] A "consent directive management system" would then acknowledge the creation of a directive and forward the directive to a "consent repository," which would check for inconsistencies with existing consent

[166] Coiera, E and Clarke, R.C. "e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment," *Journal of American Medical Informatics Association*, Vol. 11, No. 2, March/April 2004, pp. 129-40, at 132-3.
[167] *HITSP Manage Consent Directives Transaction Package, Version 1.3*. July 8, 2009, at 5. Available at: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=30.
[168] HHS-ONC. *Consumer Preferences Draft Requirements Document*, October 5, 2009, at 34. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10779_891071_0_0_18/20091005_Consumer%20Preferences_Draft_Requirements_Document.pdf.
[169] *HITSP*, *supra* note 167, at 10.

directives from the patient. A "consent registry," after confirming the security of the message, would update the directive.[170]

Currently, the HITSP protocol is not widely implemented and it is unclear how the guidelines for electronic consent directives would affect provider and other exchange entity workflow. Systems that have already obtained some form of consent from patients might need to obtain new consent or input the preferences obtained from all of their patients into the new system.[171] Another concern is the issue of whether a consent directive system could be developed to recognize and enforce state and federal laws and regulations pertaining to medical record access. Since privacy rules, such as those promulgated pursuant to HIPAA, are designed to govern people as opposed to information systems, it might be difficult for companies to develop a system that adheres to the nuances of these laws and regulations. [172] However, the idea of using a "consent directive" is attractive because it promotes interoperability by creating a mechanism by which directives can be maintained to avoid potential scenarios of conflicting patient preferences.

An electronic exchange could also rely on a patient's PHR to act as an e-consent directive for the exchange in at least three different ways.[173] First, a provider or other designated entity could view a PHR directly based on the preferences expressed by the patient. This method would be most analogous to the way the social media interface, Facebook, works, as entities could only view all or parts of the PHR according to the patient's expressed privacy choices. In the second method, a PHR could be connected directly or "tethered" to an EHR maintained by a provider or other entity. The patient's PHR consent preferences would be exchanged directly with the EHR and would apply to both the information offered by the patient and the information stored in the EHR. Finally, patient preferences expressed in a PHR could be connected to an exchange system and shared with multiple providers. Some enthusiasm exists for the PHR system of e-consent because of the relative success of "" in offering specific, granular privacy options, and the desire of patients to have direct control of their personal health information. Microsoft HealthVault, a PHR system, offers similar granular permission options to patients in some circumstances. Generally, patients have such options when sharing data with other users of HealthVault, but not when sharing through third-party applications. In the latter case, users of the system are notified in advance exactly which data elements will be shared with the third-party system.[174] This policy responds to the reluctance of some providers to support PHRs and patient control of data because they worry that patient interaction with health records could lead to the introduction of inaccurate data or the withholding of important information for treatment purposes. However, if a PHR acts simply as a pathway for patients to view health information in provider EHRs and a method for patients to input exchange preferences, providers' concerns tend to be mitigated.

---

[170] *Id.*
[171] SLHIE. *Coordinating Policies that Impact the Access, Use, and Control of Health Information, Final Report, Part II*, March 2008, at 15. Available at: http://www.slhie.org/wp-content/uploads/2009/12/SLHIE_Final_Report_Part11.11.pdf.
[172] Coiera, *supra* note 166, at 130.
[173] HHS-ONC, *supra* note 168, at 34.
[174] Phone conversation with Kathleen Connor, Principal Program Manager, Microsoft HealthVault, March 11, 2010.

There are additional drawbacks to using a PHR system to obtain consent. For example, such systems place much of the onus for information management directly on the patient—potentially without necessary support. Patients have to access the internet and take the time to record and update their consent preferences, likely requiring some level of training. One criticism of the "" system is that its default privacy settings allow extensive sharing of a person's profile information without providing consumers adequate instruction concerning those settings.[175] To prevent a PHR system from facing similar criticism, patients would need clear instruction regarding their available privacy settings and the consequences of failing to opt out, if that choice is available. Alternatively, a default setting that requires patients to opt in if they want to share their information would provide a conservative option for ensuring that their preferences are followed. Another concern in the PHR context is user authentication, as some systems allow patients to grant various levels of access or custodial rights to anyone they choose. Critics are concerned that a PHR system without stringent authentication requirements could be compromised by both malicious users and unintended errors by those granted access.

One final and related issue is the durability of consent—that is, the period of time a consent directive applies before it requires updating or re-confirmation by the patient. Requiring patients to give consent multiple times can be both beneficial and detrimental to electronic exchange. Despite education efforts, when a patient grants consent, he or she may not comprehend every situation to which it will apply. In addition, as a patient's medical status changes, he or she might wish to amend consent preferences, but not think to do so unless prompted. For this reason, some electronic exchanges require patients to renew their consent or specify how long it should last.[176] However, if a patient has already expressed his or her generalized preferences, requiring repeated consent discussions at each new provider visit might be considered unnecessary, and could increase the likelihood of conflicting directives.

LEGAL FRAMEWORK

Federal Law

HIPAA

A. *Elements of the Privacy Rule*

One of the central pieces of federal law that protects health information privacy is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides for the promulgation of privacy regulations (the HIPAA Privacy Rule). The HIPAA Privacy Rule sets forth rules governing the use and disclosure of protected health information (PHI) by "covered entities," defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with a covered transaction, such as submitting a health care claim to a health plan.[177] PHI is defined as "individually identifiable health information" that is held or transmitted by a covered entity in any form, including

[175] Conn, J. "Patient consent and 'granular' privacy control," *ModernHealthCare*, December 14, 2009. Available at: http://www.modernhealthcare.com/article/20091214/REG/312149987.
[176] For examples of this process, *see* description of Sweden model in Appendix C ; and discussion of Rhode Island model in "Durability of Consent" under "State-Led Examples of Exchange in the U.S."
[177] 45 C.F.R. § 160.103 (2009).

electronic, paper, and oral media, subject to certain limited exceptions (such as the exclusion of employment records).[178]

Pursuant to the Privacy Rule, covered entities may not use or disclose PHI except as permitted or required.[179] Covered entities are required to provide a patient's own PHI to the patient or to the patient's representative, and must disclose PHI as requested by the Secretary of the U.S. Department of Health and Human Services (HHS) for audit or other enforcement purposes.[180] All other disclosures pursuant to the law, including those that may be required by other federal or state laws, are considered "permitted," that is, allowed under the Privacy Rule."[181] In addition, covered entities are required by HIPAA to develop public privacy policies stating when and under what circumstances they disclose PHI.[182]

The Privacy Rule requires an "authorization" for uses and disclosures of PHI not otherwise permitted or required.[183] An "authorization" is a detailed document defined by the Rule that gives covered entities permission to use PHI for specified purposes. The requirements of a valid authorization are stringent. For example, a valid authorization must specify certain details (*e.g.*, a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed).[184] In addition, a valid authorization must contain an expiration date or specify an expiration event that relates to the individual or the purpose of the use or disclosure,[185] and must be written in "plain language."[186]

The Privacy Rule permits covered entities to use and disclose PHI without written patient authorization for purposes related to treatment, payment, and health care operations.[187] On the other hand, HIPAA permits, but does not require, a covered entity to seek patient *consent* for uses and disclosures of PHI for those purposes, but does not explicitly define consent or specify the necessary content of a consent form or the process by which an entity should obtain consent. HHS guidance, however, defines the term as written permission from individuals to use and disclose their PHI for treatment, payment, and health care operations.[188]

---

[178] 45 C.F.R. § 160.103.
[179] 45 C.F.R. § 164.502(a).
[180] 45 C.F.R. § 164.502(a)(2).
[181] A list of permitted disclosures may be found at 45 C.F.R. § 164.502(a)(1).
[182] 45 C.F.R. § 164.520.
[183] 45 C.F.R. § 164.508(a). Uses and disclosures requiring authorization include the use of PHI for marketing purposes; 45 C.F.R. § 164.508(a)(3); and the use and disclosure of psychotherapy notes (except to carry out certain treatment, payment, or health care operations). 45 C.F.R. § 164.508(a)(2).
[184] 45 C.F.R. § 164.508(c)(1).
[185] 45 C.F.R. § 164.508(c)(1)(v).
[186] 45 C.F.R. § 164.508(c)(3).
[187] 45 C.F.R. § 164.506(a).
[188] Office for Civil Rights, U.S. Dept. of Health and Human Services. "Summary of Privacy Rule," 2003, at 5. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

When the Privacy Rule requires an authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI.[189] In most cases, a covered entity may not withhold treatment or payment if a patient declines to authorize the particular use or disclosure.[190] Other disclosures permitted without patient authorization include, for example, disclosures for certain public health and research activities,[191] and for quality reporting purposes with respect to FDA-regulated products.[192]

In analyzing individual choice models in electronic exchange, it is therefore important to consider the *purpose* of the exchange of information. Because of the exceptions in the Privacy Rule, a HIPAA covered entity that exchanges PHI through an exchange entity for the purposes of treatment, payment, health care operations, or public health activities, for example, would not be required to obtain patient authorization pursuant to the law. However, if an entity exchanges PHI for a purpose that would require patient authorization under the Privacy Rule, such as disclosures for marketing purposes,[193] it may need to design its practices to allow for methods of transmitting such authorizations through the exchange (*e.g.*, so that a covered entity that receives a request through the exchange for the purpose of marketing has documentation that it is authorized to disclose the PHI).

B. *Implications for Individual Choice Models*

HIPAA provides a baseline standard of privacy protection for health information. State laws that offer more stringent privacy protections are allowed by the Privacy Rule,[194] and a considerable body of privacy law at the state level currently exists.[195] As a result, an entity's decision regarding potential individual choice models will likely be affected by state privacy laws. 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.[196] In addition, ARRA amends HIPAA by expanding its reach, strengthening certain aspects of the regulations, and increasing federal enforcement tools.[197] Regulations implementing ARRA's provisions are currently being promulgated, some of which will affect individual choice models in the context of electronic exchange.

Certain elements of the Privacy Rule hold particular relevance for analyzing individual choice models. Because HIPAA has applied only to "covered entities" as defined in the statute, some of the new entities being created to store, handle, or manage electronic personal health information,

---

[189] Office for Civil Rights, U.S. Dept. of Health and Human Services. "What Is the Difference Between 'Consent" and "Authorization' Under the HIPAA Privacy Rule?" 2003. Available at: http://www.hhs.gov/ocr/privacy/hipaa/faq/use/264.html.
[190] 45 C.F.R. § 164.508(b)(4).
[191] 45 C.F.R. § 164.512(b)(i).
[192] 45 C.F.R. § 164.512(b)(iii).
[193] 45 C.F.R. § 164.508(a)(3).
[194] 45 C.F.R. § 160.203.
[195] 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.
[196] McGraw, *supra* note 16.
[197] American Recovery and Reinvestment Act (ARRA), Pub. L. No. 111-5, §§ 13101-13424, 123 Stat. 115, 228-279 (2009).

such as health record banks, have not been directly covered by the Privacy Rule.[198] However, ARRA has clarified that organizations that provide data transmission of PHI to a covered entity (or its business associate) and require routine access to PHI are business associates as contemplated by HIPAA and must enter into business associate contracts with the covered entity.[199] As a result, exchange entities that meet this description will likely need to execute business associate agreements with the various covered entities involved in their exchange if they have not already done so. Additionally, ARRA provides that certain provisions of the HIPAA Privacy and Security Rules will be directly applicable to business associates (in contrast to previous requirements, under HIPAA, in which business associates were only governed by the business associates agreements).[200] In the near term, ARRA's clarification of the business associate status of these organizations and change in business associate liability may increase their contracting and administration responsibilities.

Further, ARRA requires the Secretary of HHS to conduct a study and submit a report to Congress on recommended privacy and security requirements for entities that are not currently covered under HIPAA.[201] As it has been debated whether ARRA's interpretation of the business associate provision as it applies to exchange entities that transmit and require routine access to PHI includes consumer-facing HIT tools used in health record banks or created by internet companies such as Microsoft, Google, and WebMD, it is possible that the Secretary's study will include such tools in its area of focus.

The Privacy Rule's minimum necessary requirement also holds particular relevance for an entity's selection of individual choice model. 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.[202] However, the requirement does not apply to disclosures or requests by a health care provider for treatment purposes, or to disclosures to the individual who is the subject of the information.[203] The purpose of an entity's information exchange therefore is critical to the entity's compliance with the minimum necessary requirement. If an entity exchanges information for treatment purposes only, its operations would align well with the requirement. However, if the entity exchanges PHI for purposes more accurately described as payment or health care operations, such transactions would need to be addressed to ensure compliance.

Finally, a particular provision in ARRA may affect an entity's decision regarding choice models in that it gives individuals the right to request that providers restrict the disclosure of their PHI to health plans for the purpose of carrying out payment or health care operations. Under HIPAA, choosing to honor such a request was voluntary;[204] compliance is now mandatory if the PHI pertains to a health care item or treatment for which the patient paid out-of-pocket in full and if

[198] McGraw, *supra* note 16, at 7.
[199] ARRA § 13408, 123 Stat. 115, 271 (codified at 42 U.S.C.A. § 17938 (2010)). Pursuant to HIPAA, "business associates" are entities that perform activities on behalf of, or provide certain services to, covered entities that involve the use or disclosure of individually identifiable health information. 45 C.F.R § 160.103 (2009).
[200] ARRA §§ 13401, 13404, 123 Stat at 260, 264 (codified at 42 U.S.C.A. §§ 17931, 17934 (2010)).
[201] ARRA § 13424(b), 123 Stat. at 277 (codified at 42 U.S.C.A. § 17953 (2010)).
[202] 45 C.F.R. § 164.502(b) (2009).
[203] 45 C.F.R. § 164.502(b).
[204] 45 C.F.R. § 164.522(a).

disclosure is not otherwise required by law.[205] The provision does not apply to disclosures for treatment purposes or to de-identified information. Thus, for example, if an individual paid cash for treatment of a sexually transmitted disease, he or she could prohibit disclosure for payment or health care operations purposes but could not restrict disclosures linked to treatment. In order to comply with this provision, an exchange could limit the purpose of its effort to treatment only, or could restrict the entities eligible to receive information through the exchange to health care providers. Alternatively, an exchange could apply a segmentation mechanism by which a person's information could be exchanged for treatment purposes, but not for payment or health care operations purposes, if he / she so desired and paid for the treatment out-of-pocket in full.

GINA

The Genetic Information Nondiscrimination Act of 2008 (GINA) generally prohibits employers and health insurers from discriminating on the basis of an individual's genetic information.[206] GINA has two titles: Title I affects group health plans and health insurance, while Title II applies in the employment context.[207] Title I prevents group health plans and health insurers from adjusting group premiums based on genetic information, prohibits the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental insurance markets, and limits the ability of group health plans, health insurance issuers, and Medicare supplemental insurers to collect genetic information or to request or require that individuals undergo genetic testing.[208] Title II strictly limits an employer's right to request, require, or purchase an employee's genetic information.[209] 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.[210]

Pursuant to GINA, interim final rules were recently issued that provide steps for insurers to follow to ensure that they do not collect genetic information that could be used in underwriting.[211] In addition, the Office for Civil Rights at HHS issued proposed regulations that would modify the HIPAA Privacy Rule provisions relating to the use and disclosure of genetic information.[212] If adopted as issued, the proposed rule would revise HIPAA's definition of "health information" explicitly to include genetic information; add a definition of "genetic information" to the Privacy Rule consistent with GINA's statutory definition; and prohibit the use and disclosure of genetic information by HIPAA covered entities for eligibility

[205] ARRA § 13405, 123 Stat. at 264-265 (to be codified at 42 U.S.C. § 17935).
[206] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (codified in scattered sections of 26 U.S.C.A, 29 U.S.C.A, and 42 U.S.C.A.).
[207] GINA §§ 101-213, 122 Stat. 881, 883-920.
[208] §§ 101-106, 122 Stat. at 883-905.
[209] §§ 201-213, 122 Stat. at 905-920 (codified at 42 U.S.C.A. §§ 2000ff-2000ff-10 (West 2009)).
[210] §§ 201-213, 122 Stat. at 905-920.
[211] The Internal Revenue Service, the Employee Benefits Security Administration, and the Centers for Medicare & Medicaid Services recently issued an interim final rule implementing the health insurance provisions of GINA. Interim Final Rules Prohibiting Discrimination Based on Genetic Information in Health Insurance Coverage and Group Health Plans, 74 Fed. Reg. 51,664 (Oct. 7, 2009) (to be codified at 26 C.F.R. pt. 54, 29 C.F.R. pt. 2590, and 45 C.F.R. pts. 144, 146, 148).
[212] HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information, 74 Fed. Reg. 51,698 (proposed Oct. 7, 2009) (to be codified at 45 C.F.R. pts. 160, 164).

determinations, premium computations, and any other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.[213]

As GINA prevents health insurers and employers from requesting or obtaining an individual's genetic information,[214] the law has important policy and technical implications for the types of data an electronic exchange might choose to include, its decisions regarding what entities will have access to the data, and its decision to use a particular individual choice model. In addition, GINA defines "genetic information" as information about an individual's genetic tests, as well as the genetic tests of an individual's family members or the manifestation of a disease or disorder in an individual's family members.[215] As a result, GINA prevents employers and health insurers from using family medical histories in employment and insurance decisions, in addition to genetic information about the individual.[216] If an electronic exchange chooses to include genetic information, it therefore might need to be capable of sequestering not only an individual's genetic information, but also the genetic information and medical history of an individual's family members. This ability would be necessary to prevent the disclosure to and use of genetic information by health insurers and / or employers, but still allow its disclosure to and use by treating physicians. In practice, even if an electronic exchange were able to segment data in this fashion, it is likely that organizations will choose, at least in the near term, either to omit genetic information from their exchange practices, or exclude health insurers and / or employers from the exchange entirely in order to study developments in the legal doctrine and ensure compliance with the law.

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

In the early 1970's, Congress passed legislation intended to encourage individuals to seek treatment for substance abuse. As part of this effort, the federal legislation included provisions that protect the confidentiality of persons who seek or obtain substance abuse education or treatment in federally assisted programs.[217] Pursuant to the statutes, federal regulations were promulgated to protect the identities of persons in alcohol or drug abuse treatment programs,[218] reflecting the view that: "Every patient and former patient must be assured that his right to privacy will be protected. Without that assurance, fear of public disclosure of drug abuse or of records that will attach for life will discourage thousands from seeking the treatment they must have if this tragic national problem is to be overcome."[219] In keeping with this view, Part 2 strictly limits the allowable disclosure and use of information about individuals in federally

[213] HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information, 74 Fed. Reg. at 51,700. Press Release, U.S. Dept. of Health and Human Services, New Rules Protect Patients' Genetic Information (Oct. 1, 2009), *available at* http://www.hhs.gov/news/press/2009pres/10/20091001b.html.
[214] GINA §§ 102, 203, 122 Stat. at 894, 908-909 (codified at 42 U.S.C.A. §§ 300gg-1, 2000ff-2 (West 2009)).
[215] GINA § 201, 122 Stat. at 906 (codified at 42 U.S.C.A. § 2000ff(4) (West 2009)).
[216] Office for Human Research Protections, U.S. Dep't 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.
[217] 42 U.S.C. § 290dd-2 (2006).
[218] 42 C.F.R. Part 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).
[219] H. REP. NO. 92-775, at 24 (1972), *reprinted in* 1972 U.S.C.C.A.N. 2045, 2072.

assisted alcohol or drug abuse treatment programs.[220] Any and all information obtained by such a program that could reasonably be used to identify an individual who seeks or obtains education or treatment is protected under Part 2, and all permissible disclosures are limited to information necessary to carry out the purpose of the disclosure.[221] The regulations do not protect a patient's identity *per se*, but rather his or her identity as a participant in or applicant for substance abuse treatment.[222]

Part 2 defines disclosure as a communication or verification of an individual's patient identifying information.[223] "Patient identifying information" includes names, addresses, Social Security numbers, fingerprints, photographs, or similar information by which the identity of a patient can be determined.[224] The requirements to protect information under Part 2 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.[225] "Diagnosis" includes any reference to an individual's alcohol or drug abuse or to a condition that is identified as having been caused by that abuse, [226] including psychological or social work assessment or evaluation. Treatment therefore might include counseling as well as medical care. A federally assisted program could be a freestanding program or a program that is part of a larger organization—for example, a detoxification unit in a general hospital or a substance abuse clinic in a county mental health department.[227]

Nearly all disclosures allowed under Part 2 require specific patient consent, and a patient consent form must contain certain required elements to be valid pursuant to the law.[228] However, Part 2 does include certain provisions and exceptions where disclosure is allowed without patient consent.[229] These include communications within a program or between a program and an entity having direct administrative control over that program (*e.g.*, the staff of a detoxification unit within a hospital can share information with hospital administrators where the sharing is needed to provide substance abuse services to the program's patients). In addition, communications are allowed between a program and a qualified service organization (a person or entity that provides services such as data processing, bill collection, or accounting to a program).[230] Part 2 also allows disclosure without patient consent in strictly defined circumstances for medical emergencies;[231] audit or evaluation activities;[232] and scientific research purposes.[233]

---

[220] 42 C.F.R. § 2.3(a).
[221] 42 C.F.R. §§ 2.11, 2.13(a).
[222] *See* Lopez, F. "Confidentiality of Patient Records for Alcohol and Other Drug Treatment," in *U.S. Department of Health & Human Services Pub No. (SMA) 95-3018, Center for Substance Abuse Treatment Technical Assistance Publication Series 13, Ch. 1*, 1994. Available at: http://www.treatment.org/TAPS/TAP13/tap13chap1.html.
[223] 42 C.F.R. § 2.11.
[224] 42 C.F.R. § 2.11.
[225] 42 C.F.R. § 2.11.
[226] 42 C.F.R. § 2.11.
[227] 42 C.F.R. §§ 2.11, 2.12(e)(1).
[228] 42 C.F.R. § 2.32.
[229] 42 C.F.R. § 2.12.
[230] 42 C.F.R. §§ 2.11, 2.12.
[231] 42 C.F.R. § 2.51.
[232] 42 C.F.R. § 2.53.
[233] 42 C.F.R. § 2.52.

The fact that patient identifying information may be disclosed pursuant to one of the exceptions to the general rule does not mean that the disclosed information is no longer protected by the regulations. 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.[234]

Like HIPAA, Part 2 sets a federal privacy floor. Where state laws are less protective regarding disclosure and use of information about individuals in federally assisted alcohol or drug abuse treatment programs, Part 2 is operative, and where state laws are more stringent state laws are preserved.[235] Overall, the vast majority of states essentially have adopted Part 2 as the standard for protecting this type of health information.[236]

Our discussions with experts interviewed for this paper indicated that, in the area of electronic exchange, Part 2 presents challenges in the development of policies and practices for information sharing, particularly in the areas of patient consent and granularity of choice. Although the regulations do allow information sharing under narrow circumstances, and therefore would allow an electronic exchange some operational leeway,[237] many entities perceive the policies and technical requirements that would need to be developed as prohibitively complicated. Because Part 2 generally requires written patient consent for the disclosure of patient-identifying information that specifies, *inter alia*, the purpose of the disclosure, who is to receive the information, and a date or condition upon which the consent expires, an exchange would be required to develop a means of ensuring and documenting such consent as well as the capability of managing this type of information in order to comply with the law.[238] According to the experts we interviewed, it therefore is possible that data covered by Part 2 – or provider institutions likely to contribute such data – will be excluded from some exchange operations.

In addition, the experts whom we interviewed suggested that the common co-occurrence of alcohol and drug abuse with mental illness, and the increasing availability of dual diagnosis treatment programs, might result in mental health diagnosis and treatment that indirectly falls within the restrictions of Part 2. In practice, for example, it could be difficult to confirm that a patient treated in a dual diagnosis program is receiving certain medications for depression or bipolar spectrum disorder, the exchange of which information might otherwise be acceptable according to federal and state law, but separate other parts of the patient's diagnosis or treatment for separate consent procedures. As a result, it is possible that the law could be interpreted by some to require the segmentation of some, but not all, mental health information within EHRs.

---

[234] 42 C.F.R. § 2.32.
[235] 42 C.F.R. § 2.20.
[236] Pritts, *supra* note 22, at 3-1, 3-13.
[237] *See* Beckerman et al. "Health Information Privacy, Patient Safety, and Health Care Quality: Issues and Challenges in the Context of Treatment for Mental Health and Substance Use," *BNA's Health Care Policy Report*, January 14, 2008, at 1, 9.
[238] We note that similar issues are raised by state health information disclosure laws that require consent for the disclosure of other types of health information.

State Laws

Federal privacy and confidentiality laws do not apply to every entity that holds health information. HIPAA applies only to covered entities,[239] while GINA's restrictions apply to group health plans, health insurers, and employers.[240] The privacy protections in Part 2 apply only to the disclosure and use of patient records relating to alcohol and substance abuse diagnosis and treatment that are maintained in connection with alcohol and substance abuse programs that receive federal assistance.[241] Because these laws do not preempt state laws that provide protection that is equal to or greater than their standards, state laws related to electronic exchange are highly relevant to the various choice models.

State privacy and confidentiality laws widely vary. In 2009, the Interstate Disclosure and Patient Consent Requirements Collaborative published its final report as part of the Health Information Security and Privacy Collaboration (HISPC). According to the report, states vary greatly in their requirements for consent and disclosure related to PHI in various electronic exchange scenarios.[242] The type of information required in the consent process varies from state to state,[243] as does each state's interpretation of seemingly similar statutory language.[244] Some state statutes demonstrate a high degree of complexity when addressing consent and disclosure of PHI (evidenced by statutes featuring multiple exceptions and detailed descriptions of what types of PHI are covered by the statute), while other state laws are relatively unsophisticated.[245] In sum, states differ greatly in the way their statutes address PHI types, PHI holders, PHI receivers, different treatment scenarios, consent processes and forms, and requirements for HIPAA's minimum necessary standard.[246] The differences in state laws have resulted in a range of "consent cultures" across the country that defines the context for electronic exchange.[247] The lack of uniformity is often viewed as one of the most complex challenges of implementing electronic exchange.

A review of various state laws also reveals that states are moving at different rates when it comes to implementing statewide electronic exchange programs and addressing related legal barriers to electronic exchange.[248] Some states have laws that specifically facilitate electronic exchange, while others have laws originally intended for a paper-based system.[249] Many states also have

---

[239] 45 C.F.R. § 160.103.
[240] GINA §§ 201-213, 122 Stat. at 905-920 (codified at 42 U.S.C.A. §§ 2000ff-2000ff-10 (West 2009)).
[241] 42 C.F.R. § 2.3.
[242] HISPC, *supra* note 117, at 3-2. The widest variation among state statutes appears in state approaches to consent or other disclosure requirements for the release of PHI to a health care provider for non-emergency treatment purposes. Less variation exists in state laws with regard to requirements for the disclosure of PHI in an emergency, though the definition of "emergency" varies from state to state. *See also* Purington, *supra* note 10, at 2.
[243] HISPC, *supra* note 117, at 3-7.
[244] *Id.* at 3-6.
[245] *Id.*
[246] *Id.* at 3-8-3-10. Because each state defines terms differently, comparison across state laws becomes somewhat challenging. For example, one state may define "health care provider" to include pharmacists, while another may not. Pritts, J. et al. "The State of Health Privacy: A Comprehensive Survey of State Health Privacy Statutes, August 8, 1999. Available at: https://www.gushare.georgetown.edu/jlp/1999%20State%20Report/State%20Report%201999.pdf.
[247] *Id.* at 4-1.
[248] *Id.*
[249] *Id.*

organized state-level electronic exchange initiatives by statute.[250] The following examples provide a snapshot of the wide variety of state legislation related to electronic exchange, consent and disclosure requirements, and preferences for particular choice models.

Select State Examples – (See Appendix B)[251]
One of the most common types of state legislation related to electronic exchange is a law facilitating the creation and design of a statewide HIO. Indiana, Delaware, Maryland and Rhode Island, among others, have all enacted legislation recently that enables the development of a statewide HIO.[252] In addition to creating statewide HIOs, some of these laws also address privacy issues. Indiana's legislation for example, specifies that Indiana's electronic exchange must comply with HIPAA.[253] Similarly, the statute creating DHIN mandates that patient-specific health information shall be disclosed only in accordance with the patient's consent or best interest to those having a need to know.[254]

With regard to individual consent models, many states have laws that specify the model(s) their electronic exchange will use. A Delaware law, for example, specifies that patients shall be informed of and may choose to preclude a search of their individual health information in the DHIN after consultation with their health care provider—in other words, patients are able to opt out of the query function in the DHIN system.[255] Legislation in Rhode Island provides that participation in the state's HIO will be governed by an *opt-in* system,[256] while a Wisconsin law establishes a *no consent* system for the exchange of certain types of health information.[257] Specifically, Wisconsin law allows diagnostic test results (including laboratory data, EKGs, and radiology reports) to be exchanged without the informed consent of the patient.[258] Previously, Wisconsin law had only allowed certain elements of a patient's treatment record (including a patient's demographic information, diagnosis, medications, and allergies) to be released without consent to health care providers in a "related health care entity." To facilitate electronic exchange, the new Wisconsin law allows these data, as well as diagnostic test results and symptoms, to be shared without patient consent with any health care provider involved in a patient's care.[259]

Interestingly, some states that do not currently have a working electronic exchange system nevertheless have laws related to electronic exchange. A law in Nevada, for example, which does not have any form of a statewide HIO, allows individuals to opt out of the electronic transmission of individually identifiable health information, with exceptions for Medicaid and

[250] See references to Rhode Island, Maryland and Indiana under State Led Examples of Exchange in the U.S.
[251] For a comprehensive review of state law requirements for patient permission to disclose health information, *see* Pritts, *supra* note 22.
[252] *See* IND. CODE ANN. § 5-31-3-1 (West 2009); DEL. CODE ANN. tit. 16, §§ 9920-22 (2010); MD. CODE ANN., HEALTH – GEN. § 19-143 (West 2009); Rhode Island Health Information Exchange Act of 2008, R.I. GEN. LAWS §§ 5-37.7-1 through 5-37.7-15 (2009).
[253] IND. CODE ANN. § 5-31-6-3.
[254] DEL. CODE ANN. tit. 16, § 9926.
[255] 1-100-102 DEL. CODE REGS. §§ 1.0-8.0.
[256] R.I. GEN. LAWS § 5-37.7-4.
[257] WIS. STAT. ANN. § 146.82 (West 2010).
[258] WIS. STAT. ANN. § 146.82.
[259] WIS. STAT. ANN. § 146.82.

SCHIP patients or when required by HIPAA or state law.[260] In addition, the Nevada legislation exempts HIPAA covered entities that transmit individually identifiable health information electronically in compliance with HIPAA provisions from compliance with more stringent state privacy and confidentiality laws.[261]

New York, in particular, has extensive legislation on privacy and disclosure related to electronic exchange. Section 18 of New York's Public Health Law requires that hospitals, physicians, other health care providers, and HMOs obtain written consent before disclosing personal health information for non-emergency treatment.[262] This law has been interpreted within the state as being more protective than HIPAA, as it requires patient consent even for treatment, payment, and health care operations.[263] New York courts analyzing section 18 have interpreted the law to require any individual, including a government official, who possesses medical records to keep those records confidential and not to release them to third parties without proper authorizations.[264]

New York law also establishes consequences for the misuse of health information. Under the New York Education Law, it is professional misconduct for a physician to reveal "personally identifiable facts, data or information" to a third party without patient consent.[265] The New York State Department of Health has emphasized that a provider's disclosure of records without patient consent could lead to violations under the Education Law,[266] and the New York Codes, Rules and Regulations further clarify that licensed professionals are prohibited from revealing personally identifying information obtained in a professional capacity without the prior consent of the patient, except as authorized by law.[267]

Like New York, Rhode Island has a significant body of law related to electronic exchange. The Rhode Island Health Information Exchange Act of 2008 establishes a statewide HIO and security measures that will ensure patients are aware of the exchange and have given permission to share their data.[268] The law specifies that the HIO is voluntary for both providers and patients and notes that patients have the right to terminate their participation in the HIO.[269] In addition, the law provides that patients will be able to obtain reports of what health information has been shared and who accessed it, as well as notices of security breaches.[270] Another Rhode Island law, enacted one year after the Rhode Island Health Information Exchange Act, specifies that the

---

[260] NEV. REV. STAT. § 439.538 (2007).
[261] NEV. REV. STAT. § 439.538. The Nevada statute's application to genetic information has been questioned due to the fact that the state's statutory provision addressing genetic information does not expressly incorporate 439.538, while its provisions that address mental health and substance abuse do. *See* Pritts, J., *supra* note 22.
[262] N.Y. PUB. HEALTH LAW § 18 (McKinney 2010).
[263] New York State Department of Health, *Letter to Dr. Alan Lambert*, October 14, 2003.
[264] *Grosso v. Town of Clarkstown*, No. 94 Civ. 7722(JGK), 1998 WL 566814, at *8 (S.D.N.Y. Sept. 3, 1998); *Caraveo v. Nielson Media Research, Inc., et al.*, No. 01 Civ. 9609 LBSRLE, 2003 WL 169767 (S.D.N.Y. Jan. 22, 2003).
[265] N.Y. EDUC. LAW § 6530(23) (McKinney 2010).
[266] New York State Department of Health, *Letter to Dr. Alan Lambert*, October 14, 2003.
[267] N.Y. COMP. CODES R. & REGS. tit. 8, § 29.1 (2009).
[268] R.I. GEN. LAWS § 5-37.7-4 (2009).
[269] R.I. GEN. LAWS § 5-37.7-10.
[270] R.I. GEN. LAWS § 5-37.7-10.

state's HIO will be *opt-in*.[271] In addition, the law lists situations when consent is not required for the disclosure of health information. For example, consent is not required for the release of health information to public health authorities for a specified function, to health care providers for diagnosis or treatment in an emergency, and to the organization for operation and administrative oversight of the HIO.[272]

Finally, electronic exchange legislation in some states includes enforcement clauses for the misuse of health information. As described above, New York's Education Law makes it professional misconduct for a physician to reveal personally identifiable facts, data or information to a third party without consent.[273] In Delaware, state legislation specifies that any misuse of DHIN health information or data must be reported to the state Office of the Attorney General, and that violators will be subject to prosecution and penalties under the Delaware Criminal Code or federal law.[274]

IMPACT OF MODELS

Patient Participation

Many patients want high levels of privacy and autonomy as participants in electronic exchange. Experience in the Massachusetts pilot program and other state-level exchanges demonstrates that *opt-in* models have the capacity to yield high consumer participation rates, but that this achievement requires a tremendous level of awareness and trust building, as well as education. It also requires the establishment of multiple options for accommodating preferences with respect to a consent management process. That said, such models provide great opportunity for patient engagement and the building of community trust.

When MAeHC needed to select a consent model, policy makers interviewed consumer groups to gather feedback on privacy and consent options.[275] The groups strongly favored an *opt-in* model, and were concerned that an *opt-out* approach would result in patients inadvertently opening up their medical information to security risks without their awareness.[276] Based in part on this feedback from consumers, the MAeHC developers selected an *opt-in* approach for their electronic exchange. Since the program's inception, patient participation rates have been extremely high—as of March 2009, more than 90 percent of patients had chosen to opt in and participate in the MAeHC system.[277] It should be noted, however, that the success of the approach in Massachusetts may be due in part to the relative scale of the effort. The MAeHC facilitates electronic exchange for three communities, which is less ambitious than many state-wide efforts.

---

[271] R.I. GEN. LAWS § 5-37.7-4.
[272] R.I. GEN. LAWS § 5-37.7-7. These consent requirements apply to the release of health information held within the exchange only. Information held in locations other than the exchange is subject to Rhode Island's general law regarding the confidentiality of health care information, which states that consent is not required for the release of confidential health information for treatment, payment, operations or in an emergency. R.I. GEN. LAWS § 5-37.3-4.
[273] N.Y. EDUC. LAW § 6530(23) (McKinney 2010).
[274] DEL. CODE ANN. tit. 16, § 9926 (2010).
[275] Tripathi, *supra* note 43, at 439.
[276] *Id.*
[277] *Id.* at 441.

To help it achieve high patient participation rates, MAeHC utilized the services of a professional marketing firm. Before the MAeHC exchange launched, focus groups identified the issues of greatest concern for patients, which included privacy, convenience, ease of use, and cost.[278] Marketing efforts were then directed toward working with and through providers, as it was widely recognized that patients are not likely to trust a system unless their physicians do as well.[279] Finally, consent for participation in MAeHC was designed to be obtained through a provider, which had the effect of building a relationship of trust and reassuring the patient that his / her information was secure.[280] All of these strategies proved effective in increasing patient participation in the MAeHC exchange.

Although MAeHC does not inquire about patients' reasons for not participating in the exchange, anecdotal reports from providers suggest that privacy concerns were a factor for some patients.[281] Another group that did not opt in to the MAeHC exchange consisted of patients who received their primary care services outside of the community and therefore felt that it was not worth the risk to make their information available via the exchange.[282] This experience suggests that, although it may require additional resources and effort, it is possible to engage a large number of patients in an exchange effort that relies on consent models that offer patients at least some degree of choice.

Given patient preferences for adequate privacy protections and some level of control with respect to how their health information is used and exchanged, it follows that consumers might generally prefer *opt-in* over *opt-out* models. As a rough guideline, the amount of information that is shared in an electronic exchange is inversely proportional to patient participation.[283] However, researchers have found that default policies, which can be either *opt-in* or *opt-out*, influence behavior in crucial ways.[284] Specifically, patients may believe that defaults are suggestions by the policy maker, and thus may be reluctant to deviate from what they perceive to be the recommended action.[285] For example, patients in an *opt-out* exchange may believe that the governmental or organizational entity responsible for the exchange strongly recommends participation. This belief could make patients more reluctant to opt out of the exchange and deviate from the status quo, which could help to explain, at least in part, why patient participation rates in *opt-out* models can be high. In the DHIN, for example, not a single patient has chosen to opt out of the system,[286] resulting in a 100 percent statewide patient participation rate.[287]

Research on human behavior has revealed some important explanations for why *opt-out* models might yield high levels of consumer participation. One reason is simply inertia—making the

[278] *Id.* at 437-38.
[279] *Id.* at 441.
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*
[284] Johnson, E.J. and D. Goldstein. "Do Defaults Save Lives?" *Science*, Vol. 302, November 21, 2003, pp. 1338-339.
[285] *Id.*
[286] Phone call with Sarah Matthews, *supra* note 23.
[287] *Id.*

decision to opt out requires effort, whereas accepting the default is effortless.[288] In difficult and stressful situations, many people choose to avoid decision making altogether and accept the status quo. In a study in which respondents were asked whether they would be organ donors on the basis of various conditions (*opt-in*, *opt-out*, *no prior default*), about twice as many participants elected to donate organs in the *opt-out* condition compared to those in the *opt-in* condition.[289] Researchers have also compared rates of organ donation in European countries with different default options (*opt-in* or *opt-out*) and found that the four *opt-in* countries studied had lower organ donation rates than the six *opt-out* countries.[290] Additionally, a systematic review of the literature on the impact of consent models on participation rates in observational health research found that *opt-out* consent models generally resulted in significantly higher participation rates than *opt-in* models.[291] These studies demonstrate that, even in situations where the stakes for participating in a program are high, rates of patient participation can be high in *opt-out* regimes.

Provider Participation

As discussed above, there are two primary drivers to provider participation in electronic exchange: 1) the requirements of participation cannot be too onerous; and 2) the value that providers get from the exchange must more than offset the additional process and other burdens associated with their participation. In essence, provider participation in an electronic exchange must be worth their while.

Because providers value access to complete clinical information,[292] they typically prefer a consent model that allows for the exchange of the most complete and comprehensive health information. The more comprehensive the data, the more useful it is to providers in making decisions about patient care, and the quicker such decisions can be made.[293] Because *opt-out* models usually give providers access to health information for a larger number of patients than *opt-in* models, it is likely that many providers would favor this type of consent model.

The DHIN query system, an example of an *opt-out* model, has achieved high levels of participation among Delaware health care providers.[294] To date, more than half of providers in Delaware (60 percent) use DHIN, while more than 85 percent of the state's laboratory transactions and more than 80 percent of hospitalizations in Delaware are reported in DHIN.[295]

While most providers generally view greater access to clinical information as a benefit, some have expressed concern regarding participation in electronic exchange efforts because of the perception that their liability risks could increase due to the potentially greater availability of

[288] Johnson, *supra* note 284.
[289] *Id.*
[290] *Id.*
[291] El Emam, K. et al. "A Globally Optimal k-Anonymity Method for the De-Identification of Health Data." *Journal of the American Medical Informatics Association,* Vol. 16, pp. 670-82, at Appendix A, p. 11.
[292] See section regarding provider preferences under Stakeholders Perspectives.
[293] Tang, P.C. et al. "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," *Journal of the American Medical Informatics Association*, Vol. 13, No. 2, March 2006, pp. 121-6, at 123.
[294] Phone call with Sarah Matthews, *supra* note 23.
[295] *Id.*

patient health information.[296] For example, during the selection of a consent model for Maryland's CRISP exchange, some participating providers were concerned over liability, particularly as it relates to breaches of privacy laws and medical malpractice.[297] Specifically, providers wondered whether having more information available in a patient's medical history would change the standard of care applicable in the medical malpractice context. Questions surfaced as to whether, with more information at their fingertips, they would be held to a higher standard for reviewing and considering all available information in making care decisions.[298] Thus far, attempts to evaluate the impact of electronic exchange of health information on providers' medical malpractice liability have found insufficient legal basis on which to make conclusions.[299] The legal landscape in this area will continue to evolve, however, and is likely to incorporate advances in technology slowly into the standard of care.[300]

Clinical Care

It is widely believed that the ability to exchange health information electronically will lead to a number of improvements in health care.[301] Such improvements include increasing the ability of providers to make better clinical decisions based on more complete patient information, increasing providers' ability to access vital patient records immediately in the event of an emergency, decreasing the number of patient tests that need to be repeated because the original results cannot be located on a timely basis, and lowering the risk of negative drug interactions because physicians are not aware of a patient's current medications.[302] In a recent GAO report that explored the impact of electronic exchange on quality of care, providers participating in an exchange reported a positive impact on patient care and having more timely and comprehensive patient information available. Through the use of electronic exchange, one provider reported that the receipt of patient alerts enabled timelier interventions. Similarly, providers in a large hospital emergency room were able to access critical medical information about patients, thereby avoiding numerous adverse drug interactions.[303] Although these benefits likely could be realized with the implementation of any consent model, some model types might require more effort to achieve the same level of impact.

Opt-in models force patients to be active participants in their health care. This element is advantageous, because research has shown that when patients are more engaged in their health care, they have better treatment outcomes.[304] On the other hand, consent models that allow for the exchange of large amounts of health information, such as *opt-out* models, have been shown

---

[296] CRISP Health. *Policy Formulation: A Plan for Statewide Health Information Exchange in Maryland*, February 2009. Available at: http://www.crisphealth.org/LinkClick.aspx?fileticket=aoitbKG2sSg%3D&tabid=75.
[297] *Id.*
[298] *Id.*
[299] 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.
[300] *Id.*, at 91.
[301] Markle Foundation. *Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy*, February 2005, at 4. Available at: http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.
[302] *Id.*
[303] GAO. Electronic Personal Health Information Exchange: Health Care Entities' Reported Disclosure Practices and Effects on Quality of Care, GAO-10-361 (Washington, D.C.: February 2010), at 19, 21.
[304] Tang, *supra* note 293, at 124.

to improve continuity of care and communication between patients and providers.[305] This increased communication leads to greater trust between patients and providers, often resulting in improvements in clinical care.

Although utilization of electronic exchange should lead to improvements in clinical care, reliance on EHRs in the clinical setting could, in fact, have unintended negative consequences. The more information that is available to a clinician via an electronic exchange, the greater the risk that a rushed physician may actually engage in fewer conversations with patients, and / or could cut and paste large blocks of text or notes from other physicians into a patient's record to save time.[306]

Whatever type of consent model is selected, it is vital to all stakeholders that the quality of patient care does not decline. In a survey of the members of the California Privacy and Security Advisory Board's Health Information Exchange Committee, 72 percent of members strongly agreed that the consent approach chosen by the committee should not impact the quality of care.[307] One reason given for this view was that the treatment of the patient is more important than the patient's individual privacy rights.[308] Although protecting patient privacy and autonomy through consent models is a worthy goal, many argue that it must not be achieved at the cost of diminished clinical care.

Quality Improvement, Public Health, and Other Research

A major benefit to implementing a nationwide system of electronic exchange is that health information could be gathered for quality improvement, public health, and research purposes. In order to achieve quality improvement, one must have access to measurable information captured from thousands of transactions.[309] In that respect an *opt-out* model may be preferable to its *opt-in* counterpart, as it likely will include clinical information for a larger percentage of the patient population.

Best practices are discovered based on analysis of entire populations. Using data mined from databases of vital signs, images, laboratory values, medications, diseases, interventions, and patient demographic information, analysts can create guidelines for care in a more effective manner than by using, for example, a roundtable discussion of experts or a limited evidence base.[310] For example, a health exchange examined in the recent GAO report merges data from hospitals, laboratories, providers and health plans to develop metrics related to preventive care and chronic disease management as part of a quality improvement program designed to assist providers in adhering to evidence-based practices.[311] An electronic exchange model that allows for the exchange of a wide variety of clinical information (*e.g.*, laboratory data, radiology

---

[305] *Id.* at 123.
[306] Hartzband, P. and J. Groopman. "Off the Record – Avoiding the Pitfalls of Going Electronic," *New England Journal of Medicine*, Vol. 358, No. 16, April 17, 2008, pp. 1656-658, at 1656.
[307] California Health and Human Services Agency. *CalPSAB HIE Committee Consent Survey Results*, September 14, 2009. Available at: http://www.ohi.ca.gov/calohi/PSAB/HIECommittee.aspx.
[308] *Id.*
[309] D'Avolio, L. W. "Electronic Medical Records at a Crossroads: Impetus for Change or Missed Opportunity?" *JAMA*, Vol. 302, No. 10, September 9, 2009, pp. 1109-11, at 1110.
[310] *Id.* at 1110.
[311] GAO, *supra* note 303, at 20.

reports, medication history, etc.) will be the most useful in collecting data for quality improvement purposes.

According to the National Committee on Vital and Health Statistics (NCVHS), EHRs must be designed with quality reporting requirements in mind in order to produce comparative quality data effectively.[312] Currently, the lack of standard definitions for quality measurements and their underlying data elements is a barrier to the effective use of reporting initiatives.[313] To be useful for quality reporting purposes, EHRs must be able to capture relevant clinical data using standardized definitions for data and quality measures.[314] NCVHS also specifies that, in order to receive incentive payments from HITECH, "providers will need to collect specific clinical data to build quality of care reports."[315] An electronic exchange system designed to collect a wide variety of health information from a large percentage of the population will help providers build these quality of care reports.

Mining data through an electronic exchange system also has the potential to reap large public health benefits. If the information exchanged is made available to public health agencies for the purpose of identifying disease outbreaks and long-term population health threats, tremendous strides can be made in the field of public health. The more information that can be accessed, the better, and the ability to access clinical information in real time is also critical so that public health officials can respond to outbreaks and threats quickly.[316] For example, the recent GAO report offers the example of an exchange that connected its hospitals to the state's public health department, allowing for real-time reporting of conditions and detection of disease outbreaks. According to the exchange, this system enabled the state to obtain information regarding H1N1 cases more quickly than other states.[317]

Networking electronic databases together on a regional or national level increases the power to improve health care exponentially.[318] Regional networks of databases can be used to identify outbreaks or infections, or to highlight differences in patient care from one hospital to the next.[319] An HIO that makes genomic information, environmental factors, and family history accessible in its database would also enable clinicians to engage in personalized medicine.[320]

The opportunity to realize public health benefits through electronic exchange is vast. Potential public health use cases for electronic exchange include the mandated reporting of laboratory diagnoses and physician-based diagnoses, public health investigation (in which a health department investigator would query an HIO for additional information on a previously reported disease or outbreak), antibiotic-resistant organ surveillance, and using electronic exchange to monitor the prevalence of diseases like diabetes, heart disease, and colon cancer and their quality

---

[312] NCVHS. *Letter to the Secretary of Health and Human Services re: Meaningful Measurement of Quality Health Care Using Electronic Health Records*, December 1, 2009. Available at: http://www.ncvhs.hhs.gov/091201lt.pdf.
[313] *Id.*
[314] *Id.*
[315] *Id.*
[316] CRISP Health, *supra* note 296.
[317] GAO, *supra* note 303, at 19.
[318] D'Avolio, *supra* note 309, at 1110.
[319] *Id.*
[320] *Id.*

metrics (rates of colonoscopy, mammograms) across a community.[321] One of the exchanges highlighted in the recent GAO report has begun working with the local public health department to create metrics related to health conditions prevalent in the community, such as the percentage of each provider's eligible patients who have been screened for cancer or received appropriate immunizations.[322] Consent models that allow for a wide variety of data types to be collected from the majority of the population seem to be best for realizing improvements to public health.

In addition to potential uses in public health research, data mined from electronic exchange databases can be used for a broad array of other research purposes, which possibility raises a number of privacy and consent issues. In its report on privacy and health research published in February 2009, the Institute of Medicine (IOM) recommended changes to the standard of obtaining patient consent before using data for research.[323] Specifically, the report recommends that Congress authorize HHS and other federal agencies to develop new standards for protecting privacy in health research that would apply uniformly to all health research.[324] IOM further recommended that, after the new standards have been implemented, all health research should be exempt from the HIPAA Privacy Rule.[325] The report also proposes an approach in which programs or institutions could be certified by HHS or another accrediting body to qualify for "safe harbor" protection from regulation.[326] Certified entities would then be permitted to "collect and analyze personally identifiable health information for clearly defined and approved purposes, without individual consent."[327] Finally, in situations where personally identifiable health information is needed for research and researchers cannot use data with direct identifiers removed, approval by an "ethics oversight board" would be required.[328]

IOM's proposal to dispense with the informed consent requirement in clinical research has naturally drawn criticism.[329] Instead of enhancing privacy, critics charge that the report seems to suggest that health research can be improved by relaxing privacy protections. In the electronic exchange context, the proposal could be interpreted to mean that patients would not need to provide consent for their health information to be used in certain research situations. The IOM report is merely a proposal, however, and has yet to manifest in any regulatory action.

Disparities

An important consideration in selecting an electronic exchange choice model is the extent to which it will impact – either positively or negatively – racial, ethnic, and socioeconomic health disparities. The Summit Health Institute for Research and Education (SHIRE) recently identified

---

[321] Shapiro, J. "Evaluating Public Health Uses of Health Information Exchange." *Journal of Biomedical Informatics*, Vol. 40, Issue 6, Supplement 1, December 1, 2007, pp. S46-S49.
[322] GAO, *supra* note 303, at 20.
[323] Institute of Medicine. January 27, 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: The National Academies Press.
[324] *Id.* at 30.
[325] *Id.*
[326] *Id.* at 33.
[327] *Id.*
[328] *Id.* at 34.
[329] *See* Rothstein, M.A. "Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark," *Journal of Law, Medicine & Ethics*, Vol. 37, No. 3, September 30, 2009, pp. 507-12.

several barriers to reducing disparities in HIT adoption.[330] These barriers include disparate access to technology required for HIT use, lack of culturally / linguistically appropriate outreach, lack of capital investment in HIT and HIT sustainability, trust issues surrounding privacy, and lack of participation by minority stakeholders.[331]

An electronic exchange model that relies on the internet to obtain patient consent and / or educate patients about consent options could have a negative effect on racial and ethnic health disparities, as minority populations have less access to such technologies than other populations. Statistics show that 73 percent of white adults use the internet compared to 61 percent of African Americans, and that 68 percent of whites but only 50 percent of African Americans have a home computer.[332] Further, health disparities could persist if communities without access to broadband technology continue to experience this lack of essential infrastructure for electronic exchange.[333]

In addition to decreased access to online resources, African Americans report higher levels of distrust in health providers and health care systems than their white counterparts.[334] As a result, African Americans may perceive privacy threats related to online health records and electronic exchange systems differently, and might be more likely to opt out of electronic exchange.

Studies examining disparities related to PHRs and electronic exchange have yielded varying results. A two-year study of Georgia Kaiser Permanente enrollees found lower rates of participation in a Kaiser Permanente PHR system among African Americans (30.1 percent) than among whites (41.7 percent).[335] In addition, those with postgraduate education were more likely to register in the PHR system (44.4 percent) than adults with a high school education or less (24.4 percent).[336] Researchers in the Kaiser study concluded that, because racial and ethnic minorities and those with lower education, advanced age, and rural addresses have decreased access to information technology, PHRs also have the potential to widen disparities in health care.[337]

In contrast, results from the Massachusetts pilot program (an *opt-in* model), revealed virtually no disparities in participation among the three sites in the pilot study, although each site had a very different socioeconomic makeup.[338] One reason for the lack of disparities in the Massachusetts

---

[330] Summit Health Institute for Research and Education, Inc. (SHIRE). *Perspectives on the HIT/Health Disparities Connection*, March 2007. Available at: http://www.shireinc.org/reports/HIT%20Congressional%20Briefing%20-%20SHIRE%20Perspectives%20March%202007%20-%20Edited.pdf.
[331] *Id.* at 3-4.
[332] *Id.* at 4; *see also* Livingston, G. and Parker, K. "Latinos Online, 2006 – 2008: Narrowing the Gap." *Pew Hispanic Center*, Washington D.C. (December 22, 2009). Available at: http://www.pewhispanic.org/files/reports/119.pdf (76% of whites use the internet, compared to 63% of blacks and 64% of Hispanics).
[333] SHIRE, *supra* note 330, at 5.
[334] Roblin, D.W. et al. "Disparities in Use of a Personal Health Record in a Managed Care Organization, *Journal of the American Medical Informatics Association*, Vol. 16, No. 5, September 2009, pp. 683-89, at 684.
[335] *Id.* at 685.
[336] *Id.*
[337] *Id.* at 687.
[338] Tripathi, *supra* note 43, at 436.

pilots could be the program's sophisticated direct-to-consumer marketing effort, which focused on reaching patients through their clinicians instead of over the internet.[339]

Regardless of the consent model chosen, care must be taken to ensure that existing health care disparities are not exacerbated, and to make progress toward their reduction. These goals can be accomplished by working to ensure that essential infrastructure components are available to support a broad range of populations involved in electronic exchange, by increasing and diversifying community outreach and education efforts, and by working to ensure that the specific needs and concerns of minority populations are addressed adequately through the policies and practices of an exchange.

METHODS OF POLICY IMPLEMENTATION

As described throughout this whitepaper, the development of policies regarding consent requirements can be a vexing challenge for the establishment of successful electronic exchange, especially with regard to sensitive information. Some stakeholders have argued that the federal government should establish policies regarding consent that would preempt the field and set one uniform national standard that all organizations engaging in electronic exchange would be required to follow. Others have argued that state law should establish consent principles with regard to general consent, specific conditions, interstate information exchange, information exchange with employers and purchasers, use of information for marketing, and waivers of consent in public health emergencies and when a patient's life is at risk. Arguments have also been made for the adoption by the entire health care industry of a standardized or uniform patient consent form and process.[340]

In essence, the many stakeholders in electronic exchange are actively seeking ways to simplify the questions surrounding the issue of consent. From a policymaking viewpoint, there are a variety of possible vehicles to use in approaching that goal. Each method, of course, has both advantages and disadvantages, and the methods themselves could have varying effects on the availability of and benefits / burdens calculation relating to possible consent models. This section briefly discusses some of the available tools and possible effects of their use in three large categories: 1) federal legislative and regulatory options; 2) state-driven methods; and 3) voluntary approaches.

Federal Legislative and Regulatory Approach

In order to achieve consistency across states in privacy law and practices related to consent, thereby facilitating regional, and even national, electronic exchange, Congress could enact a uniform federal privacy law that preempts conflicting state laws. Adopting a uniform law would provide immediate homogeneity and consistency across states. The approach could also include the creation of a standard consent form for electronic exchange. [341]

---

[339] *Id.* at 439.

[340] Dimitropoulos, L.L. "Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions, Executive Summary," June 30, 2007. AHRQ Contract No. 290-05-0015, *RTI International*. Available at: http://www.rti.org/pubs/avas_execsumm.pdf.

[341] HISPC, *supra* note 117, at 4-3.

A major drawback of adopting a preemptive federal law, however, is the length of time needed to enact such legislation. In addition, the fact that there is no general consensus on the ideal level of individual consent in electronic exchange among exchange entities, let alone the country, would increase the time and, indeed, the realistic possibilities for a law to be enacted. Finally, adopting a uniform federal law would not prevent statewide variations in interpreting and implementing that law, as has occurred in the case of the HIPAA Privacy Rule.[342]

History has shown, however, that if Congress chooses to pass a sweeping law, its implementation can be accomplished quickly. In 1964, for example, Congress passed Title VI of the Civil Rights Act, which prohibits the provision of federal funds to organizations or programs that engage in racial segregation.[343] In order to desegregate hospitals without delay, Congress conditioned the receipt of Medicare funds on compliance with the anti-discrimination provisions of Title VI.[344] Because hospital solvency depends heavily on Medicare payments, they were in essence forced to choose between compliance with the law and bankruptcy. Nationwide compliance with Title VI was immediate. In less than four months, more than 1,000 hospitals had integrated their medical staffs, waiting rooms, and hospital floors; by 1966, over 92 percent of all American hospitals were integrated.[345]

The Medicare Title VI experience is an extraordinary example of rapid implementation of and compliance with a federal law. In that case, the venture succeeded because: 1) its financial incentives were strong and unambiguous; 2) all hospitals across the nation were subject to the same financial pressure; 3) the effort was forward-looking and no sanctions were involved; and 4) the goal of Title VI – dismantling racial segregation – was visible and easily verifiable.[346] Lessons from the Title VI experience are instructive in analyzing the feasibility and / or likely success of enacting and implementing a uniform federal law regarding consent in electronic exchange.

Rather than enacting federal legislation that would preempt state privacy laws explicitly, Congress instead could enact legislation that would permit exchange entities to share personal health information for treatment purposes according to defined consent parameters and only under certain conditions.[347] An advantage of this approach is that it would also create uniformity across states, while a disadvantage is the possibility of duplicative consent requirements (or requirements where none previously existed) if the requirements under federal law differ from those provided by state law.[348]

An alternative to the federal legislative approach is implementation of electronic exchange policies regarding consent through federal rulemaking. Generally, in notice and comment rulemaking, an administrative agency first publishes a notice of proposed rulemaking in the

---

[342] *Id.*
[343] Smith, D.B. "Racial and Ethnic Health Disparities and the Unfinished Civil Rights Agenda, *Health Affairs*, Vol. 24, No. 2, March 2005, pp. 317-24, at 319; 42 USC § 2000d et seq. (2006).
[344] 42 U.S.C. § 2000d et seq.
[345] Watson, S.D. "Race, Ethnicity, and Quality of Care: Inequalities and Incentives," *American Journal of Law, Medicine & Ethics*, Vol. 27 Nos. 2-3, 2001, pp. 203-24, at 215.
[346] *Id.* at 216.
[347] HISPC, *supra* note 117, at 4-3.
[348] *Id.* at 4-5.

Federal Register.[349] Interested persons then have the opportunity to submit comments on the proposed rule, which the agency considers before adopting and publishing a final rule.[350] In addition to publishing new rules, agencies also have the option to use the rulemaking process to modify or clarify existing regulations (*e.g.*, revisions to the HIPAA Privacy Rule currently being promulgated pursuant to the HITECH Act). Although federal rulemaking would establish uniformity across states and can sometimes be a swifter process than enacting federal legislation, it too can be time-consuming and generally requires political consensus as to the goals of the regulation.

A separate option within the federal rulemaking sphere is negotiated rulemaking, in which a negotiation process takes place before an agency issues a proposed regulation.[351] In negotiated rulemaking, the agency convenes a committee of interested parties and agency staff who meet publicly to negotiate a proposed rule.[352] If the committee reaches a consensus, the agency uses the agreement as a basis for its proposed rule and proceeds according to the notice and comment provisions of the Administrative Procedure Act.[353] Although negotiated rulemaking is designed to decrease the delays endemic to the rulemaking process, some scholars claim that these reductions are actually minimal.[354] Negotiated rulemaking does, however, have one major benefit: interested stakeholders are present from the beginning of the discussions and have a concrete role in shaping policy.

State-Driven Approach

Policy vehicles for addressing consent requirements in electronic exchange also abound at the state level. For example, in order to harmonize state health information disclosure laws, thereby facilitating the sharing of patient information across state lines, state laws could be amended based on a "trading partner" basis, where neighboring states or medical markets develop a plan for resolving differences.[355] To facilitate a trading partner framework, a federally-designated organization could be established to coordinate and support the effort.[356] Although this approach would help to resolve differences in regions that would directly benefit from reconciling state privacy approaches, it is unlikely that amending state laws would fully resolve variations among states.[357]

Alternatively, an interstate compact approach could be used to provide a consistent and potentially nationwide approach for addressing what consent law or policy applies to interstate exchange.[358] As discussed by the HISPC Intrastate and Interstate Consent Policy

[349] The Administrative Procedure Act, 5 U.S.C. § 553 (2006).
[350] 5 U.S.C. § 553.
[351] Coglianese, C. "Assessing the Advocacy of Negotiated Rulemaking: A Response to Philip Harter," *New York University Environmental Law Journal*, Vol. 9, June 2001, pp. 386-447. *See also* Negotiated Rulemaking Act of 1990, 5 U.S.C. §§ 561-570 (2006).
[352] *Id.* at 391. *See also* 5 U.S.C. §§ 561-570.
[353] *Id.*
[354] *Id.* at 446.
[355] HISPC, *supra* note 117, at 4-5.
[356] *Id.*
[357] *Id.* at 4-7.
[358] HISPC. *Intrastate and Interstate Consent Policy Options Collaborative—Final Report*, July 31, 2009.

Options Collaborative, development of an interstate compact might be approached in a number of different ways:

1. A "reciprocity" or "choice of law" approach, according to which member states would decide in advance that *either* the consent laws of the state requesting health information or those of the state receiving information would prevail when PHI is exchanged between member states;
2. A "harmonization" approach, according to which such a compact would set forth agreed-upon consumer consent rules or laws that would apply to member states and that would supersede existing, contradictory consent laws or rules; or
3. An approach wherein the structure of a compact would be determined by the policy leaders and stakeholders developing the compact. [359]

Another policy implementation option at the state level would be to amend state privacy laws to reduce variation among them regarding specific types of disclosures.[360] For example, national reference guidelines could be adopted to alleviate inconsistencies among states without using the harsh measure of preempting state law. Such guidelines, as well as a similar vehicle, model codes, have been successful historically in regulating certain areas.[361] However, model codes typically take at least three years to develop, and more time might be needed to draft a model law that takes into account various state approaches.[362] Finally, because states would remain free to adopt and modify any model law, differences between states would likely persist.[363]

States could also allow the sharing of defined types of personal health information based on a uniform consent requirement.[364] For instance, the HISPC Interstate Disclosure and Patient Consent Requirements Collaborative found that about half of the eleven states surveyed permit the disclosure of certain types of data without consent for non-emergency treatment.[365] Use cases could be developed for the purpose of analysis in which specific data types, such as diagnoses, procedures, and medication records, are exchanged without consent to determine which state laws would permit specific data holders to participate in electronic exchange. Similar analyses using different data types and data holders could give insight into segments of electronic exchange that face the fewest state law barriers. As a result, exchange priorities could be shaped based on the types of data exchange that are most feasible.

Finally, the development of regional or national electronic exchange could be approached within the existing framework of state laws. One possibility within this framework is to develop a database that documents each state's requirements regarding when disclosure of patient data can be accomplished without consent and, if consent is required, what elements must be satisfied.[366] Such a database could be used to create electronic exchange approaches that actively manage

[359] *Id.* at 1-2.
[360] *Id.* at 4-6.
[361] *See e.g.*, The Uniform Commercial Code (commercial transactions) and the Uniform Probate Code (probate affairs of decedents).
[362] HISPC, *supra* note 117, at 4-7.
[363] *Id.*
[364] *Id.* at 4-6.
[365] *Id.*
[366] *Id.* at 4-8.

state variations in consent requirements. Technical vendors could be enlisted to increase the capability of the rules database even further, allowing its incorporation as a functioning consent and disclosure management component of interstate electronic exchange networks.[367] If successful, electronic exchange systems could access the database in real time to automate disclosure decisions, reconcile consent requirements, and generate compliant consent forms for a particular disclosure situation.

The options outlined above could allow for identification and resolution of divergent consent and disclosure requirements among states, and would also offer states flexibility to align with new federal developments. The creation of a sophisticated database might present cost and technical barriers, however, in addition to requiring an entity to host and maintain the online rules database and update it as state laws change.

Voluntary Compliance

Finally, various systems of voluntary compliance could be used to set consent standards for electronic exchange at both the state and federal level. For example, voluntary compliance could be achieved through the use of model codes or best practices, or through other options including procurement, accreditation, connectivity requirements, or pledges of support for a particular approach.

As previously discussed, model codes or reference guidelines historically have been a successful means of policy implementation. In the health care arena, both plaintiffs and defendants in medical malpractice litigation regularly rely upon clinical practice guidelines,[368] and the implementation of clinical practice guidelines in medicine has had positive quality improvement results.[369] In 1985, for example, anesthesiologists developed practice guidelines aimed at reducing preventable harm to patients. After implementation of the guidelines, the risk of death from anesthesia dropped from one in 5,000 to about one in 250,000.[370] Today, it is estimated that more than 1,400 sets of clinical practice guidelines exist across medical specialties.[371] A national model code or guidelines for implementing electronic exchange therefore might be successfully used to set standards, establish policy, and achieve uniformity in exchange models across states.

Alternatively, implementation of consent policies in electronic exchange could be achieved through "best practices" rulemaking, which occurs when regulated entities themselves develop practices to comply with fairly broad regulatory requirements.[372] In best practices rulemaking, descriptions of successful practices are submitted to an administrative agency by regulated entities, and the "best" practices are then selected and publicized. Although the practices are never mandated explicitly by central administrators, they have proven to be effective in harmonizing action among regulated entities.[373]

---

[367] *Id.* at 4-9.
[368] Center for Justice and Democracy. *Clinical Practice Guidelines as Legal Standards: The Wrong Cure for Health Care*, October 2008. Available at: http://www.centerjd.org/archives/issues-facts/PracticeGuidelinesFactSheetF2.pdf.
[369] *Id.*
[370] *Id.*
[371] *Id.*
[372] Zaring, D. "Best Practices," *New York University Law Review*, Vol. 81, April 2006, pp. 294-350, at 297.
[373] *Id.* at 299.

Best practices rulemaking is well suited for situations when a standard administrative scheme across jurisdictions is desirable,[374] offers low administrative cost, and can mobilize private parties to action through its strong compliance pull. In short, best practices rulemaking can be a flexible, informal method of policy implementation, but ultimately is not open to enforcement. Another disadvantage of the model is that it often produces only common practices rather than ideal ones. Instead of the "right" regulatory program being adopted, the first ones to be submitted and publicized often are implemented. Because the use of best practices depends on replication, regulators in such a regime could be susceptible to cascades and other network effects.[375] As a result, experts have suggested that best practices rulemaking should only be used as long as Congress can provide supervision (which does not currently exist under law), or as long as regulators can ensure that the best practices are publicized and subject to informal comment by interested parties.[376]

Several federal departments and agencies have successfully used best practices as a means of regulation, including the U.S. Department of Housing and Urban Development, the U.S. Department of Homeland Security, and the U.S. Environmental Protection Agency (EPA) in its efforts to regulate water pollution.[377] Specifically, the EPA has encouraged states to develop best practices voluntarily by making funding available to the states that do so.[378] The EPA collects best practices from participating states, and consolidates information from successful best practices in a database of success stories.[379] Although the EPA's best practice program is not mandatory, it has been extraordinarily effective because of its link to federal funds. To date, every state has participated in the program.[380]

Finally, there are several forms of voluntary compliance that could be implemented immediately by the federal or state governments. Exchange entities could be regulated via public procurement, which would involve, for example, building specific requirements into government contracts for electronic exchange. Alternatively, the federal or a state government could oversee or implement a program that conditions accreditation of exchange entities on complying with and implementing specific requirements. A similar approach could be taken in the future by mandating requirements for national electronic exchange connectivity. Finally, the federal and / or state governments simply could promote compliance by encouraging entities to serve as model corporate citizens by pledging their support for a chosen electronic exchange approach.

Implications

As discussed above, the political and operational feasibility of various methods of policy implementation widely varies. On a more fundamental level, however, the method chosen to pursue goals in public policy can have a profound effect on the consent models that are available for use by exchange entities.

---

[374] *Id.* at 296-301.
[375] *Id.* at 298-300.
[376] *Id.* at 301.
[377] *Id.* at 339.
[378] *Id.* at 329.
[379] *Id.* at 332.
[380] *Id.* at 329.

For example, should federal policy makers choose to support a *no consent* model through statute or regulation, electronic exchange at all levels could continue as currently operating (unless such a policy disallowed more restrictive consent models, such as *opt-out* or *opt-in*). That is, state laws and regulations would remain in force and the only federal restrictions relevant to electronic exchange would reside in current law (*e.g.*, HIPAA, GINA, Part 2, etc.).

On the other hand, a federal statute or regulations that require use of an *opt-out* model of consent in electronic exchange would preempt state laws that support systems that do not require patient action at all (*i.e.*, *no consent* models). Such systems (*e.g.*, IHIE, DHIN results delivery function) would be required to change their practices in the absence of applicable state law. Depending on the details of the federal requirement, whatever granularity level is mandated by the federal policy would thereafter be required of every entity participating in electronic exchange.

Federal law requiring use of an *opt-in* model of consent would preempt state law regarding systems that do not require patient action at all, as well as laws supporting the use of *opt-out* models (*e.g.*, DHIN query function, CRISP, CareSpark). Such a policy would also mandate the use of *opt-in* models by all exchange entities even in the absence of state law. If an exchange entity currently includes information in a system before offering patients the ability to *opt-out*, any further use of that information would likely be blocked before seeking patients' affirmative consent. Again, depending on the details of the federal mandate, any particular granularity level could be required.

Voluntary compliance measures implemented by the federal government, however, could induce desired results across the board, regardless of the particular consent model at issue. Such measures could require state-led entities and other exchanges to act within certain parameters in order to receive various federal benefits (*e.g.*, accreditation, incentive payments); could support the adoption of model laws or practice guidelines; or could simply entreat state-led entities and / or other exchanges to use a particular consent model through the use of consensus-building (the "bully pulpit" method).

The effects of policy implementation at the state level with regard to consent models are substantially similar, except that states only have the legal power to mandate action within their geographic boundaries and cannot contradict superseding federal law. State laws supporting the use of *no consent* models would essentially maintain the status quo; laws mandating use of an *opt-out* model would require entities to develop compliant policies; and laws requiring use of an *opt-in* model would demand alteration of the practices of all entities currently using *no consent* or *opt-out* models. The methods available to states in the area of voluntary compliance are also similar to those available at the federal level. States could place requirements on the receipt of public funds to support electronic exchange, as well as develop less exacting methods of voluntary compliance, such as practice guidelines and model governance structures.

Because utilization of various methods of policy implementation at the state and federal levels can have such clear-cut effects on operational exchange entities, including those established pursuant to state law and those whose existence pre-dated federal investment and involvement in electronic exchange, policy makers at every level must remain cognizant of the high costs that such actions should entail. The benefits and burdens of potential actions must be assessed

carefully for their economic, human, and systemic costs. That said, however, such a wide variety of implementation methods exist that we cannot allow fear of possible consequences to paralyze policy decision making.

RECOMMENDATIONS / CONCLUSIONS

The choice of which patient consent model to apply for the purposes of electronic exchange will have immediate implications for a variety of stakeholders, and possibly longer-term consequences for our national HIT goals—improving the quality, safety, and efficiency of care while reducing disparities; engaging patients and families in their care; promoting public and population health; and promoting the privacy and security of EHRs.[381]

Patients, providers, payers, HIOs, and other participants in electronic exchange efforts all have something at stake in individual choice model decisions. Complicating the matter further is the fact that the issue of consent is multifaceted and not easily isolated from other important policy decisions. For example, a patient's perspective on participation in electronic exchange may depend considerably on the determination of who can access his / her data, under what circumstances, for what purposes, etc. Similarly, the extent to which HIOs have access to financial resources and support from the provider community likely will impact their willingness to entertain consent models that allow for greater patient choice. Add to this the highly variable and contextual legal, cultural, and political circumstances surrounding such decisions, and it becomes clear why consent to electronic exchange has become such an important and often polarizing issue.

This tension generally can be characterized in two dimensions: one that pertains to respecting the interests of individuals (*e.g.*, patients, providers) as well as those of society as a whole (*e.g.*, reduced health care costs and health disparities), and another that pertains to considering the often divergent interests of the various stakeholders relative to one another. As previously discussed, an example of the former dimension is the possible scenario in which – due, perhaps, to the selection of an *opt-in* model – data on very few patients are made available via electronic exchange for treatment or public health surveillance purposes. On the other hand, an example of the latter might be that, in order to honor patient preferences for sequestering whatever data they deem sensitive, significant resources are expended by participating provider organizations or an exchange entity to develop and sustain a preference management system. Although there is no "right" answer to this dilemma, whatever solution is applied in a given context should take into account the most relevant (to the particular exchange environment) factors in both of these dimensions.

Given the highly variable contexts in which electronic exchange efforts are emerging, it also makes sense to weigh external factors that, although not directly related to patient consent, have a notable impact on the issue. The best example of this is the presence or absence of laws, regulations, and other mechanisms for consumer protection. Unless, for example, the practice of using consumer health information as a basis for financial and other discrimination is prohibited, then the importance of incorporating greater trust and protection elements into the exchange

[381] Blumenthal, D. "Launching HITECH." *New England Journal of Medicine*, Vol. 362, No. 5, February 4, 2010, pp. 382-385.

environment could outweigh other competing considerations. In essence, where broader systemic protections fail, an HIO or other governance entity may need to assume more responsibility for assuring the privacy and security of patient information.

This contextual diversity also makes it challenging to develop a set of specific recommendations that would apply to all electronic exchange efforts. While it may be tempting to suggest that one consent model should apply to all electronic exchanges, or that all exchanges should be required to do "XYZ," to do so would disregard completely the diversity in stakeholder preferences, and the unique contextual elements of each electronic exchange entity (*e.g.*, the type of information exchanged, the process by which consent is obtained, the resources available to support the effort). On the other hand, it can be useful to articulate some higher-level principles and / or recommendations that could help guide decision makers in the midst of establishing active electronic exchange initiatives. At this particular juncture, with more than $560 million in HITECH funds dedicated to helping states develop electronic exchange capabilities within and across jurisdictions,[382] it is an appropriate time for the provision of guidance. Absent some level of direction, the concern, articulated by more than one expert interviewed for this whitepaper, is that each exchange effort will expend vast amounts of time, energy and resources determining its own particular approach to consent. There is some acknowledgement that we have neither time nor resources to waste, so interventions that could generate greater collaboration and efficiency, along with investments to support the generation of additional evidence, would be welcome.

One possible suggestion for helping to further these consent deliberations would be to encourage decision makers at all levels to apply compensatory measures to help offset the imposition placed upon some stakeholders by the decision to implement a particular consent model. This approach would mean, for example, that if policy makers (at various levels) implement an *opt-out* approach, they might also want to consider:

1. Development and active provision of clear and highly-accessible education materials for patients;
2. Provision of a relatively permissive and simple vehicle for patient opt out,
3. Provision of at least one type of granularity option;
4. Establishment of more comprehensive or stringent systemic patient privacy and confidentiality protections; and / or
5. Provision and enforcement of strong oversight and accountability measures.

It is also worthwhile to point out a few higher-level policy issues of direct relevance to the choice model debate. The first concerns the rapidly evolving federal policy landscape, particularly the anticipated clarification of regulatory language in the HIPAA Privacy Rule that is required by ARRA. Chief among these are guidance that the Secretary of HHS is required to establish on the minimum necessary standard,[383] and a study of the current HIPAA de-identification provisions.[384] Clearly, efforts to clarify how much information is the minimum necessary in the context of electronic exchange and to strengthen the de-identification standards in HIPAA may have implications for and inform electronic exchange choice model deliberations. In addition,

[382] *Id.*
[383] ARRA, Pub. L. No. 111-5, § 13405, 123 Stat. 115, 264-268 (2009).
[384] ARRA § 13424.

while the issue is not directly addressed by ARRA in areas other than marketing, many health care stakeholders have long advocated for clarification of the definition of "health care operations."[385] Given that each of these issues potentially could impact exchange decisions regarding appropriate consent models, it seems wise to coordinate broader policy debates regarding these areas of regulatory change with those regarding choice models.

The second area pertains to the tremendous opportunity for coordinated learning that exists through the health information exchange grants and technical assistance planned by HHS pursuant to the requirements of HITECH. Through the HISPC process, numerous state-level decision makers were able to take advantage of collaboration, peer-to-peer learning and technical assistance from experts. It now seems evident that there is at least some desire for additional direction and support from the federal government, both to ensure compliance with relevant laws and regulations and to generate greater efficiency and expedite what has been a lengthy process. Such direction could be provided in the form of clear and consistent information and tools that can be used by state health information exchange grantees to ensure that the full range of issues and options with respect to consent are explored.

A third, and far more specific, area for consideration pertains to the need for greater evidence to inform and support those tasked with making choice model decisions. At present, there are far too few active electronic exchanges to generate such data, and those that exist vary considerably in almost every aspect. Further, the stakes are so high and the level of necessary resources so great that it is even difficult to summon the will required to test a number of different models to see which one works best. While we acknowledge the challenges associated with determining the real impact of various consent models on such important outcomes as provider participation, patient engagement, and public health, it seems likely that there are surrogate markers that could be evaluated at least to provide policy makers with some level of evidence regarding the true (as opposed to surmised) advantages and disadvantages of various consent models. One such example might be to conduct studies regarding the effectiveness and desirability of providers themselves acting as the party responsible for obtaining and managing consent. A variation on this theme could involve studies that compare the effectiveness of different types of providers (*i.e.*, nurses, staff assistants, physicians) as consent managers. Although it may not be possible to conduct such inquiries using data from operating electronic exchange entities, analogous studies could be conducted regarding general consent to information exchange in the treatment context.

Ultimately, the data we need to assess the real-life costs, benefits, and impacts of various consent models in electronic exchange do not currently exist. If we are to move beyond this point in the discussion, we must develop the political will among stakeholders and policy makers to study these issues more deliberately. In the absence of such data, policy makers will be forced to make hard choices in the face of factual uncertainty. While this scenario is by no means new or unique, unintended consequences in the area of electronic exchange concern patients' most personal information. Until the time when we are confident that we can protect such information in a systematic and thorough way, prudent use of the mechanism of consent appears to be one of the most reliable ways to pursue that goal.

[385] *See, e.g.*, McGraw, *supra* note 16, at 25.

APPENDIX A

State-Led Examples of Exchange in the U.S.

State	Consent Model and Related Data Sharing Information
DE	**Type of Consent Model:** Combination of *No Consent* (results delivery) and *Opt-Out* (query function) for the Delaware Health Information Exchange (DHIN). The DHIN has two functions: 1. Results delivery function—all patient laboratory data, radiology reports, and hospital admissions, discharge, and transfer data (ADT data) is uploaded into the system. • There is no patient consent component to this function, so all laboratory, radiology, and ADT data captured on a patient after May 2007 is automatically included in the system. 2. Query function—allows providers to query the system to obtain specific data on a patient. • Patients may choose to opt out of the query function, which effectively blocks all providers from accessing the patient's data in the system. To date, no patients in the state of Delaware have chosen to opt out of the query function, meaning that the entire population of Delaware is currently in the exchange. There is no form of granular consent for DHIN, meaning that patients are either all in or all out. **Type of Information Exchanged:** DHIN began distributing clinical laboratory test results, radiology reports, and admission face sheets (containing admission, discharge, and transfer data) from hospitals and laboratories statewide in May 2007. In January 2010, DHIN expects to add PACS data to the system, which would allow a provider to view a patient's radiology images (x-rays, etc.) through a link in radiology reports. In the near future, DHIN expects to include a patient's 90-day medication history of prescriptions filled. **Obtaining Data and / or Consent:** At the point of care, a provider must educate a patient on DHIN and the *opt-out* procedure. DHIN offers providers talking points, sample privacy language and confidentiality forms to help providers educate patients. Patients can also visit the DHIN website for more information. If a patient chooses to opt out of DHIN, he / she must have a form signed by a provider or notary public (to validate the patient's identity) and return the form to DHIN. This action automatically blocks the data of certain high profile government officials (*e.g.*, Joe Biden) from queries. **Patient Rights and / or Durability of Consent:** Patients may opt out of the exchange at any time. If a person decides to opt out, his / her data remains in the system (and is continually collected by the results delivery function) but providers are blocked from

State	Consent Model and Related Data Sharing Information
	viewing the data. There are no requirements for how often (if at all) consent is to be discussed / revisited (only applicable if the patient has exercised his / her right to opt out). Theoretically, a provider could discuss consent once (if at all) with a patient, and then never again. **Other Related Details:** More than half the providers in Delaware (60%) now use DHIN. Over 85% of lab transactions in the state go through the system, and more than 80% of hospitalizations are reported in it. DHIN contains a relatively sophisticated security system. Providers are only able to access records of current patients, and must "break glass" (list reason for viewing a patient's records and establish a time frame for viewing data) to obtain data on a patient they have not yet treated. Providers can also set the security so that only certain staff members can access the system. DHIN routinely conducts audits to ensure that the system is being used correctly, and revokes privileges of providers who misuse DHIN. A patient has the right to obtain an audit report from DHIN of providers who have accessed their records.
IN	**Type of Consent Model:** *No Consent* required for the Indiana Health Information Exchange (IHIE). (Federally funded substance abuse treatment programs do not provide data to the HIO.) Participating hospitals describe uses of the data in their privacy policies and a provider must suppress the data if a patient requests that his / her information not be shared. **Type of Information Exchanged:** Types of data eligible for exchange include: labs, pathology, radiology, electrocardiogram reports, ER info, hospital encounter info, transcriptions, medication history, discharge summaries, allergies / immunization, tumor registry, ambulatory appointment data, claims processing, and prescription data (dispensing evaluation). In 1994, with funding from the National Institutes of Health and the National Library of Medicine, Regenstrief Institute Medical Informatics extended the Regsenstrief Medical Record System (RMRS) to the Indiana Network for Patient Care (INPC), a city-wide clinical informatics network. Five INPC hospital systems in Indianapolis (Community Hospitals Indianapolis, St. Vincent Hospitals and Health Services, St. Francis Hospital and Health Centers, Clarian Health, and Wishard Health Services) operate a total of 11 different hospital facilities and more than 100 geographically-distributed clinics and day surgery facilities. Collectively, these systems admit 165,878 patients, and serve more than 390,000 emergency room visits and 2.7 million clinic visits per year. All INPC participants now deliver registration records, all laboratory tests, and all UB92 records (diagnosis, length of stay, and procedure codes) for hospital admissions and emergency room visits to separate electronic medical record vaults in a central INPC server located at Wishard Hospital. The computer system standardizes all clinical data as it arrives

State	Consent Model and Related Data Sharing Information
	at the INPC vault, laboratory test results are mapped to a set of common test codes (LOINC) with standard units of measure, and patients with multiple medical record numbers are linked. Each institution has the same file structure and shares the same term dictionary which contains the codes, names (and other attributes) for tests, drugs, coded answers, etc. When a patient is seen in any of the 11 emergency rooms operated by the consortium hospitals, and the patient consents, the information from all of these institutions about one patient can be presented as one virtual medical record. **Obtaining Data and / or Consent:** Data is only used for purposes allowed under HIPAA. **Patient Rights and / or Durability of Consent:** Data is only used for purposes allowed under HIPAA. **Other Related Details:** To gain access to the exchange, providers must be authenticated to the system. Types of HIE services offered in Indiana include: 1. A clinical messaging service that delivers test results from labs to the doctor's office; 2. A patient look-up service; and 3. A quality metrics and reporting service, where the data are used for quality purposes A patient's data is maintained in separate "vaults" or clinical data repositories by the institution until one of the allowed uses is triggered. Then, the patient's data are merged virtually. The triggers are highly specific and tightly controlled.
MD	**Type of Consent Model:** *Opt-Out* (though it functions as an *opt-in*) for the Chesapeake Regional Information System for Our Patients (CRISP; http://www.crisphealth.org/). By default, all patients will be notified about the existence of CRISP and will be in the exchange unless they opt out of exchange participation. Even if patients opt out, a certain amount of basic patient demographic information will still technically reside in the exchange, but in a separate data repository used for the master patient index. Other basics include: 1. No "break the glass" provisions to obtain information for a non-participant (an individual who has opted out) will be permitted, and CRISP does not recommend granular control for exclusion by data type or provider organization; 2. Hospitals and other providers will be permitted to allow patients greater control over which of their records are published to the exchange; and 3. Health record banks (HRB) and personal health records (PHRs) will be an exception to the all-in or all-out principle. A patient will have the option of excluding himself / herself from the exchange for every other purpose, while still allowing information to flow from an HRB to a healthcare provider. This feature of the HIE is designed for patients desiring more granularity than an all-out option. **Type of Information Exchanged:** Two pilot efforts are currently operational: One in Baltimore involves the exchange of medication history between a few hospitals.

State	Consent Model and Related Data Sharing Information
	The other is in Montgomery County and involves the exchange of certain clinical data (not full CCR) between a few hospitals. The state has mapped out 20 use cases and will build up capacity to eventually roll out each one statewide. The purpose for data exchange is treatment, but there are secondary uses of the data—including biosurveillance and public health. **Obtaining Data and / or Consent:** Patients will be able to opt out of the exchange, becoming a non-participant, by calling a toll-free phone number and requesting to be excluded. Patients may enroll via phone or direct contact with a provider (*e.g.*, use of a form), and can also choose to participate at the point of care. HRBs and PHRs are exceptions to the all-in or all-out principle. By using an HRB, a patient has the option of excluding himself or herself from the exchange for every other purpose, while still allowing information to flow from an HRB to a healthcare provider. A policy board will determine the approach for a number of issues that have yet to be decided, including whether to have one consent form that would cover all (or most) use cases, or multiple forms tailored to the type of electronic exchange service. **Patient Rights and / or Durability of Consent:** Patients may revoke their participation in the exchange at any time. If they do so, the existing data in the exchange will remain, but will be sequestered from further circulation unless required by law. Patients are also able to alter their status in either direction (*i.e.*, participate after previously opting out).
MA	**Type of Consent Model:** *Opt-In* for the Massachusetts e-Health Collaborative (MAeHC). Three pilot projects under MAeHC formally ended in December 2008, but MAeHC is maintaining relationships with all participating providers through 2010, in order to allow ongoing collection of performance and evaluation data. In addition, MAeHC gives providers access to a community repository of clinical summaries. The goal of the pilot project was to study and demonstrate the effectiveness and practicality of implementing EHRs in community settings. As of November 2008, the patient *opt-in* rate exceeded 90%. MAeHC is one of four major HIOs in MA. The other three are the MA Health Data Consortium (MHDC), the New England Healthcare Electronic Data Interchange Network (NEHEN), and MA Simplifying Healthcare Among Regional Entities (MA-SHARE). MA-SHARE is a major regional collaborative involving payers, providers, patients, and employees in the state. MA-SHARE seeks to do the following: 1. Promote the inter-organizational exchange of healthcare data using information technology, standards, and administrative simplification, in order to make accurate clinical health information available wherever needed in an efficient, cost-effective, and safe manner;

State	Consent Model and Related Data Sharing Information
	2. Facilitate and incubate new projects exploring healthcare data connectivity in order to develop, pilot, and demonstrate new healthcare information technologies across communities and enterprises; and 3. Design technology solutions that assemble, organize and distribute a variety of up-to-date clinical information to a broad range of clinical settings; all accomplished in a secure, confidential manner. **Type of Information Exchanged:** Data exchanged in the three MAeHC pilots include: problems, procedures, allergies, medications, demographics, smoking status, diagnosis, lab results, and radiology reports. The MA-SHARE program contains a record locator service, medication histories in emergency departments, e-prescription integration, and clinical messaging services. As part of the MA-SHARE Push Pilot, discharge documents created by Beth Israel Deaconess Medical Center, Children's Hospital Boston, and emergency department systems were routed over the new infrastructure to physicians and practices who have volunteered to participate in the pilot. **Obtaining Data and / or Consent:** A patient is given the option to participate in the MAeHC when he / she visits a clinical entity for care, where he / she may opt in all clinical data from each entity. The patient chooses which entity's records to make available to the network, and pre-defined data are then sent to the central server. Data are retrieved by the physician, who views the data prior to or during the patient visit. In the *opt-in* model, a signed patient consent form is required for that patient's clinical data to be uploaded from his / her physician's office EHR to the exchange's community database.
NY	**Type of Consent Model:** *Opt-In* (NY refers to it as an "affirmative consent model"). Consent is considered to be all or nothing, meaning that any data contributed to the exchange could be made available (*i.e.*, no ability to segment by data type). Examples of NY RHIOs include: Long Island Patient Information Exchange (LIPIX), HealtheLink (Buffalo), and Southern Tier Health Link (Binghamton) PCIP. **Type of Information Exchanged:** State-level policies are broad so as to allow for variation by region / HIO. As such, the type of data included in a given exchange varies from one to another. **Obtaining Data and / or Consent:** There are two approaches, depending on the RHIO: 1. The provider organization obtains consent at the point of service. For example, the Brooklyn Health Information Exchange uses a "provider by provider" consent process rather than a universal consent process for enrollment; and 2. The RHIO obtains consent through a RHIO multi-provider consent form, which can be accessed either at the point of service or online via the RHIO website.

State	Consent Model and Related Data Sharing Information
	Patient Rights and / or Durability of Consent: Patients have the ability to revoke their participation in the exchange at any time. If they do so, the existing data in the exchange will remain, but will be sequestered from further circulation unless required by law. **Other Related Details:** The Primary Care Information Project, governed by the NYC Health Department, contains extensive privacy safeguards. These safeguards include the ability of a patient and doctor to see who has gained access to the records, and to lock certain data behind a firewall so it can be seen only by the PCIP. According to the February 17, 2009 Appendix of the Public Governance Models Report, there are 9 state-designated RHIOs in New York.
RI	**Type of Consent Model:** *Opt-In (Double)*. Consent for exchange participation is all or nothing, so there is no granularity of choice with respect to the types of data that can flow through the exchange. Once a patient has enrolled in the exchange, there are three options for his / her participation: 1. All providers involved in care are permitted to access information (akin to HIPAA); 2. Only certain (selected by the patient) provider organizations (no segmentation at the individual provider level) are authorized to access information; and 3. The default setting, in which providers have temporary access to information only in an emergency or unanticipated event. **Type of Information Exchanged:** RI is still in test mode, so no data are currently being exchanged, but the near-term plans are for laboratory and medication history exchange. Eventually, the hope is to exchange other types of data, including radiology reports and discharge summary reports. For the near future, the exchange will be used only to support treatment, including care coordination. An advisory council will determine which, if any, additional purposes should be added. **Obtaining Data and / or Consent:** The RI Quality Institute (RIQI) has been training staff in participating provider and other organizations (including ambulatory and inpatient care settings, employers, community-based organizations, and long-term care facilities) how to walk patients through the consent process. To enroll, a patient completes an enrollment and authorization form for the exchange. Patients can also enroll directly through the Current Care RI website, but will need to call a hotline to indicate their provider preferences if they select participation option 2 (described above). To help offset the cost of administration, RI DHHS is paying a one-time, $3 authentication fee for every participant enrolled. **Patient Rights and / or Durability of Consent:** Patients have the ability to revoke their participation in the exchange at any time. If they do so, the existing data in the exchange

State	Consent Model and Related Data Sharing Information
	will remain, but will be sequestered from further circulation unless required by law. For participants selecting the default option (described above as the third option), information can only be accessed for up to 72 hours. **Other Related Details:** All provider organizations submitting data to the exchange will need to determine if the patient in question is currently participating in the RI exchange. Due to provider reluctance to perform this function, the state is supporting development of a technology solution that will reside (for now) with each contributing provider site. This interface will look up participation status for patients before any information is shared outside of the firewall.
WA	**Type of Consent Model:** *Opt-In* for four HRB pilot programs. Three pilot program locations are state-funded: Bellingham, Wenatchee, and Spokane. The pilot in Tacoma is federally-funded (Madigan Army Medical Center in Fort Lewis, funded by the Department of Defense). HRBs implement a consumer-centric model. The consumer-centric model has instilled some uncertainty among providers, who are concerned that patients would change or misuse their health information in the HRB. **Type of Information Exchanged:** Prescription data, allergies, laboratory results, immunization records. Laboratory results, x-rays, and medication data are currently in the repository. **Obtaining Data and / or Consent:** Patients give consent for the HRB by creating their own personalized account and then, using the HRB model, patients authorize the release of their information to specific providers. Copies of a patient's health information are transferred into a patient's HRB account like a deposit. Patients who choose to participate use web-based tools like Microsoft HealthVault and Google Health to store their personal health information in one location. The Google software does not provide the same level of granularity as Microsoft. With Microsoft, patients can choose what type of information providers can see, and can choose which providers are allowed to view the information. Currently, patients do not have the ability to input or alter their health information in the bank. They can only view the information on the screen and print it out to share with providers in hard-copy form. **Patient Rights and / or Durability of Consent:** There is no time limit. A patient may disenroll from the HRB at any point. If a patient decides to disenroll, the HRB offers a window of time (30 – 90 days) during which the patient can change his / her mind and re-enroll without losing valuable HRB data. Because the HRB model is consumer-centric, the holders of data are released from HIPAA issues (the HRB is obligated under ARRA to release a patient's health information to him /

State	Consent Model and Related Data Sharing Information
	her). HRBs also contain an audit function, which allows patients to find out when their records are accessed. **Other Related Details:** The Washington State Heath Care Authority plans to publish an interim progress report on the pilot projects in the near future.
VA & TN	**Type of Consent Model:** Similar to IN, state laws in VA and TN do not require affirmative consent from patients to share their general clinical information electronically for treatment purposes (or other purposes expressly permitted under the law). CareSpark is a non-profit regional health information exchange operating in a 34-county area of East Tennessee and Southwest Virginia. At present, five provider entities participate in the exchange: 1. Two ambulatory primary care practices; 2. One hospital system; 3. One payer; and 4. One public health agency. As of mid-November 2009, there were 310,000 patients in the master patient index. Only a subset of this population has data in the actual exchange because not all have had a clinical encounter subsequent to receiving notice / opting-in. The Carespark board of directors wanted to ensure that community members whose data were to flow through the exchange would be well-educated about the process. As such, the board established an *opt-out with notice* policy, meaning that no data are collected for exchange until the patient is at least minimally educated about the exchange. In addition, the board allowed individual provider organizations to adopt an *opt-in* protocol, meaning that providers who choose to do so can require affirmative consent. Currently, the information in the exchange is to be used for treatment only, but participants understand that the goal is to be able to expand to public health, and eventually to other approved research applications. Although not yet determined, the organization is leaning toward having a blanket statement for consent on how information can be used for research purposes, but with a supplemental patient consent form for specific studies that would require IRB approval. **Type of Information Exchanged:** At present, Carespark is only exchanging general clinical information, which expressly excludes any type of information deemed sensitive under either state's laws. This issue is currently under consideration, however, so the board may change this policy in the future. They do their best to ensure that sensitive information is not shared by: 1. Restricting the participation of facilities that primarily serve patients with sensitive conditions; and 2. Asserting that the provider is the one responsible for filtering data, and not allowing such information to enter the exchange.

State	Consent Model and Related Data Sharing Information
	Obtaining Data and / or Consent: Carespark has adopted a provider-centric approach to patient education and, where applicable, consent. Based on some early research with patients in the community, they learned that most stakeholders thought it would be best for the provider to directly educate the patient. Carespark has an employee who trains provider organizations, and also supplies them with written and other educational materials that can be used during the notification process. Most of the provider organizations use a paper form (either for notice or for consent) when they first interface with the patient about the exchange. To manage consent more broadly, they have built a custom software solution called Master Patient Option Preference (MPOP). For every patient, a provider can enter a medical record number into the system to see whether that person is has opted out (in which case any clinical info found in the system should not be exchanged), or has either been notified or opted in. **Patient Rights and / or Durability of Consent:** The issue of durability of consent is left to the provider's discretion. If a patient participates and then later decides to opt out, his / her information remains in the exchange, but will not flow.

APPENDIX B[1]

TABLE 2

State	Selected State Laws
DE	**DEL. CODE ANN. tit. 16, §§ 9920-22 (2010):** Creates the Delaware Health Information Network (DHIN) to "promote the design, implementation, operation, and maintenance of facilities for public and private use of health care information in the State"; assigns powers and duties to DHIN. **DEL. CODE ANN. tit. 16, § 9926 (2010):** Mandates that the Delaware Health Care Commission shall, by rule or regulation, ensure that patient specific health information be disclosed only to those having a need to know in accordance with the patient's consent or best interest. Any misuse of DHIN health information or data shall be reported to the Office of the Attorney General, and is subject to prosecution and penalties under the Delaware Criminal Code or federal law. **DEL. CODE ANN. tit. 16, § 1203 (2010):** **1-100-102 DEL. CODE REGS. §§ 1.0-8.0 (2009):** Provides the requirements of participation in DHIN; specifies the obligations of business associates under HIPAA; and specifies that patients shall be informed of and may choose to preclude a search of their individual health information (opt-out) in the DHIN Interchange after consultation with their health care provider.
IN	**IND CODE ANN. §§ 5-31-3-1, 5-31-6-3 (West 2009)**: Establishes the Indiana Health Informatics Corp. to assist in the development of a statewide HIE system. Specifies that an HIE system must comply with HIPAA.
MA	**MASS. GEN. LAWS ANN. ch. 40J §§ 6D-G (West 2009)**: Establishes the E-Health Institute Fund for the purpose of advancing the use of HIT in the Commonwealth. Grantees receiving money from the Fund must: • allow patients to opt-in to the health information network and opt-out at any time • securely maintain identifiable health information • provide individuals the option to receive a list of individuals who have accessed their identifiable health information • develop guidelines addressing the privacy and confidentiality of identifiable health information

[1] For a comprehensive review of state law requirements for patient permission to disclose health information, *see* 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. Available at: http://www.healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_910326_0_0_18/DisclosureReport.pdf. *See also* Purington, K., et al., "Electronic Release of Clinical Laboratory Results: A Review of State and Federal Policy." Prepared for: *California HealthCare Foundation*, January, 2010. Available at: http://www.chcf.org/topics/view.cfm?itemid=134157.

State	Selected State Laws
	• report any unauthorized access or disclosure of patient health information **MASS. GEN. LAWS ANN. ch. 112 § 2 (West 2009)**: Effective January 1, 2015 the board of registration for medicine, which licenses physicians, will require that all applicants be competent in the use of computerized physician order entry, e-prescribing, EHRs and other forms of HIT.
MD	**MD. CODE ANN., HEALTH-GEN. § 19-143 (West 2009):** Required the Maryland Health Care Commission to designate a state HIE on or before Oct. 1, 2009. On or before September 1, 2011, the Commission must adopt regulations that require State-regulated payors to provide incentives to health care providers to promote the adoption and meaningful use of EHRs. On or after the later of January 1, 2015 or the date established for penalties under ARRA, health care providers must use EHRs that are certified by a national certification organization designated by the Commission and capable of connecting to and exchanging data with the HIE designated by the Commission in order to qualify for incentive payments.
NV	**NEV. REV. STAT. § 439.538 (2007):** Allows individuals to opt out of the electronic transmission of individually identifiable health information, except when required by HIPAA or state law. Medicaid and CHIP recipients may not opt out. Exempts HIPAA-covered entities that electronically transmit individually identifiable health information in compliance with HIPAA provisions from compliance with more stringent privacy or confidentiality provisions under state law.
NY	**N.Y. PUB. HEALTH LAW § 18 (McKinney 2010):** Requires that hospitals, physicians, other health care providers, and HMOs obtain written consumer consent before disclosing personal health information for non-emergency treatment. Requires patient consent even in the case of treatment, payment, and health care operations. *New York courts analyzing Public Health Law, § 18 have required "any individual, including government officials, who possess medical records to keep those records confidential and not to release them to third parties without proper authorizations." Grosso v. Town of Clarkstown, No. 94 Civ. 7722(JGK), 1998 WL 566814, at *8 (S.D.N.Y. Sept. 3, 1998); Caraveo v. Nielson Media Research, Inc., et al., No. 01 Civ. 9609 LBSRLE, 2003 WL 169767 (S.D.N.Y. Jan. 22, 2003).* **N.Y. EDUC. LAW § 6530(23) (McKinney 2010):** It is professional misconduct for physicians, physician's assistants, and specialist's assistants to reveal personally identifiable information obtained in a professional capacity to a third party without the consent of a patient. **N.Y. COMP. CODES R. & REGS. tit. 8, § 29.1 (2009):** Prohibits licensed professionals from revealing "personally identifiable facts, data or information obtained in a professional capacity without the prior consent of the patient or client, except as authorized by law."

State	Selected State Laws
	Disclosure of HIV- related information: **N.Y. PUB. HEALTH LAW § 2782 (McKinney 2010):** Provides that confidential HIV-related information shall not be disclosed (with exceptions for disclosures to a health care provider or health facility when necessary to provide appropriate care or treatment to the individual, a child of the individual, a contact of the individual, or a person authorized to consent to health care for such contact). **N.Y. COMP. CODES R. & REGS. tit. 10, § 63.5(a) (2009):** Provides that no confidential HIV-related information shall be disclosed under a "general release," but disclosure is permitted under a "specific release" that has been approved by DOH **Disclosure of Mental Health Information:** **N.Y. MENTAL HYG. LAW § 33.13(d)–(f) (McKinney 2010):** Permits disclosure of PHI among mental hygiene law-licensed providers for treatment purposes without obtaining patient consent, but disclosure is limited to that information necessary in light of the reason for disclosure. **Additional State Laws** **N.Y. SOC. SERV. LAW § 364–j-2 (McKinney 2010)**: Allows for providers who meet certain standards set by DOH to receive supplemental payments for the increased cost of the use of EHRs. **N.Y. SOC. SERV. LAW § 367–a (McKinney 2010)**: Allows the Office of Health Information Technology Transformation to establish an EHR and electronic prescribing program to award incentives to physicians and pharmacies who implement such programs.
RI	**Rhode Island Health Information Exchange Act of 2008**, **R.I. GEN. LAWS §§ 5-37.7-1 through 5-37.7-15 (2009)**: Establishes a statewide HIE under state authority and specifies that the HIE will be opt-in, that is, patients and providers have the choice to participate in the HIE (7-4). The act also specifies that authorization is not required for release of information to public health authorities for a specified function, to health care providers for diagnosis or treatment in an emergency, and to the RHIO for operation and administrative oversight of the HIE (7-7). Additionally patients have the right to terminate participation and will be able to obtain disclosure reports as well as notices of security breaches (7-10). **Rules and Regulations Pertaining to the Regional Health Information Organization and Health Information Exchange** (effective Aug. 11, 2009) (not codified): Promulgated pursuant to the authority conferred under R.I. Gen. Law § 5-37.7. Establishes safeguards and confidentiality protections for Rhode Island's HIE in order to improve the quality, safety, and value of health care, keep confidential health information

State	Selected State Laws
	secure, and use the HIE to progress toward meeting public health goals. Provides that confidential health information should only be accessed, released, or transferred from the HIE in accordance with R.I. Gen. Law § 5-37.7, these Regulations, and any other applicable state or federal law or regulation.
WA	**WASH. REV. CODE ANN. § 41.05.031 (West 2009):** Directs specific state agencies to cooperate with the Washington State Health Care Authority in the establishment of health care information systems. **WASH. REV. CODE ANN. § 41.05.035 (West 2009):** Establishes pilot of a consumer-centric health information infrastructure and health record banks that will facilitate the secure exchange of health information.
WI	**WIS. STAT. ANN. § 146.82 (West 2009)**: Allows for the sharing of data with any health care provider involved in the patient's care without the informed consent of the patient. Allows a provider to release a portion of a patient health care record to: - Any person, if the patient or a person authorized by the patient agrees to the release - Any of the following, if the patient and person authorized by the patient are incapacitated or not physically available, if an emergency makes it impracticable to obtain patient consent, and if the health care provider determines the release is in the patient's best interest: ▪ to a member of the patient's immediate family, a relative, close personal friend, or an individual identified by the patient; that portion of the record that is directly relevant to the involvement of that person in the patient's care ▪ to any person, that portion of the record that is necessary to identify, locate, or notify a member of the patient's immediate family or another person who is responsible for the care of the patient concerning the patient's location, general condition, or death. **Exec. Order No. 303, Relating to the Governor's WIRED for Health Board (Dec. 1, 2009):** Creates the Wisconsin Relay of Electronic Data for Health Board (WIRED) to lay the groundwork for a statewide health data exchange. The Board must offer recommendations for technical infrastructure, oversight, accountability, long-term funding and common rules to protect patients by June 2010. The Board's activities will be funded by a $9.4 mil grant from the federal economic stimulus package.

APPENDIX C

Select Examples of Exchange in Other Developed Countries

Canada

Canada is currently developing interoperable electronic exchange for its 32 million residents. The system is being developed and funded primarily through Canada Health Infoway, a not-for-profit corporation whose members are the 14 federal, provincial, and territorial Deputy Ministers of Health.[1] Infoway supports HIT development by way of strategic investments in local and regional infrastructure projects. Specific consent policies are developed primarily at the provincial level and are largely *opt-out* systems with granularity.[2] The federal government has created a set of guidelines to promote further harmonization and development of consent policies nationwide – the Pan-Canadian Health Information Privacy and Confidentiality Framework[3] – and is developing a nationwide system to track consent directives through the Consent Directive Management Service.[4] Infoway plans to have fully interoperable EHRs for its entire population by 2016.[5]

In Canada, each of the 14 provinces is responsible for developing specific health privacy and security provisions. Almost all provinces are pursuing an *opt-out* system with varying levels of granularity, allowing implied consent to store and transmit health information for treatment purposes (the sole exception is Quebec, which requires a patient's express consent before sharing information).[6] Many jurisdictions currently require that patients be informed that their health information is being collected and how it may be used, as well as be given information regarding the security safeguards in place to protect their data. This notice may be given at any time before or at the time that the information is being collected, and can be given either directly by a provider or by way of posters, brochures, websites, or other educational materials.[7] It remains an open question what, if any, additional consent provisions are needed for secondary uses of health data, such as research and public health surveillance.[8]

---

[1] Canada Health Infoway. "2009-2010 Corporate Business plan," at 4-5 [hereinafter "Business plan"]. Available at: http://www.infoway-inforoute.ca/lang-en/about-infoway/about/annual-reports-and-business-plans.

[2] Canada Health Infoway. "White Paper on Information Governance of the Interoperable Electronic Health Record," March, 2007 [hereinafter "White Paper"]. Available at: http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf.

[3] Health Canada, "Pan-Canadian Health Information Privacy and Confidentiality Framework," January 27, 2005. Available at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php.

[4] Canada Health Infoway. "An Overview of the Electronic Health Record Privacy and Security Conceptual Architecture," March 2006, at 8 [hereinafter "Overview"].

[5] Canada Health Infoway. "2015: Advancing Canada's Next Generation of Health Care" [hereinafter "Advancing"]. Available at: http://www.v1.theglobeandmail.com/partners/free/infoway/pdf/2015%20Health%20care%20full%20report%20EN.pdf.

[6] Pritts, J. and K. Conner. "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 17.

[7] Canada Health Infoway, "White Paper," *supra* note 2, at 9-10.

[8] *Id.* at 13-14.

Because Canadian privacy policy is set at both the federal and provincial levels, Infoway has developed the Pan-Canadian Health Information Privacy and Confidentiality Framework in order to harmonize consent requirements. The framework specifies a set of core privacy principles upon which provinces can develop consent requirements (as the framework itself is not legally binding). These principles specify that the individual patient should be permitted to mask data by content or provider, and have been endorsed by all provinces except for Quebec and Saskatchewan.[9] Individual provinces are currently developing or updating their data segmentation rules to allow for as much or more granularity as specified in the Pan-Canadian Framework.[10] At present, many provinces permit highly granular consent options, allowing individuals to mask discreet data elements in addition to categories of data.

As of the end of the 2009 fiscal year, Infoway had approved the allocation of $1.58 billion (out of a total budget of $1.64 billion) toward 283 infrastructure projects undertaken at the provincial and local levels for building core electronic exchange systems, including client and provider registries, diagnostic imaging, drug and laboratory information systems, clinical reports, and immunization records. As of March, 2009, these functionalities had been integrated into the EHRs of 17 percent of Canadian citizens.[11] Originally, Infoway had aimed at extending these basic functionalities to 50% of the population by 2010, but the organization recently acknowledged that this timetable is unlikely to be met, and that EHR infrastructure development remains highly varied among provinces.[12]

Although Canadian privacy standards are set and health data is stored at the local and provincial levels, a nationwide consent system – Consent Directive Management Services (CDMS) – is being developed to obtain and track consent directives nationwide. Consent may be obtained either electronically or at the point of service and stored within the national CDMS, while the records themselves are maintained at the practitioner or regional level (depending on whether there is an existing regional electronic exchange infrastructure in place). Consent data moves through the system along with health information, and it is incumbent upon individual data custodians to maintain data security and uphold consent directives in accordance with the rules of the particular jurisdiction in which data is collected or received.[13] However, there remains some uncertainty as to how consent directives are maintained between provinces with differing granularity options.[14]

The Netherlands

The Dutch National Healthcare Information Hub (LSP), currently being implemented by the National Information and Communication Technology Institute for Healthcare (NICTIZ), is an *opt-out* system with granularity built around remote information hubs connected to a national, searchable database. This system, referred to as the "health care Google," maintains patient records at the practitioner or regional level (where regional electronic exchange already exists), and makes them available through a searchable database accessible to eligible practitioners

[9] Health Canada, *supra* note 3.
[10] Pritts, J. and K. Conner, *supra* note 6, at 20.
[11] Canada Health Infoway, "Business plan," *supra* note 1.
[12] Canada Health Infoway, "Advancing," *supra* note 5.
[13] Canada Health Infoway, "White paper," *supra* note 2, at 7-8.
[14] *Id.* at 11.

throughout the country (*i.e.*, those who meet a set of minimum security and functionality requirements).[15] The country is currently debating whether to require all practices to connect to the LSP.[16] 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 even opt out of the exchange entirely.[17]

The vast majority of practitioners in the Netherlands (97%) currently utilize EHRs in their practice.[18] The goal of the NICTIZ is to link all practices to the central database in the near future, although there has been delay due to many of the existing systems not meeting the LSP security requirements.[19] At present, efforts are focused on nationwide implementation of two "front-runner" functionalities – electronic medication lists and general practitioner's summary records.[20] Additional functionalities, such as acute care records and specialized systems chronic disease management, are currently being developed by NICTIZ.[21]

Within the Dutch LSP, citizens are identified by their Citizen Service Number (which functions as an analog to U.S. Social Security numbers).[22] In order to participate in the LSP, a practitioner must satisfy a set of security requirements. The individual practitioner is then connected to the LSP through certified commercial entities known as Healthcare Service Providers, which act as intermediaries between the provider and the hub and are responsible for tracking consent data and maintaining data security.[23] The system allows the option of opting out of electronic exchange entirely, as well as a high degree of granularity. All information is available for treatment purposes only; private entities such as insurance companies and employers cannot access the system.[24]

Months before the LSP became operational in November, 2008, a form was sent to Dutch citizens informing them of the system and giving them the choice to opt out. Some 330,000 (out of 16.5 million residents) did so, leading to concern over the implementation strategy, which was criticized for not adequately explaining the available granularity options and security measures in

---

[15] Pritts, *supra* note 6, at 3.
[16] HIMSS Enterprise Systems Steering Committee. "Electronic Health Records: A Global Perspective." August 2009, at 25. Available at: http://www.himss.org/content/files/200808_EHRGlobalPerspective_whitepaper.pdf.
[17] Pritts, *supra* note 6, at 42-45.
[18] Schoen, C et al. "A Survey of Primary Care Physicians in Eleven Countries, 2009: Perspectives on Care, Costs, and Experience." *Health Affairs Web Exclusive*, 5 November 2009, 1171-1183, at 1175. Available at: http://www.commonwealthfund.org/~/media/Files/Publications/In%20the%20Literature/2009/Nov/1336_Schoen_survey_primary_care_MDs_11_countries_HA_WebExcl_11052009_ITL_v2.pdf.
[19] Reis, Leo van der. "Lessons for the U.S. from the Netherlands' National Electronic Medical Records System." *eHealth International*, Vol. 5, No. 1, March 2009, at 37. Available at: http://www.ehealthinternational.org/vol5num1/Vol5Num1p35.pdf.
[20] Ministry of Health, Welfare and Sport. "ICT in Healthcare." Available at: http://www.minvws.nl/en/themes/ict-in-healthcare/default.asp.
[21] Spronk, R. "AORTA, the Dutch National Infrastructure." Available at: http://www.ringholm.de/docs/00980_en.htm.
[22] NICTIZ. "The National Healthcare Information Hub," February 15, 2006. Available at: http://www.sanita.forumpa.it/documenti/0/200/240/242/nictizuk3.pdf.
[23] National ICT Institute for Healthcare. "The National Healthcare Information Hub," at 2. Available at: http://www.sanita.forumpa.it/documenti/0/200/240/242/nictizuk3.pdf.
[24] Laurens J. van Baardewijk. "Electronic Health Record in the Netherlands: Afraid of the Unknown." *Amsterdam Law Forum*, August 2009, at 41.

place.[25] The system has also been criticized by both consumers and some physicians for not providing adequate security and privacy protections.[26]

Sweden

Sweden has recently started to implement a national health information exchange. In pursuance of this goal, the Swedish Parliament passed the Patient Data Act on July 1, 2008. The law aims to allow patients to decide who can access their medical record, while allowing care providers to communicate permitted patient data in the exchange securely.[27] In Sweden, 100% of medical records related to primary care services are digitized and 80 to 90% of those related to hospital care services are digitized.[28] The focus of the new exchange (NPÖ) is to allow these records to be shared between providers with appropriate patient consent to allow for increased preventive health improvements and correct diagnosis.[29] The exchange will contain several "information volumes," including diagnoses, care services, medicines, care contacts, care documents, status, care planning, and examination results.[30] It took one year after a contract was awarded for an HIT company to establish the legal context, patient consent, and technological capability for the system. These were completed on May 4, 2009.[31]

To meet the goal of the legislation, the Swedish system uses an *opt-in with restrictions* consent model. Sweden plans to place all digitized records on the central server for the exchange, but to allow patients to decide which physicians will ultimately be able to access their records in the database. A national level security database, "BIF," was designed to parallel the new national patient records system. This system will act as the authorization management service for secure information-handling across organizations in the health care sector. A digital communication system, "Sjunet," ensures that doctors use a special electronic ID card to log in, and keeps track of each instance that a health record is accessed. In order to view any healthcare record, health care professionals must have a "patient relation" with the patient, meaning the patient has given consent for them to look at his or her health record. Patients not only have the option of restricting which professionals can access their record, they can also restrict the period of time after the visit that the professional can continue to access it. Sweden also restricts health care professionals on how much of the record they can see. However, county councils and municipalities, not patients, designate which professionals can see which parts of the record. The system has a "break the glass" provision that allows health care professionals to access the record in an emergency, but the access will be logged and professionals will have to explain why they needed to view the information.[32]

The Swedish government began to implement this system in May 2009 on a trial basis within the Municipality and County Council of Örebro. After evaluating its establishment and making

---

[25] *Id.* at 42.
[26] Reis, *supra* note 19, at 36.
[27] National Patientöversikt. "Focus on Delivery." Available at: www.npö.nu.
[28] Elfgren, E. L. "Prevention progression," *Public Service Review: Health 20*, July 2009, p. 1.
[29] *Id.*
[30] National Patientöversikt, *supra* note 27.
[31] Intersystems Press Release. "Tieto and InterSystems Create Swedish National Electronic Health Record," June 3, 2009. Available at: http://www.intersystems.com/press/2009/sweden_print.html.
[32] Elfgren, *supra* note 28, at 1.

appropriate changes, the government's goal is to establish the system gradually in additional counties and municipalities before extending it to the rest of the country.[33]

[33] National Patientöversikt, *supra* note 27.