Architectures and Processes for Nationwide Patient-Centric Consent Management

P. Mork, A. Rosenthal, and J. Stanford

The MITRE Corporation, 7515 Colshire Drive, McLean, VA 22102 USA

Public Release Approval Case Number 11-2683

Abstract

Before electronic health information can be shared, the patient's consent must be obtained. However, the current paper-based process is insufficient at a nationwide scale. As an alternative, we propose an architecture for *patient-centric* consent management based on our experiences developing a prototype of such a system. We describe how our approach provides patients with a single location for specifying their privacy preferences covering a variety of possible uses of their personal health information (including emergencies and research). Then, we describe how a record holder uses the consent service to obtain a set of privacy constraints that need to be enforced for a particular request (i.e., the consent service provides value by simplifying the patient's preferences down to the minimum necessary in a given context). With today's systems, many of these constraints will need to be verified manually, but we also describe how, with incremental progress, further automation is possible by allowing the consent service to interact with ancillary knowledge sources and enforcement engines. We illustrate our architecture through a variety of use cases that we are able to support. Finally, we conclude by demonstrating that all of the stakeholders have an incentive to participate because they all derive benefits from our approach.

1. Introduction

As the nation moves towards widespread adoption of electronic health records (EHRs), one of the most frustrating problems is how to obtain patients' consent to share data with other parties. The business case for interoperable EHRs rests in their ability to exchange data to support patient care, clinical research, and biomedical surveillance. However patients have a justified fear of exposing their health information to third parties and consider the ability to control the use of their data to be critically important. In one survey, "ninety-one percent of respondents agree that 'how my health information is handled online is so important to me that the online services should always require my express agreement for each use.' Most (68.3 percent) say they 'strongly agree' with this statement." [2 Mark1] This paper proposes a technical approach to meet many of the consent management desiderata established by the Office of the National Coordinator for Health Information Technology (ONC) [1 Gold1, 2 Mark1]. We also discuss the policy issues that arise when sharing health information on a nationwide scale, such as the Nationwide Health Information Network.

The current state-of-the-practice is for each provider to maintain a stack of paper consent forms that cover a narrow range of anticipated data sharing. Unfortunately, the already-signed forms may not address common information exchanges, such as future referrals, nor can they handle the unanticipated data sharing needs of secondary (research) use. Some record holders insist on signed paper, perhaps because they do not trust that an easily forged fax sufficiently protects them. A service that supplied authenticated consent would avoid this problem. When a consortium of New York City hospitals agreed to upload all data to their HIE and then rely on each others' claim to have an authentic consent, sharing increased fourfold. [10 GSK1]

Paper forms are, essentially, a *provider-centric* mechanism for managing patient consent. Each provider institution provides its own form, usually notifying patients of the institution's HIPAA data sharing policies, but not allowing patients to express their own privacy preferences. As an alternative, in this paper, we propose a *patient-centric* electronic system for managing consent, where the patient expresses their own privacy preferences in generalized terms, and these preferences restrict the response to each data release request. Patient-centric consent management benefits all of the participants in a health information exchange: a) patients can establish their privacy preferences once, and the service appends them automatically to each request transaction; b) record holders meet demands to give patients control over releases of their data, can demonstrate the justification for each release, and do not need to elicit a new consent for each new exchange of health information; and c) requests are less likely to be blocked due to lack of consent and recipients know what privacy constraints apply to the health information they receive. Further, a patient-centric consent management system would also relieve data providers of a major administrative burden from handling paper forms. [1 Gold1, page ES-2].

We have prototyped a system in which a patient manages a policy preferences document that can be applied to many data sharing instances and can be referenced by any record holder to obtain current, actionable consent preferences at any time. This allows patients to communicate their privacy preferences to organizations that have their electronic health information, but of which the patients are not necessarily aware, such as independent laboratories, imaging centers, and health information exchanges (HIEs). By providing nationwide access to patient consent policies, we give patients a method to control the release of their data without having to track down every potential record holder.

In this paper, we show how to build a patient-centric consent management system by describing the various capabilities that such a system would include. We focus on the *consent service* that manages a patient's privacy preferences. The service's two main duties are to help patients manage their preferences, and upon request, to send applicable constraints to the record holder. We anticipate that nationwide consent management will require many interconnected capabilities to manage identity, credentials, etc. and describe how these capabilities interact. To demonstrate efficacy, we describe several use cases that the proposed architecture supports.

The remainder of this paper is organized as follows. Section 2 describes the background and related work. Section 3 describes the capabilities needed to manage patient consent and how to assemble those capabilities into a consent management system. Section 4 describes how our proposed architecture handles several common use cases, with varying degrees of automation. In Section 6 we summarize the benefits of patient-centric consent management as realized by our architecture and comment on future work.

2. Background

The ubiquitous paper consent forms on clipboards do not effectively convey a patient's preferences. Often they make no attempt to do so; the form merely informs the patient (in non-negotiable language) about the provider's policies regarding releasing data to various payers and public health agencies. If a patient needs to have his records forwarded to another physician, the patient often has to complete additional paper forms for each request—a process that is inefficient and prevents automated sharing of electronic health information (such as for participation in clinical research or sending data to personal health records (PHRs)). The completed paper forms are simply filed away for defense in case of a lawsuit. One wonders what happens if a patient scrawls amendments to the boilerplate: does anyone even notice?

Providers supply the consent forms, explain them to patients and bear the burden of enforcement, so their concerns tend to be favored over the patients' concerns. To minimize burdens, they rarely provide the ability to express nuanced consent preferences [4 Mark2]. Despite this, paper-based consent management is still a hassle for all concerned. We conclude this section by describing efforts to transition to electronic management of patient consent.

Integrating the Healthcare Enterprise (IHE) has developed a conceptual model for consent management [9 IHE1] to be integrated with EHRs. Their provider-centric work is complementary to ours. They describe what each record holder can implement, while we ask what each patient wants, to apply across all their record holders. As they standardize constructs, some could be incorporated into user interfaces, to promote easy enforcement. Long term, tools will assist in mapping patients' constructs to constructs the record holder has declared they support.

Goldstein, et al. [1 Gold1] discuss the usual privacy options a patient may be given: none, opt-in, opt-out, opt-in with restrictions and opt-out with restrictions. This paper notes that patients perceive a need for granular options to restrict access to their health information based on such aspects as diagnosis, source, recipient, etc. However, few (if any) of the systems surveyed in Goldstein allowed patient-specified granular restrictions. Supporting specification of this granularity, as part of a general rule, is one of our contributions.[1]

To explore electronic alternatives, ONC's Security and Privacy Tiger Team [13 ONC2] discussed the state-of-the-art in automated consent management systems, with testimony by several organizations working on such systems. In particular, InterSystems has a system that allows the patient to specify which diagnosis codes can be released to whom (within that organization). [14 Inter1] This within-organization focus is common among vendor offerings. Preferences specified in one location cannot be transferred to another system, resulting in coordination challenges as highlighted by HITSP.

The President's Council of Science and Technology Advisors (PCAST) report [16 PCAST1] recommended that primary care providers explain consent policies and capture patient preferences face to face, but that patients should also have access to a helpful web interface. Though we began this work two years before the PCAST report was

[1] We provide a means to specify the granular privacy preferences and to advise record holders of those that apply to each record request. It is an open problem to automatically screen each record to determine if any of the privacy-protected concepts are present or implied.

published, the consent system we describe here can ease these tasks with its intuitive presentation of preferences and by storing and presenting educational materials.

Halamka would like to encourage patients to delegate authority to clinicians, to share their data as desired. He notes that physicians would want to obtain the other clinician's permission (to accept patient delegation) before sharing (once to cover all patients), and suggests a "friends list" as a mechanism. [15 Hal1]

Our work draws on the privacy use cases established by the Health Information Technology Standards Panel (HITSP), sponsored by the American Standards Institute [6 HITSP1] augmented by ONC guidance [7 ONC1]. The HITSP Privacy Consent Directive Working Group presents key questions regarding the *"cross validation and verification of conflicting consents:*

- *What is the most recent/latest consent from a patient?*
- *Does that override the other consents for specific data, specific purpose?*
- *Where can I find the various consents issued by a consumer to perform cross-validation and verification?"* [8 Moehrke1]

Our patient-centric consent architecture with a single preferences document for each patient answers all of these questions.

3. Patient-Centric Consent Management

This paper explores an architecture for consent management centered on the patient. It captures each patient's preferences in a single location, accessible by multiple parties.

- We provide the *patient* with an intuitive interface with which to capture their privacy preferences.
- We provide *record holders* (often a health care provider, but not necessarily) with a service that allows them to retrieve the patient's current preferences, along with relevant legal restrictions (e.g., state privacy rules based on the location of the provider or the patient).

This section first describes the capabilities of the consent service, and then capabilities on which it relies: identity management (Section 3.2Error: Reference source not found) and ancillary knowledge sources (Section Ancillary). Finally, it describes the overall architecture and workflows, in two configurations. The utility of this approach is shown via use cases in Section 4.

3.1. Consent Service Capabilities

The consent service associates each patient with a set of rules that identify circumstances where health information can be released. The rules may reference the request itself, the content of the health information to be released, and additional knowledge (such as affiliations and referrals). Most rules specify a condition under which release is permitted; others define a reusable condition or state default protections.

3.1.1. Establishing Privacy Preferences

Patients establish their preferences through a graphical user interface. Our prototype includes an interaction that first prompts the patient to establish a *scenario*, which consists of a purpose and a set of recipients. She is then prompted to indicate her privacy preferences for requests fitting that scenario. For example, for treatment provided by her primary care physician (PCP), she might stipulate that all information can be shared with her PCP. But, for a referred physician (again, for treatment purposes), she may stipulate that allergies and medications may be shared, except those that pertain to mental health treatment.

However, we anticipate that different organizations will supply their own UIs to the consent service. By storing the patient's preferences as a set of logical rules, we can support a wide range of UIs. A provider organization could give its patients a UI that produces rules that execute easily in its EHR; advocacy groups could develop UIs designed to address their concerns. These UIs can be tailored for the gamut of patients, with patient-friendly natural language explanations of technical terms, and templates for patients with differing concerns.

In addition, a patient can specify proxies who are authorized to consent to data sharing on behalf of the patient (e.g., if the patient is uncomfortable with electronic consent management or is a minor). A patient might even identify a trusted physician as a proxy (assuming the physician is willing), with partial rights to authorize individual releases or to make permanent changes, the former as discussed by Halamka, above.

3.1.2. Managing Requests

A request for patient data typically describes the data requested, plus values for numerous attributes; our current request attributes include *purpose, requestor, recipient, record holder,* and *patient consent ID*. The consent service receives the request, retrieves the patient's preferences, and forwards them to the record holder. Drawing on information in the request message and from ancillary information sources, it can simplify before forwarding, excluding preferences that are inapplicable (e.g., wrong purpose, not an emergency request) and pre-evaluating some conditions (e.g., is the requestor the patient's PCP?). In some cases, (increasingly, as standards and ancillary sources improve), the service will make a final decision to allow or reject the request, but often, it will forward simplified constraints for the record holder to evaluate.

The record holder needs to enforce the constraints it receives. We aim to serve record holders with advanced electronic capabilities, plus others who are largely manual. Moreover, even an advanced system needs to be able to "ask a human" when faced with subtle content judgments. Therefore they should be able to receive these constraints in a machine-interpretable format (such as XACML [17 XACML1]) *and* in a human-readable format.

Finally, the consent service maintains an audit log of all activity. This audit log indicates:

- All information in the request message
- Any additional factors that influence the decision-making process (e.g., the patient told the consent system that Dr. Jones is her PCP)
- Endorsement of this request from the patient or proxies (if applicable)
- The constraints sent to the record holder

The patient can interact with the consent service to see the history of requests, or to define alerts that notify him of requests that meet specific criteria (e.g., a request to access the results of an HIV test). These are capabilities of the consent service, and do not involve or burden the record holder.

To manage consent on a large scale, additional capabilities are needed, to make the system trustworthy, and to obtain ancillary information that belongs in external sources, not in EHRs. These are addressed in the next two subsections.

3.2. Consent Identifiers

This section addresses the need to link medical identities. To process any remote request, the name used by the requestor needs to match the right patient at the record holder. This familiar issue of linking records actually occurs before consent is checked—the record holder determines which patient's data matches the patient described in the request. [18 MARK3] Consent introduces a new requirement, namely to ensure that the preferences of the correct patient are enforced. We need a link between the record holder's patient identity and a consent service patient identity.

To establish such a link, the first step is for the patient to establish an identity with the consent service, much as at an eCommerce site. Then, the patient authenticates with the record holder (in person or by securely logging into the record holder's system). The patient then provides the record holder with his consent identifier, which the record holder stores. Once this is established, the record holder knows that the preferences sent by the consent service correspond to this patient.

A global consent identifier for each patient would make it easier to correctly link their data across different providers. Some patients will appreciate the benefit in reducing errors, while others object to the reduction in privacy. We can satisfy both groups. Upon request, the consent system creates an alias that a patient can give to a record holder; a patient might give a distinct identifier to each record holder, or alternatively might give distinct identifiers only in sensitive circumstances (e.g., at a substance abuse or reproductive health center). When records at different record holders contain different consent identifiers, comparing those identifiers will not reveal the link. The consent system knows the links, but does not make them public.

Our design avoids several pitfalls. First, our approach does not depend on a universal medical record number or national identification number, nor does it create one for unwilling patients. Also, at each record holder, there is only one consent identifier per patient, and it can be bound to the record holder's master identifier for that patient, rather than requiring links to individual records.

3.3. Ancillary Knowledge Sources

The consent service also relies on external ancillary knowledge, such as the identity of a patient's PCP, the PCP's referrals, a physician's specialty, and hospital affiliations. These might be managed by, respectively, the patient, the PCP, a state license board, and the hospital. These knowledge sources will often be incomplete, unstandardized, and uncertified. Since the consent service makes no promise of completeness, it can work in such environments and be improved incrementally. For sources it does reach, it simply passes on the knowledge they offer. In view of these limitations; patients need to be counseled (and UIs customized) to avoid creating policy clauses that require too much work for record holders to check.

Having retrieved whatever ancillary knowledge is available, the consent service matches that information against the patient's preferences, allowing the consent service to further simplify the constraints it forwards to the record holder. When ancillary knowledge is not available, the record holder instead relies on manual enforcement of the implied constraints. For example, if the recipient's credentials cannot be supplied by an ancillary knowledge source, then the record holder must obtain that information manually (e.g., by calling the recipient's institution).

Once ancillary knowledge is available electronically, the record holder needs to determine if it trusts the source of the information. Standard trust infrastructure (such as is used for PKI) can be used to determine if ancillary knowledge is provided by a trusted source.

3.4. Sample Architecture

Figure : Sample architecture for retrieving a patient's consent. The record holder (R) forwards the request to the consent service (C), which uses a policy reasoner to determine which privacy constraints R needs to enforce using a XACML engine.

The capabilities described above can be combined in multiple ways to instantiate a consent management system. In this section, we present two sample configurations, one fully electronic and one largely manual. They can coexist, with each site automating as much as is appropriate.

Configuration A: Figure 1 demonstrates one possible configuration for a consent management system, utilizing substantial automation (attained today in some leading edge systems) and standardization (present within some established provider networks). It assumes that requests arrive in formatted messages, and that the record holder (R) can access health information about their patients via a single EHR interface. To support consent, this EHR has been augmented in four ways.

- The EHR maintains a consent identifier for each patient. (For example, the record holder's master index might contain the identifiers, and all records are logically connected to that index).
- An extra piece of software forwards requests for health information to the consent service to retrieve and simplify the patient's preferences.
- Components of the patient's record are tagged with metadata that describe their contents. These tags describe the type of information (also useful for querying and indexing) in that component and any potentially sensitive topics that apply to the component.
- A security module (e.g., a XACML engine) enforces the privacy constraints provided by C based on the metadata stored by R.

In addition, there is a consent service (C) that maintains the patient's privacy preferences and related audit logs in a consent database. C receives the consent identity used by the record holder, finds the proper consent account (resolving aliases), and connects with external sources to obtain ancillary knowledge. This is the architecture we prototyped, as a natural extension to today's practice.

Configuration B: Consider a provider who relies on paper records (i.e., R does not have an EHR) or has several silos that a human must query manually. In this case, the overall architecture is still applicable, but the interactions with C and with the records will involve a human. For example, a medical records specialist would enter information about the recipient and request into a web form hosted by the consent service. Instead of receiving machine-interpretable results, R would receive a human-readable version of the patient's preferences, to be interpreted by the records specialist, who may access ancillary sources through their websites.

4. Use Cases

To show how a consent management system works and provides our claimed benefits, we consider six use cases (several adapted from HITSP). For generality, the descriptions allow for a range of automation both in terms of the record holder's capabilities and the collection of ancillary knowledge. This robust treatment allows the system to improve, without changing the use cases or the overall architecture. The explanations highlight configuration A.

1) A patient establishes his privacy preferences for the first time.
2) A specialist (Dr. Lee) was unable to obtain the patient's health information. She asks the consent system to "fix this" (i.e., to request that patient to appropriately modify his existing preferences to allow access). The patient is willing and does so.
3) After the change, and on subsequent visits, Dr. Lee asks for recent records about the patient.
    a. The patient's consent releases all health information to treating physicians.
    b. The patient's consent excludes data that is known to relate to mental health.
4) The PCP refers the patient (who is not physically present) to a new provider, Dr. Jones. The record holder seeks to send information to Dr. Jones before the patient's visit.
5) The patient is admitted to the emergency department (ED), and the ED requests the patient's medication and allergy data.
6) A researcher wants to screen kidney patients to find ones suitable for a new clinical trial. Many patients have consented to have their data screened by accredited researchers, either broadly or for specific kinds of research.

In the first use case, the patient connects to the consent service using a browser (e.g., at home, at the library, on a mobile phone, or in a kiosk in the waiting room). Because the patient does not have an existing consent account, he is given a new consent identifier. Next, he is walked through a series of wizards to establish his initial privacy preferences. We envision wizards tailored to several common situations, for example, treatment by the PCP, emergency treatment, and determining with whom the patient has a treatment relationship. Extending the suggestions from the IHE report discussed earlier [9], we hope that organizations will establish reasonable prepackaged options for the patient to select from. The system can also support the current style of narrow consents—each preference can restrict applicability to one record holder, one requestor, or one request although we would discourage this option.

In the second use case, the policy reasoner determines one or more plausible modifications to the patient's current preferences, and the consent service contacts the patient for choice and approval. For example, it might determine that plausible choices are a) to declare a treatment relation with this specialist; b) to approve this single release, or c) to create a new rule for Dr. Lee or for all specialists. Note that Dr. Lee did need not see the existing preferences. Once the update is saved, it will apply to all future requests.

For case 3a, the consent system receives the request, determines that Lee is an MD, and has a treatment relationship with the patient. It authorizes release and writes the request and the ancillary knowledge employed to the audit log. With less automation, the record holder might know that Lee is a doctor, and obtain the remaining ancillary information manually.

Now the consented request is processed. For the advanced record holder (configuration A) the request is sent to their EHR and the results assembled. In configuration B, a medical records person receives the request, forwards a message to the consent system, and receives the approval message. She then formulates requests to the various systems at her site (possibly including paper) and assembles a response. In either case, the result is then securely transmitted to the recipient.

For case 3b, the consent system tells the record holder "release is approved except for information known to relate to mental health." The retrieval from the EHR system includes the restriction "not tagged as mental health." If mental health information is kept in a segregated data store, that store will not be queried; if tagged, mental health data will be redacted from the response.

The above restriction was provider centric, allowing the provider to define what they knew. A more privacy conscious patient might issue a different consent, allowing release of data "not obviously" related to mental health. This will be harder to enforce One might expect the record holder to filter out obvious cases, e.g., a problem list including the diagnosis of "bipolar disorder." Natural language clinical notes would require further manual filtering. For providers performing manual retrieval, even if records are tagged, they might need to be checked individually. Due to this burden; the provider might be likely to refuse to process queries with privacy constraints.

In the fourth use case, the consent system first uses the record holder as an ancillary knowledge source to verify that Dr. Jones is a clinician and that the patient's PCP has referred the patient to Dr. Jones. As in case 3a, once this information has been retrieved (from a source the record holder trusts), the consent system returns any remaining privacy constraints that need to be enforced. In general, the consent service returns the patient's preferences (for this situation) to the record holder, with an indication of all the checks it has completed. The record holder is then responsible for enforcing the remaining constraints.

In the fifth use case, an Emergency Department nurse in Utah initiates a "break the glass" request to retrieve a patient's medications and allergies from a California record holder. The consent service returns the patient's preferences for "break the glass" scenario; this patient ignored the question, so the state default applies. For example: For a request from a known emergency care facility by a credentialed professional, release data for treatment.

The consent service again collects relevant ancillary information. Suppose it succeeds in verifying the first clause, a known ED, but cannot interpret responses from Utah professional registries. The record holder's staff receives the remaining constraint ("a credentialed professional") and recognizes that surfing to find the Utah agency for ED nurses will delay the response. They apply the California default, which is assumed to be "credential checks fail only if one can access a registry responsible for this category, and it denies that the person is credentialed in this state. Absent such access, the "credentialed" clause is ignored. They may now release the relevant records.

Another patient might have overridden the state default to forbid emergency releases to the particular clinic where an abusive spouse works and further require exclusion of information that is known to concern mental health. (The UI wizard had persuaded her to accept this automatable filtering to avoid dangerous delays.)

For the sixth case, many patients have stipulated (via a UI option) that they are willing to let their information be employed to match them to clinical studies; some have even offered to share deidentified data without being contacted. To recruit, the researcher first asks the consent service to search across all patients to find those who have consented to recruitment for kidney research. Second, the EHR performs eligibility screening based on demographics, dates, diagnoses, and treating clinicians. The eligible candidates may then be sent invitations to contact the researcher. For the most willing patients, the EHR may be sent a consented request to send deidentified data directly to the researcher.

Today's paper-based system offers no effective way for researchers and suitable willing subjects to find each other, nationwide. Full automation is needed, because record holders have limited desire to process such requests, especially from outside their institution. The search process need not reach every suitable patient—a small fraction from a nationwide population may suffice (e.g., type 2 diabetes patients under age 60, taking certain drugs). Once consent is established, studies that do not require the patient's physical presence might be fully automated and thus enormously cheaper.

5. Conclusions and Future Work

We have described a path toward patient-centric consent management. Patients, record holders, and requestors all benefit, and thus have incentives to participate.

Patients get a single location for expressing their consent preferences, so they do not need to separately notify every record holder. They gain flexible user interfaces that go beyond provider legalese or HIPAA forms, making it easier to review and modify their preferences. The UIs are available over the web anytime, anyplace, not just at the provider's check-in desk. Relevant federal or state regulations are visible from the same interface, allowing patients to see how their preferences interact with legal constraints. UIs can exist on mobile devices, can incorporate record holder idioms, and compete for patient adoption. Patients get better care because their providers can better share information.

Record holders are freed from maintaining a stack of consent documents and can apply the patient's generalized preferences without contacting the patient again. They receive an authenticated, up to date consent statement, not a fax. They need not interpret privacy conditions attached to data they have imported, nor attach such conditions to data they export. Logical simplifications help reduce the complexity of dealing with any one situation. Also, the consent service may be able to evaluate some claims in the request, e.g., that the request really comes from an emergency department, or from an on-call substitute.

Requestors benefit because they can seek information from multiple record holders without pair-wise consent negotiation. By reusing existing generalized consents, they can get the data they need, without waiting for the patient in to sign a new document. The consent system can even give them a preview of what it will send the record holder (if that preview is consented), thus reducing unexpected rejections. Data may also be pushed rather than pulled; the requestor, record holder, and recipient can all be different entities. For a referral, a record holder could initiate a request to transfer information to the recipient; the policy can examine both the requestor's and the recipient's privileges.

Finally, the consent service creates an audit log of requests it has processed. Patients can access a complete record of approved, denied, and pending requests, and see associated rationales. Patients can further enhance their control by setting up alerts. Record holders and requestors get a certified record of their actions, enhancing compliance and strengthening evidence for those who currently do not have digital logs, and allowing others (if they wish) to reduce audit efforts. To avoid volume and exposure, the log does not contain medical data from EHRs.

Additional UI research is needed to establish a range of user interfaces, based on device (such as paper, desktop computer, or smart phone), the degree to which patients wish to customize their preferences, and the nature of their concerns. UI research is also needed to help the patient reuse partial descriptions. Patients also need help in understanding terminology (e.g., "mental health") and to reason about the impact of their preferences.

We are beginning to explore the amount of simplification actually obtained by the policy reasoner. Approaches for including government stakeholders and for dealing with uncertain enforcement (e.g., to say they prefer release over confidentiality only in emergencies) also need elaboration and testing. Also, we are exploring how best to include discovery services into the architecture with suitable enforcement of privacy preferences.

Finally, we have begun researching requirements for standardization. We can exploit other groups' work on data sharing to automatically translate consent constraints to EHR queries. However, we also need to enable interoperability to allow patients to switch consent systems, and to enable competition and innovation in individual components, such as UIs. For ancillary knowledge sources, interface standards, governance, and certification need to be addressed.

Perhaps most importantly, one could build a useful consent system today. Our architecture consciously avoided depending on universal participation, employment of data standards, record holder automation, or ancillary data completeness. Progress in these areas would permit greater automation, but in the near term, all tasks can be processed partly manually, with incremental automation.

Of course, no consent system can make everything easy. In particular, we cannot make it easy for record holders to enforce highly complex rules with dependencies on ancillary information that is hard to locate or verify. Nor are constraints based on content sensitive topics that the record holder has not tagged or segmented easy to enforce—efficiency depends on improving the systems that interact with a consent service.

Author biographies

Peter Mork has conducted research in data interoperability, discovery and privacy and consulted for a range of HHS agencies. He received a Ph.D. from the University of Washington (Seattle).

Arnon Rosenthal has worked on data sharing, security, and administration, at several industrial research centers and universities. He received a Ph.D (Computer Science) from the University of California (Berkeley)

Jean Stanford has worked in biomedical informatics for 35 years, for clients ranging from hospitals to payers to major government organizations (including the Office of the National Coordinator).

Acknowledgments

Patti Reynolds provided invaluable editorial assistance. Ivan Ramiscal, Keri Sarver, Jaya Tripathi, and Jeremy Walsh implemented the prototype, and helped clarify many ideas.

References

[1 Gold1] Goldstein, M.M., and Rein, A.L. Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis. [Internet] Department of Health Policy, School of Public Health and Health Services, The George Washington University Medical Center [2010 March 23] [cited 2011 April 4] [93 pp.] Available from: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1147&parentname=CommunityPage&parentid=32&mode=2&in_hi_userid=11113&cached=true.

[2 Mark1] Markle Foundation. Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve Their Health. [Internet] [2008 June 1] [cited 2011 April 4] Available from: http://www.connectingforhealth.org/resources/ResearchBrief-200806.pdf.

[3 Blum1] Blumenthal, D. Stimulating the Adoption of Health Information Technology. N Engl J Med. 2009: (360): 1477-1479. Available from: http://content.nejm.org

[4 Mark2] Markle Foundation. Connecting for Health Common Framework, Policy Notice to Consumers Appendix A. [Internet] [2008 June [cited 2011 April 4] [about 10 pp.] Available from: http://www.markle.org/health/markle-common-framework/connecting-consumers/cp2.

[5 ARRA1] Public Law: American Recovery and Reinvestment Act of 2009, Pub. L. No 111-5 (February 17, 2009).

[6 HITSP1] HITSP/ISO3. HITSP Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification, Version 4.0. [2008 December 18] [cited 2011 April 4] [122 pp.] Available from: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=1&PrefixNumeric=03.

[7 ONC1] Consumer Preferences Draft Requirements Document. [2009 October 5] [cited 2011 April 4] [42pp.] Sponsored by U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology. Available from: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1202&PageID=16769&mode=2.

[8 Moehrke1] Moehrke, J. Consumer Privacy using HITSP TP30. [2010 October 20] [cited 2011 April 4] [27 pp.] Available from: ftp://ftp.ihe.net/.../ Consumer%20Privacy%20–%20using%20HITSP%20TP30%20-10202010.pptx.

[9 IHE1] Integrating the Healthcare Environment (IHE). Basic Patient Privacy Consents. [Internet] [cited 2011 April 4] [about 6 pp.] Available from: http://wiki.ihe.net/index.php?title=Basic_Patient_Privacy_Consents.

[10 GSK1] N. Genes, J. Shapiro, G. Kuperman "Health Information Exchange Consent Policy Influences Emergency Department Patient Data Accessibility", Proceedings of AMIA Symposium, 2010

[11 HIPAA1] Public Law: Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191 (August 21, 1996).

[12 Priv1] Public Law: Privacy Act of 1974, Pub. L. 93-579 (December 31, 1974).

[13 ONC2] ONC Privacy and Security Tiger Team. Consumer Choice Technology Hearing, June 29, 2010. [cited 2011 April 6], Available from: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910

[14 Inter1] Michael LaRocca, Intersystems Corporation Written Public Testimony, Consumer Choice Technology Hearing, June 29, 2010, p. 3

[15 Hal1] Halamka, J. Solving Secure Transport. [Internet] [place unknown] [2010 January 19] [cited 2011 April 5]; [about 1 screen]. Available from: http://geekdoctor.blogspot.com/2010/01/solving-secure-transport.html.

[16 PCAST1] President's Council of Advisors on Science And Technology, "Report to the president: Realizing the full potential of health information technology to improve healthcare for Americans: The path forward." , December 2010, p. 46

[17 XACML1] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#CURRENT

[18 MARK3] Markle Foundation "Linking Health Care Information: Proposed Methods For Improving Care And Protecting Privacy", Working Group on Accurately Linking Information for Health Care Quality and Safety, February 2005