4-23-2014

Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities

Claudia Allen
Greater Cincinnati HealthBridge, Inc., callen@healthbridge.org

Terrisca R. Des Jardins
Southeastern Michigan Health Association, Terrisca@hotmail.com

Arvela Heider
HEALTHeLINK, arvela@holark.com

Kristin A. Lyman
Louisiana Public Health Institute, klyman@lphi.org

See next pages for additional authors

The Electronic Data Methods (EDM) Forum is supported by the Agency for Healthcare Research and Quality (AHRQ), Grant 1U18HS022789-01. eGEMs publications do not reflect the official views of AHRQ or the United States Department of Health and Human Services.

Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities

Abstract

Purpose: Unprecedented efforts are underway across the United States to electronically capture and exchange health information to improve health care and population health, and reduce costs. This increased collection and sharing of electronic patient data raises several governance issues, including privacy, security, liability, and market competition. Those engaged in such efforts have had to develop data sharing agreements (DSAs) among entities involved in information exchange, many of whom are "nontraditional" health care entities and/or new partners. This paper shares lessons learned based on the experiences of six federally funded communities participating in the Beacon Community Cooperative Agreement Program, and offers guidance for navigating data governance issues and developing DSAs to facilitate community-wide health information exchange.

Innovation: While all entities involved in electronic data sharing must address governance issues and create DSAs accordingly, until recently little formal guidance existed for doing so – particularly for community-based initiatives. Despite this lack of guidance, together the Beacon Communities' experiences highlight promising strategies for navigating complex governance issues, which may be useful to other entities or communities initiating information exchange efforts to support delivery system transformation.

Credibility: For the past three years, AcademyHealth has provided technical assistance to most of the 17 Beacon Communities, 6 of whom contributed to this collaborative writing effort. Though these communities varied widely in terms of their demographics, resources, and Beacon-driven priorities, common themes emerged as they described their approaches to data governance and DSA development.

Conclusions: The 6 Beacon Communities confirmed that DSAs are necessary to satisfy legal and market-based concerns, and they identified several specific issues, many of which have been noted by others involved in network data sharing initiatives. More importantly, these communities identified several promising approaches to timely and effective DSA development, including: stakeholder engagement; identification and effective communication of value; adoption of a parsimonious approach; attention to market-based concerns; flexibility in adapting and expanding existing agreements and partnerships; and anticipation of required time and investment.

Acknowledgements

Support for the development of this paper was provided by the Commonwealth Fund and by the Office of National Coordinator for Health Information Technology Beacon Community Cooperative Agreement Program. The opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the United States government. The authors would like to acknowledge the following individuals and organizations for their support of this collaborative writing effort: Anjum Khurshid, Liam Bouchier, Gaurav Nagrath, David Kulick, and Megan Tulikangas of the Louisiana Public Health Institute; HealthInfoNet; and Eastern Maine Healthcare Systems. The authors would also like to thank Melissa Goldstein of George Washington University for her early review and feedback on the manuscript.

Keywords

Governance, Data Use Agreements, Health Information Exchange, Health Information Technology

Authors
Claudia Allen, *Greater Cincinnati HealthBridge, Inc.*; Terrisca R Des Jardins, *Southeastern Michigan Health Association*; Arvela Heider, *HEALTHeLINK*; Kristin A Lyman, *Louisiana Public Health Institute*; Lee McWilliams, *EMHS*; Alison L Rein, *AcademyHealth*; Abigail A Schachter, *AcademyHealth*; Ranjit Singh, *State University of New York*; Barbara Sorondo, *Eastern Maine Healthcare Systems*; Joan Topper, *Geisinger Health System*; Scott A Turske, *Southeastern Michigan Health Association*.

Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities

Claudia Allen, JD;[i] Terrisca R. Des Jardins, MHSA;[ii] Arvela Heider, PhD;[iii] Kristin A. Lyman, JD, MHA;[iv] Lee McWilliams, MA;[v] Alison L. Rein, MS;[vi] Abigail A. Schachter, BA;[vi] Ranjit Singh, MB BChir, MBA;[vii] Barbara Sorondo, MD;[v] Joan Topper, BS;[viii] Scott A. Turske, BA[ii]

Abstract

Purpose: Unprecedented efforts are underway across the United States to electronically capture and exchange health information to improve health care and population health, and reduce costs. This increased collection and sharing of electronic patient data raises several governance issues, including privacy, security, liability, and market competition. Those engaged in such efforts have had to develop data sharing agreements (DSAs) among entities involved in information exchange, many of whom are "nontraditional" health care entities and/or new partners. This paper shares lessons learned based on the experiences of six federally funded communities participating in the Beacon Community Cooperative Agreement Program, and offers guidance for navigating data governance issues and developing DSAs to facilitate community-wide health information exchange.

Innovation: While all entities involved in electronic data sharing must address governance issues and create DSAs accordingly, until recently little formal guidance existed for doing so – particularly for community-based initiatives. Despite this lack of guidance, together the Beacon Communities' experiences highlight promising strategies for navigating complex governance issues, which may be useful to other entities or communities initiating information exchange efforts to support delivery system transformation.

Credibility: For the past three years, AcademyHealth has provided technical assistance to most of the 17 Beacon Communities, 6 of whom contributed to this collaborative writing effort. Though these communities varied widely in terms of their demographics, resources, and Beacon-driven priorities, common themes emerged as they described their approaches to data governance and DSA development.

Conclusions: The 6 Beacon Communities confirmed that DSAs are necessary to satisfy legal and market-based concerns, and they identified several specific issues, many of which have been noted by others involved in network data sharing initiatives. More importantly, these communities identified several promising approaches to timely and effective DSA development, including: stakeholder engagement; identification and effective communication of value; adoption of a parsimonious approach; attention to market-based concerns; flexibility in adapting and expanding existing agreements and partnerships; and anticipation of required time and investment.

Introduction

Across the United States, unprecedented efforts are under way at the community, state, and national levels to electronically capture and exchange information to improve health care and population health, and reduce costs.[1] Health information technology (health IT) tools such as electronic health records (EHRs) capture clinical data that can be used at the point of care, shared among providers to facilitate care coordination, and aggregated and analyzed to support quality improvement (QI), population health management, and research. These electronic clinical data can drive improvements in health and health care by increasing the accuracy, accessibility, and utility of patient information.[2] With these tremendous benefits comes responsibility; the electronic collection and sharing of patient information raises the data governance issues of patient privacy, information security, organizational liability, and market competition among participating organizations.

Data governance broadly refers to policies and practices established to inform decisions about what data can be shared, with whom, under what conditions, and for what purposes.[3] Those engaged in data sharing affirm that data governance policies must be built upon trust and a shared vision among applicable stakeholders to overcome common barriers.[4] Historically, most barriers derive from interpretation and application of legal and statutory requirements,

[i]Greater Cincinnati HealthBridge, Inc. [ii]Southeastern Michigan Health Association [iii]HEALTHeLINK [iv]Louisiana Public Health Institute [v]Eastern Main Healthcare Systems [vi]AcademyHealth [vii]State University of New York [viii]Geisinger Health System

while some have been market based (e.g., reluctance of providers to share patient data with competitors).[5] Therefore, before data sharing between two or more parties can occur, those parties must reach a point of sufficient mutual trust to collaboratively establish governance policies and corresponding agreements. Such governance policies are typically codified in a variety of legal documents, collectively known as data sharing agreements (DSAs).[4]

The Office of the National Coordinator for Health IT (ONC) released a Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information in 2008,[6] and a Governance Framework for Trusted Electronic Health Information Exchange in early 2013.[7] However, these frameworks serve as guiding principles rather than rules by which entities involved in sharing health information must abide, and contain no specific guidelines for developing DSAs. Given this fact and the multiple reasons for developing DSAs, the types, components, and approaches to their development vary widely; similarly, given that these types of health information exchange efforts are a relatively recent development, published evidence on best practices or successful strategies for data governance are limited.

In 2010, the ONC funded 17 communities across the U.S. under the Beacon Community Cooperative Agreement Program, a three-year initiative to demonstrate the impact of leveraging health IT to achieve improvements in care and reduce costs. Most Beacon Community interventions required community-wide clinical information sharing to facilitate diverse activities, including care coordination, laboratory results delivery, quality reporting, quality improvement, and population health management. In doing so, the communities initiated information exchange with entities not previously considered "partners" in the delivery of care; these included providers (e.g., hospitals, primary or specialty care practices, long-term care facilities, hospice), laboratories, health plans, local and state health information exchanges (HIEs), research centers, health IT vendors and contractors (e.g., analytics or reporting services), quality improvement organizations (QIOs), public health agencies, and other government agencies (e.g., state Medicaid programs).

This put many Beacon Communities at the forefront of cultivating new relationships with diverse partners, and navigating data governance issues as part of this process—*before* the ONC Governance Framework guidance became available. In developing their DSAs, several Beacon Communities—including the six whose leaders co-authored this paper (Bangor [Maine], Greater Cincinnati [Ohio], Crescent City [Louisiana], Keystone [Pennsylvania], Southeast Michigan, and Western New York; see Table 1 for an overview of each community)—worked through complex legal and technical challenges; in so doing, they identified a number of promising practices that may be useful to others. By identifying these practices, this paper aims to add to the growing body of literature on best practices for data governance. We first provide an overview of data governance, DSAs, and legal requirements for the use and re-use of health data. We also highlight some common data governance challenges, and then share lessons learned and practical guidance based on the experiences of these six Beacon Communities.

Table 1. Overview of the Beacon Communities

Beacon Community	Location	Lead Grantee	Population Size (Approx.)	Urban/ Rural	Data Sharing Participants
Bangor	Bangor, Maine, and 43 surrounding cities and towns in eastern-central Maine	Eastern Maine Healthcare Systems	164,000	Largely rural	Health systems, hospitals, physician practices, FQHC, behavioral health providers, home health, long-term care facilities, HealthInfoNet (statewide HIE)
Crescent City	New Orleans, Louisiana, and 2 surrounding parishes (Jefferson and Orleans)	Louisiana Public Health Institute	800,000	Urban	Hospitals, FQHCs, health systems, medical centers, community organizations, hospital association, Louisiana Dept. of Health and Hospitals, health plan, Louisiana Healthcare Quality Forum (NGO, runs state HIE)
Greater Cincinnati	Cincinnati, Northern Kentucky, Western Indiana	HealthBridge	2.2 million	Urban/rural mix	Ohio Hospital Ass'n; 26 area hospitals; 40 practice groups; Cincinnati Health Council; Health Improvement Collaborative
Keystone	5 counties in Central Pennsylvania	Geisinger Health Systems	2.5 million	Largely rural	Hospitals, health systems, physician practices, community clinics, home health services, nursing homes, hospice
Southeast Michigan	Detroit, Michigan, and surrounding cities of Highland Park, Hamtramck, Dearborn, and Dearborn Heights in Wayne County	Southeast Michigan Health Association	1.8million (Wayne County)	Urban	Hospitals, health systems, FQHCs, physician organizations, physician practices, labs, payers, State of Michigan Medicaid, Medicare data through Michigan's QIO
Western New York	Buffalo, New York, and 8 surrounding counties	HEALTHeLINK	1.6 million	Mixed urban/rural	Health systems, hospitals, health plans, physician organizations, physician practices, laboratories, radiology providers, home care, long term care, FQHCs, pharmacy, Veterans Administration

FQHC = federally-qualified health center; HIE = health information exchange; NGO = non-governmental organization; QIO = quality improvement organization

Methods

All interested Beacon Communities were invited to participate in a collaborative effort on the topic of data governance. The result was this group of six communities listed above. Conference calls were held to identify key themes and develop an initial outline. The Beacon co-authors each contributed written content relevant to the themes in the outline based on their experiences participating in Beacon governing bodies and developing DSAs. AcademyHealth conducted a literature scan in PubMed and Google Scholar to identify manuscripts on health information exchange and governance, and drafted the introduction. The Beacons' submitted sections were collected and integrated into a single manuscript. The co-authors discussed the resulting draft during subsequent conference calls and conducted iterative rounds of review and revision to streamline the disparate examples, identify and highlight overarching themes, and edit for clarity, consistency, and flow. All authors reviewed and approved the final manuscript to ensure that it accurately reflected their experiences and lessons learned.

Background: Data Governance and DSAs

Rosenbaum defines data governance in relation to the closely related concept of data stewardship, which "denotes an approach to the management of data, particularly data, however gathered, that can identify individuals."[8] This approach may include methods for acquiring, storing, aggregating, and de-identifying data with a fiduciary responsibility for protecting the interests and rights of those who contributed the data. Data governance is thus defined as "the process by which stewardship responsibilities are conceptualized and carried out, that is, the policies and approaches that enable stewardship." In the context of electronic health information exchange, data governance aims to ensure compliance with legal requirements related to the protection, use, and disclosure of personally identifiable information, and to address issues of data over-protectiveness due to market-based competition.[3] Data governance encompasses designated roles and responsibilities of data stewards and stakeholders as well as policies, technical system requirements, and procedures that participating entities and those under their employ agree to follow when accessing and using data.[8]

Health care organizations participating in health information exchange initiatives develop and codify their data governance policies in a variety of legal documents, collectively known as data sharing agreements (DSAs).[4] Some common types of DSAs include Data Use Agreements (DUA), Business Associate Agreements (BAA), and Participation Agreements (PA).[4] See Table 2 for definitions and components of each type of agreement. These agreements typically authorize specific entities to access data; define the entities' roles and responsibilities; and specify which data can be shared, when, how, and under what circumstances. DSAs may also enumerate acceptable data uses and prohibitions; address issues of liability and patient consent; specify safeguards for data privacy and security; and establish policies for handling breach notification, grievances, and sensitive data.[3,4]

DSAs may be negotiated as multi-party agreements that facilitate data sharing among all signatories, or they may be contracted between each pair of entities that share data (e.g., a health information exchange organization and a hospital). For example, the Western New York Beacon Community participated in the multi-party Data Use and Reciprocal Support Agreement (DURSA) to allow data sharing via the Nationwide Health Information Network (NwHIN).[9] In contrast, the Bangor Beacon Community established separate agreements between each participating organization and HealthInfoNet, the statewide HIE. Entities may also need to execute multiple agreements to address specific aspects of the data, their sources, and/or their subsequent uses; this experience was common across several Beacon Communities.

DSAs are often written to satisfy or comply with the requirements of multiple entities (e.g., stakeholders, laws, statutes). For instance, in the Greater Cincinnati Beacon Community the legal team already had experience structuring agreements authorizing use of health data in compliance with the federal Health Information Portability and Accountability Act (HIPAA) Privacy Rule. However, given that the interventions proposed by the Cincinnati Beacon team involved movement and use of health data in novel ways, the legal team also recognized the potential need to adhere to additional state laws; consequently, they undertook an extensive review of legislative history and case precedents to identify additional regulations that may have applied. These considerations are discussed in greater depth in the following sections.

Legal Requirements Governing Data Sharing and Use

The most relevant federal laws that influence the sharing and use of health information are the HIPAA Privacy and Security Rules[10] and the Federal Policy for the Protection of Human Subjects (the "Common Rule").[11] HIPAA and related state laws establish requirements for safeguarding the privacy and security of protected health information (PHI); obtaining consent to share and use PHI for specific purposes; and developing protocols for preventing, reporting, and mitigating the effects of data breaches or unauthorized disclosures.[10] The Common Rule establishes requirements for federally-funded research with human subjects, including institutional review board (IRB) approval and informed consent;[11] these requirements are discussed in more detail below.

Under the HIPAA Privacy Rule, covered entities—which include most health care providers, health plans, and health clearinghouses—are permitted to use or disclose PHI without patient authorization for treatment, payment, or health care operations, among other purposes specified by the Rule.[12] Non-covered entities are required to comply with most provisions of HIPAA when they are engaged by a covered entity as a business associate to provide services or complete health care functions on its behalf, in which case a business associate agreement (BAA) is required.[13] BAAs ensure that business associates engaged by a covered entity comply with applicable HIPAA privacy and security standards and protocols. As of September 2013 under the HIPAA Omnibus

Table 2. Types, Definitions, and Components of Data Sharing Agreements

Type of Agreement	Definition	Components
Data Use Agreement (DUA)	Data Use Agreement (DUA): A covered entity may use or disclose a limited data set if that entity obtains a data use agreement from the potential recipient. This information can only be used for: Research, Public Health, or Health Care Operations. A limited data set is protected health information that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual.[12]	• Establishes what the data will be used for, as permitted above. The DUA must not violate this principle. • Establishes who is permitted to use or receive the limited data set. • Provides that the limited data set recipient will: – Not use the information in a matter inconsistent with the DUA or other laws. – Employ safeguards to ensure that this does not happen. – Report to the covered entity any use of the information that was not stipulated in the DUA. – Ensure that any other parties, including subcontractors, agree to the same conditions as the limited data set recipient in the DUA. – Not identify the information or contact the individuals themselves.
Business Associate Agreement (BAA)	A business associate is a person or entity that performs certain functions or activities involving the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e).[11]	• Describes the permitted and required uses of protected health information by the business associate. • Provides that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; • Requires the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
Data Use and Reciprocal Support Agreement (DURSA)	The DURSA is the legal, multi-party trust agreement that is entered into voluntarily by all entities, organizations and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services and policies developed in coordination with the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services.[27]	• Multi-party agreement that specifies: – Participants actively engaged in health information exchange – Privacy and security obligations – Requests for information based on a permitted purpose – Duty to respond – Future use of data received from another participant – Respective duties of submitting and receiving participants – Autonomy principle for access – Use of authorizations to support requests for data – Participant breach notification – Mandatory non-binding dispute resolution – Allocation of liability risk
Participation Agreement (PA)	Designed to ensure that participants comply with the data sharing policies and procedures, Participation Agreements spell out the terms of the relationship, including the roles, rights and responsibility of each party as they pertain to the initiative.[4]	May include or reference one or more of the above-named agreements.

Final Rule, the Privacy and Security rules are directly applicable to business associates of covered entities, meaning they are directly liable for noncompliance with the regulations.[14] However, this development occurred as the Beacon program was concluding, and thus did not apply to the Beacon Communities' DSA development efforts.

In addition, covered entities may disclose a limited data set (i.e., PHI from which certain specified direct identifiers have been removed) for use in research, public health, or health care operations if they sign a DUA with the data recipient.[14] The HIPAA Security Rule also sets national standards for administrative, technical, and physical safeguards to ensure that electronic PHI remains confidential and secure.[15]

Because HIPAA does not preclude states from enacting more stringent privacy and security laws,[16] many Beacon Communities enlisted legal support to determine whether their states had stricter standards for data sharing and consent than those outlined in the federal laws. For instance, state laws regarding informed consent for health information could be either opt-in (perceived as more stringent) or opt-out (perceived as less stringent). In the former, patients must provide explicit consent for providers to share their health information; in the latter, information is shared by default unless the patient specifically indicates a preference to not share.

Common Governance Challenges

The legal requirements outlined in HIPAA and the Common Rule vary significantly based on the answers to three important questions:

1. Who will be sharing or accessing the data (e.g., covered entity, business associate)?
2. What types of data will they share or access (e.g., de-identified, sensitive)?
3. Why are they sharing or accessing the data (i.e., for what purpose? e.g., research, QI, operations)?

As the Beacon Communities implemented a variety of novel health IT-enabled interventions in partnership with diverse stakeholders, many of the challenges that they faced in developing data governance policies and associated DSAs stemmed from ambiguity in answering these questions and interpreting the relevant legal requirements (see Table 3). Other barriers were related to fostering trust and buy-in to data sharing in competitive health care marketplaces.

Table 3. Data Governance Challenges for Health Information Exchange

Legal Challenges	Market-Based Challenges
• Navigating requirements for limited, de-identified, and sensitive data • Identifying activities as research, QI, or operations	• "Overprotectiveness" of data as intellectual property or a strategic asset • Handling concerns over "stealing" patients

Navigating Requirements for Limited, De-Identified, and Sensitive Data

As legal requirements and participants' comfort levels vary depending on whether the data being shared are individually identifiable, de-identified, or sensitive, these characteristics affect the policies contained in the resulting DSAs. As described above, PHI (ie, individually identifiable health information) is subject to more stringent privacy and security regulations regarding acceptable use and disclosures than de-identified and/or aggregated data. Likewise, limitations on the access and sharing of sensitive categories of patient information (e.g., behavioral health, genetic information, sexually transmitted infections) are expressed in both federal and state laws. For example, federal law requires individual patient authorization for covered entities to access or share psychotherapy notes[17] and alcohol and substance abuse treatment records,[18] and health plans are forbidden from disclosing genetic information for underwriting purposes.[19] State-specific laws also address these types of information as well as other sensitive information, such as behavioral health, HIV status, and sexually-transmitted infections.

Variation in sensitive data laws at the state level introduces additional challenges in the context of health information sharing in that governance, privacy, and security mechanisms developed in one state to address sensitive data laws are rarely scalable to other states. For instance, consent requirements and exchange protocols may differ for sensitive data between and even within states; an "opt-out" state may require patients to "opt-in" to sharing of sensitive data. This proves problematic when trying to exchange multiple types of information across state boundaries, and when adapting governance policies or information exchange protocols from another state. Because these laws are complex and vary widely, a full discussion of their implications is outside the scope of this paper. Worth noting, however, is that several Beacon Communities grappled with these issues and in some cases revised their data sharing plans to be less ambitious as a result.

Identifying Activities as Research, QI, or Operations

Entities must also abide by different requirements when using PHI for treatment, payment, and health care operations than for downstream uses ("re-use") of clinical data, such as for research. Accordingly, another primary consideration when developing DSAs is the purpose for which data is being shared, in particular, whether the data are to be used for research. Under the Common Rule, anyone conducting federally-funded research with human subjects must obtain institutional review board (IRB) approval or a waiver of exemption from the IRB if the research is subject to certain narrowly defined exceptions.[20] Researchers must also obtain informed consent from all participants, unless the IRB grants a waiver of patient authorization.[3] Both the Common Rule and HIPAA define "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge," [20,21] a rule of thumb that typically applies to researchers who plan to publish the results of their activities.

In the context of health information exchange, however, it is not always clear whether this definition (and thus, HIPAA and the Common Rule) applies; this is largely due to ambiguity regarding what health care activities constitute "research" as opposed to treatment, QI or operations. As we progress toward the vision of a learning health care system—one that continually captures clinical data for analysis and generates evidence to improve the safety and quality of care—this distinction between QI and research grows ever blurrier.[22,23] To mitigate this ambiguity, entities sharing data can define which of their activities are considered research and which are considered treatment or operations, and clarify this distinction in DSAs.

Market-Based Challenges

Another important role of DSAs is to pre-empt the market-based implications of sharing electronic clinical data. In addition to concerns over ethical and legal liability for misuse or mishandling of data being shared, health care organizations and providers are often hesitant to share data out concern for intellectual property, proprietary, or commercial interests.[8] For instance, a common concern is the fear (either real or perceived) that sharing patient data will allow competing providers to "steal patients" or lead to loss of control over the data.[3] In this light, data resources are considered strategic assets and, without a compelling case for sharing, organizations remain protective to ensure that data are

not used, repurposed, or disseminated in ways that put them at a disadvantage.[3] New care delivery and payment models emerging as part of ongoing care delivery reform efforts, such as Accountable Care Organizations (ACOs), may alter the markets in which these health care entities operate, with clear implications for data sharing and governance.

Lessons Learned and Approaches to Developing DSAs

In working through these data governance challenges, the Beacon Communities learned a number of important lessons and identified successful strategies for developing DSAs. These approaches and lessons learned are listed in Table 4 and described in detail in the sections that follow.

Table 4. Beacon Community Approaches to Developing DSAs

- ✓ Engage Stakeholders
- ✓ Identify and Communicate the Value Proposition
- ✓ Start Small, Then Expand: Adopt a Parsimonious Approach
- ✓ Address Market-based Concerns
- ✓ Adapt and Expand Existing Agreements and Partnerships
- ✓ Anticipate the Time and Investment Needed

Engage Stakeholders

When initiating data sharing relationships, all Beacons emphasized the importance of identifying and engaging a core set of relevant stakeholders to build a foundation of trust. These stakeholders participated in governance discussions and DSA development through participation in advisory committees as well as less formal mechanisms. Their experiences suggest that data exchange should not be driven by a single stakeholder entity or type, but rather should be informed from the outset by the expectations and needs of participating members, and periodically re-evaluated as partners and priorities change.[3] The Beacon Communities found that it was important for the governance of data sharing to be viewed as neutral and balanced in its representation of all stakeholder interests, with multi-stakeholder involvement to avoid issues of trust related to misuse of data.[3] The Beacon Communities also sought multiple types and levels of leadership to be represented from within each participating organization.[4] In addition to board and operational executives, the Beacon Communities often included clinical, IT, legal, QI, and privacy and security leadership as well as consumer representation in their governance discussions and the DSA development process.

In the Crescent City Beacon Community, DSA development for the Greater New Orleans Health Information Exchange (GNOHIE) involved a lengthy period of discussion that included clinical and health IT leadership from participating clinics and hospitals. The GNOHIE Administrative Committee served as the governance body for the GNOHIE and involved leaders from each GNOHIE member organization.

Similarly, in Western New York, the participation agreement for HEALTHeLINK, the regional HIE, was developed with guidance and supervision at various levels of HIE governance, and included a range of stakeholder perspectives at the executive board and operating committee levels. All services provided by the HIE were approved by this multi-stakeholder governance structure.

In Southeast Michigan, the Beacon Privacy and Security Committee reported to the Beacon Executive Board, which was the Beacon Community's primary governing body. The Committee had both legal and non-legal health system, hospital, and physician representation as well as representation from local universities and other community stakeholders. The Committee produced draft agreements, policies and procedures for Executive Board review, and monitored adherence to agreements, policies, and procedures to provide needed enhancements.

Identify and Communicate the Value Proposition

When engaging stakeholders in early discussions around data sharing and accompanying agreements, the Beacon Communities found that a certain amount of education was often necessary to communicate the critical value of data sharing to the broader health care and patient communities as well as directly to each level of leadership in prospective partner organizations. Given the multiple and competing demands faced by health care stakeholders (e.g., public and private care delivery and payment reform initiatives, and health IT incentive programs), many Beacon Communities needed to emphasize ways that Beacon efforts aligned with these ongoing activities in their respective health care marketplaces. In doing so, the Beacon teams had to identify how to communicate that working with them could help these stakeholders further their other objectives, such as demonstrating Meaningful Use of EHRs, meeting accountable care organization or patient-centered medical home requirements, and reducing avoidable hospital readmissions, among other incentive programs and opportunities.

In some communities, large integrated delivery systems that had implemented or planned to implement their own internal HIEs seemed less willing to join the community-wide HIE since many of their resources already were tied up in implementation or planning. The Beacon Communities found it especially critical to articulate a clear value proposition to convince these organizations of the benefits of connecting to entities outside of their health system. In several communities, only after Beacon leaders presented utilization data demonstrating that patients were seeking care outside their primary health system approximately 30 percent of the time did these organizations decide to participate in community-wide data sharing.

Often, the entity initiating the data sharing relationship needed to communicate several key points; several Beacons noted that the onus was on them to demonstrate the legality of the proposed activities, the lack of or minimal risk of participation, and a compelling business case for each partner to participate.[3] This involved working to identify the underlying values of each organi-

zation, how data sharing aligned with and supported those values, and the common health improvement objectives shared across the community as a whole. This was easier said than done, and Beacons faced several challenges in identifying optimal methods for communicating these points to the relevant audiences at each organization.

For instance, as HealthBridge (the regional HIE and lead grantee in the Greater Cincinnati Beacon Community) already had been facilitating data sharing for several years in the Greater Cincinnati area, the HealthBridge leadership team assumed they would only have to demonstrate the legality and lack of new security risks in the additional data uses proposed under the Beacon program (e.g., automatic transmission of alerts to primary care providers when their patients are admitted to the hospital) to the IT, privacy and security officers of the organizations providing the data in order for them to sign the agreements. However, instead of immediately proceeding, hospital representatives expressed concern, questioning the value their employers would receive by contributing their data. This was especially important since the Beacon projects would be adding work at a time when the hospitals were already burdened with a significant EHR implementation initiative. Well into the process, the HealthBridge team realized that, had they first developed a strategy for garnering support from hospital leadership by focusing on the potential benefits to providers, and allowed the executives to communicate the value proposition to their employees, providers might have seen the Beacon work as a logical next step that would build on their EHR infrastructure work, as opposed to a distraction from other competing priorities.

Start Small, Then Expand: Adopt a Parsimonious Approach

All six Beacon Communities (and other networked collaborations) have suggested that starting small helps build trust among participating entities and facilitates future expansion of data sharing initiatives to include additional participants, data streams, and/or data uses.[3] As Beacon stakeholders faced competing priorities (e.g. limited resources, multiple ongoing IT and QI initiatives), adopting a parsimonious approach that minimized required work, simplified the DSA development process, and expedited the initiation of data sharing.

For example, before the Beacon program, providers in the Keystone Beacon Community received analytics specific only to their organization and containing the minimum necessary data for analytics and care management operations. When they initiated the Keystone Beacon Community, they asked for only the top seven diagnoses from inpatient admissions, but over time they collected additional data to conduct their analyses, expanding the request to include all diagnoses.

In Cincinnati, this lesson was learned when the HealthBridge team attempted to explain the entirety of the proposed Beacon Community initiative to area hospitals, thinking it would make sense to show the value of all aspects of the work. Prior to the Beacon Program, HealthBridge, as the Cincinnati regional HIE, already was facilitating the flow of electronic health data from participating hospitals in the Ohio-Indiana-Kentucky tri-state area as part of its everyday operations. However, since HealthBridge's existing agreements with the hospitals only allowed transmission of data to designated ultimate users (i.e., clinicians) for treatment purposes, HealthBridge needed to develop additional DSAs with the participating hospitals to authorize use of data flowing through the HIE to implement additional Beacon initiatives (e.g., evaluation, automatic data transmission to primary care practices). Likewise, new agreements were necessary to enable HealthBridge to use the existing data banks of the Ohio Hospital Association to establish a baseline for pre/post analysis of the Cincinnati Beacon projects.

Instead of making a compelling case for action, the Cincinnati team found that introducing the full scope of these proposed data sharing activities raised more concerns than could be managed at the outset of a new initiative. In hindsight, the team suspects that a small initial request, followed by others after gaining some traction on the first, might have yielded more rapid buy-in. When they started asking for small "bites of the apple," drafting very short and narrowly written DSAs requesting specific types and proposed uses of data, comfort levels rose and the process began to move along more swiftly.

In the case of Southeast Michigan, some Beacon Communities also adopted flexible agreements that allowed organizations to participate to the extent they were able and felt comfortable. They developed different DSAs for different purposes and levels of participation in data sharing activities. One abbreviated DSA was developed to enable sharing of aggregated, de-identified data among private payers, health systems, hospitals, a QIO, Medicaid, a local uninsured initiative, and lab vendors to enable evaluation of QI interventions. Another DSA allowed participating health systems, hospitals, federally qualified health centers (FQHCs), and ambulatory clinics to share individually identifiable patient data through the HIE for treatment purposes, including care management and coordination. An additional DSA allowed for data sharing across regional HIEs, and yet another facilitated data sharing between the community-based and the statewide HIE. This tailored approach of taking on one use case at a time resulted in multiple agreements, but helped to enable the data to flow to support their initiatives.

Address Market-Based Concerns

By engaging participants and stakeholders in discussions around data governance, the Beacon Communities gained valuable insights into the primary market-based concerns of various entities, and worked to develop a fabric of trust supported by governance policies and DSAs that mitigated those concerns to the extent possible. In the Beacon experience, these market based concerns were generally addressed in one of three ways: 1) a neutral entity was identified as the independent custodian of shared data; 2) the types and/or characteristics of data shared were limited to certain purposes; and 3) additional safeguards were applied to protect the data and/or the organization.

In the Greater Cincinnati Beacon Community, the HIE HealthBridge found that adopting the role of an independent data aggregator assuaged some fears of competing health systems about misuse of data. They also found that, since their proposed data uses were focused on quality indicators and not on "research" per se, there was more willingness to proceed. Furthermore, to reduce the likelihood of data putting any practice at a competitive disadvantage, the Cincinnati DSAs specified that the data gathered from tracking Beacon interventions would be reported back to the originating practice and the hospital that owned it to be acted upon; the data would then be aggregated and de-identified to prevent attribution to any particular practice, hospital, or provider. With these provisos, HealthBridge was able to enlist practices to participate.

Similarly, the Keystone Beacon Community opted to exclude comparative data across facilities or physician practices from the Keystone Beacon analytics package, which helped to mitigate concerns about competition. They achieved greater buy-in to share data among Keystone Beacon participants by not asking for business data considered to be market-sensitive (e.g., total charges or visit net revenue).To provide additional privacy assurances, the Beacon project director served as the data custodian to authorize individual user access to the community data warehouse and ensure appropriate data use. Each KeyHIE user was required to obtain a unique identifier to use when logging into the system, which allowed tracking of individuals' access and use within each participating organization. Written explanations of the business need to access the data and its intended use were submitted to the project director for review.

The Southeast Michigan Beacon took a similar approach in excluding provider-specific comparative data from the aggregated data collected quarterly for evaluation purposes. Providers engaged in clinical transformation and EHR system optimization efforts received analytics specific to their organization only, along with community-wide averages and in some cases national benchmarks for informational purposes, but did not receive practice-specific comparative data.

At the start of the program, providers in the Bangor Beacon Community addressed market concerns by signing a non-compete agreement that assured partners they would not use performance improvement data to harm other providers. They also de-identified and aggregated their data, and executed agreements with a third-party reporting vendor to ensure that details of data would not be released. To encourage providers to use their data to drive practice-level discussions and improvement activities, provider-level performance data were shared within practices and at monthly multi-organizational performance improvement meetings. Initially these data were de-identified, but soon became fully-identified once the participating providers developed sufficient trust.

The Bangor Beacon Community has transitioned to an ACO model, which creates a shared savings/shared risk arrangement focused on improving population health rather than generating revenue from medical services. This focus emphasizes the cooperative relationship among provider partners and thus reduces the incentive to market to, or compete for, patients. In light of this transformation, ACO participants continue to share aggregated, de-identified patient data to support community-wide QI, and drew up BAAs with non-provider entities having access to patient information to ensure that it would not be used for marketing purposes or shared in any way that would benefit one partner over another.

Adapt and Expand Existing Agreements and Partnerships

Communities where hospitals, payers, and other health care organizations had a history of collaboration and sharing of administrative or clinical data were often able to build upon these existing trust relationships—and in some cases, existing agreements—when developing governance policies and DSAs for Beacon Community initiatives.[3] The Beacon Communities adapted existing agreements in various ways, such as adding simple addenda to address additional data streams or uses, or drafting new agreements (e.g. BAA or Statement of Work) that referenced definitions, policies, and procedures outlined in existing agreements.

For instance, although DSAs existed from earlier collaborative data-sharing projects in Western New York, enhancements were required for HIE use for Beacon interventions. With specific data uses for certain Beacon initiatives, Statements of Work were necessary and were developed with support of internal legal staff using other agreements as a precedent.

Within the Crescent City Beacon Community, the local safety net hospital had a long history of working closely and sharing data with the community health centers in the Greater New Orleans area. Since 2005, community health centers have had access to their patients' hospital records through the hospital's EHR, and have engaged in clinical QI and care coordination efforts that continued throughout the Beacon Program. Thus, when presented with the concept of data sharing through a new regional HIE, the community clinics and hospitals built on their strong foundation of trust and familiarity to facilitate the rapid development and execution of the GNOHIE DSAs. This trust foundation served as an example of successful data sharing when approaching potential new members to participate the GNOHIE, which helped allay concerns and increase participation.

Anticipate the Time and Investment Needed

The time and effort required to work through data governance issues and develop DSAs for community data sharing initiatives cannot be underestimated. Typically, the more complicated the agreement and organizations, the more time was required prior to execution of the agreement. Even organizations that were enthusiastic about sharing data encountered internal bureaucracy. The Beacon Communities spent several months—and some even up to a year— negotiating and executing DSAs.

Notwithstanding the history of data sharing in the Crescent City Beacon Community and the existing trust relationships among participants, the DSA for the GNOHIE went through nearly a year of review by potential participants before it was finalized. Similarly, the Keystone Beacon Community took approximately nine months to draft the Beacon PA, including input from a Management Oversight Team, participating providers, and legal review; it required hundreds of hours invested by all parties. The sheer volume of agreements can also create logistical issues and bottlenecks; the Cincinnati Beacon Community alone executed more than 200 DSAs in the span of approximately ten months.

Besides the investments in technical infrastructure required to enable data sharing, the costs of developing DSAs are also substantial, factoring in the time spent engaging advisory committees and legal counsel. One Beacon Community estimated spending more than $32,000 developing the primary DSA alone (based on a template from another community, not from scratch). This estimate does not include time or money spent negotiating with potential participants, or on participants' final legal review and signature.

Conclusion

Unlike many aspects of health IT, in which diverse stakeholders are striving for increased development and adoption of common standards (e.g., data elements, vocabulary, transport protocols, patient identifiers, etc.), DSAs and governance policies are customized at virtually every level, and depend on many factors. Because of the number and variety of potential partners involved in community-based QI initiatives, and the variability across applicable state laws, this is particularly true at the community level. However, certain generalizations can be drawn from the diverse experiences of the Beacon Communities and applied to the efforts of others. Notable are the importance of trust, multi-stakeholder input, a clear value proposition, and shared QI objectives.

Policymakers can support these efforts by providing additional guidance for data governance through policies, programs and, in some cases, regulations. Some of this work is underway; in addition to the ONC's Governance Framework, the ONC (along with the National eHealth Collaborative) launched the National HIE Governance Forum, which convenes key stakeholders to identify solutions to common data governance challenges at the community, state, and national levels. Additionally, through the Exemplar Health Information Exchange Governance Entities Cooperative Agreement Program, the ONC is supporting two grantees—DirectTrust and the New York eHealth Collaborative—to develop health information exchange policies, interoperability standards, and business practices.[23]

As electronic sharing of health information grows more widespread and sophisticated, these guiding principles will be increasingly important in helping participating entities establish the necessary trust for successful data governance, and execute DSAs accordingly. Communities engaged in data sharing efforts should continue to learn from and document their experiences so that others might benefit; they can facilitate this by contributing sample agreements and other useful work products or resources to publicly-available repositories, such as the Research Toolkit developed under the Clinical and Translational Science Award (CTSA) by the Practice-Based Research Network and HMO Research Network,[25] and the Electronic Data Methods (EDM) Forum Governance Toolkit.[26] These and similar repositories may be used to surface best practices and evolve principles that can ease the way for others driving toward health care improvement.

References

1. Adler-Milstein J, Bates DW, Jha AK. Operational health information exchanges show substantial growth, but long-term funding remains a concern. Health Aff 2013;32(8):1486-92.
2. Furukawa MF, Patel V, Charles D, Swain M, Mostashari F. Hospital Electronic Health Information Exchange Grew Substantially In 2008–12. Health Affairs 2013; 32(8):1346-54.
3. McGraw D, Leiter AB. Pathways to Success for Multi-Site Clinical Data Research. eGEMs (Generating Evidence & Methods to improve patient outcomes). 2013;1(1): Article 13.
4. Middleton B, Fleming M, Wiegand T, Merritt D, Bakalar R, Georgiou A, Marchibroda J, Whitlinger D, Davidson G, Schlaifer D. Best Practices for Community Health Information Exchange. Center for Community Health Leadership. 2013.
5. Williams C, Mostashari F, Mertz K, Hogin E, Atwal P. From the Office of the National Coordinator: The strategy for advancing the exchange of health information. Health Aff 2012;31(3):527-536.
6. Office of the National Coordinator for Health Information Technology. Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. U.S. Department of Health and Human Services. 2008.
7. Office of the National Coordinator for Health Information Technology. Governance Framework for Trusted Electronic Health Information Exchange. U.S. Department of Health and Human Services. 2013.
8. Rosenbaum S. Data governance and stewardship: designing data stewardship entities and advancing data access. *Health Serv Res*. 2010; 45 (5p2): 1442-55.
9. Dixon BE, Zafar A, Overhage JM. A framework for evaluating the costs, effort, and value of nationwide health information exchange. J Am Med Inform Assoc 2010 May-Jun; 17(3): 295–301.
10. The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, August 21, 1996)
11. Protection of Human Subjects. 45 CFR Part 46.
12. Security and Privacy. 45 CFR § 160.103; 45 CFR §§ 164.502, 164.504(e).
13. Standards for Privacy of Individually Identifiable Health Information. 45 CFR § 164.514(e).
14. Security and Privacy. 45 CFR § 160.102; 45 CFR § 164.302.
15. Security Standards for the Protection of Electronic Protected Health Information. 45 CFR Part 160 and 45 CFR Part 164, Subparts A and C.

16. General Administrative Requirements. 45 CFR § 160.203
17. Standards for Privacy of Individually Identifiable Health Information. 45 CFR § 164.508.
18. Confidentiality of Alcohol and Drug Abuse Patient Records. 42 CFR Part 2.
19. Standards for Privacy of Individually Identifiable Health Information. 45 CFR § 164.502.
20. Protection of Human Subjects. 45 CFR §§ 46.102, 46.103.
21. Standards for Privacy of Individually Identifiable Health Information. 45 CFR § 164.501.
22. IOM (Institute of Medicine). Best Care at Lower Cost: The Path to Continuously Learning Health Care in America. National Academies Press. 2012.
23. Hripcsak G, Bloomrosen M, Flately Brennan P, Chute C, Cimino J, Detmer D, Edmunds M, Embi P, Goldstein M, Hammond W, Others. Health data use, stewardship, and governance: Ongoing gaps and challenges: A report from AMIA's 2012 Health Policy Meeting. *J Am Med Inform Assoc. 2013 Oct 29*.
24. Healthit.gov. Health Information Exchange Governance. [Online] Available from: http://www.healthit.gov/policy-researchers-implementers/health-information-exchange-governance [Accessed 24 Sep 2013].
25. Research Toolkit. 2013. [online] Available at: http://researchtoolkit.org/ [Accessed 8 Apr 2014].
26. EDM Forum. 2013. Governance Toolkit. [online] Available at: http://repository.academyhealth.org/govtoolkit/ [Accessed: 6 Dec 2013].
27. eHealth Exchange. Restatement I of the Data Use and Reciprocal Support Agreement (DURSA). Healtheway. 2011. Available from: http://healthewayinc.org/images/Content/Documents/Application-Package/2011.03.05-restatement-i-of-the-dursa-final.pdf [Accessed 24 Sep 2013].