

### 3. Forming Partnerships

#### Data Governance and Data Sharing Agreements *Supplemental Reading*

The following information is summarized from and based on "Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities".<sup>1</sup> The article provides guidance based on the experiences of six federally funded communities that made their way through the data governance issues and creation of data sharing agreements necessary for creating a health information exchange in their communities.

The increase in initiatives focused on community health information exchange highlights the importance and complexity of data governance in such exchanges. The term data governance in such cases encompasses how decisions are made about who shares data with whom, under what rules and for what purposes. Governance structures and policies can be codified in various ways: through project charters, memorandums of understanding, and contracts. With data sharing, they will almost certainly be codified in data sharing agreements (DSAs) that may take the form of Data Use Agreements (DUA), Business Associate Agreements (BAA), or Participation Agreements (PA).

These agreements typically authorize specific entities to access data, define the entities' roles and responsibilities, and specify what, when, how, and under what circumstances data can be shared. 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.

The most relevant federal law regarding the sharing and use of health information is the HIPAA Privacy and Security Rules. However, state laws also establish requirements for privacy protections, allowable uses for governmental agencies, consent requirements, and many other provisions.

The following table, taken almost verbatim from the above-referenced article, describes three types of data sharing agreements from the perspective of HIPAA. Although your agency may or may not be a covered entity under HIPAA regulations, your clinical partners will almost certainly have the status of covered entity. Check with your attorneys to determine your agency's status if you are unsure.

---

<sup>1</sup> Allen, Claudia; Des Jardins, Terrisca R.; Heider, Arvela; Lyman, Kristin A.; McWilliams, Lee; Rein, Alison L.; Schachter, Abigail A.; Singh, Ranjit; Sorondo, Barbara; Topper, Joan; and Turske, Scott A. (2014) "Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities," eGEMs (Generating Evidence & Methods to improve patient outcomes): Vol. 2: Iss. 1, Article 5. Available at: <http://repository.academyhealth.org/egems/vol2/iss1/5>

### 3. Forming Partnerships

#### Data Governance and Data Sharing Agreements Supplemental Reading

Type of Agreement	Definition	Components
Data Use Agreement (DUA)	<p>A covered entity may use or disclose a limited data set (health information from which certain direct personal identifiers have been removed) if that entity obtains a data use agreement from the potential recipient.</p> <p>This information can only be used for: Research, Public Health, or Health Care Operations. A limited data set is protected health information under HIPAA.</p>	<ul style="list-style-type: none"> <li>• Establishes what the data will be used for.</li> <li>• Establishes who is permitted to use or receive the limited data set.</li> <li>• Provides that the limited data set recipient will:               <ul style="list-style-type: none"> <li>○ Not use the information in a manner inconsistent with the DUA or other laws.</li> <li>○ Employ safeguards to ensure that this does not happen.</li> <li>○ Report to the covered entity any use of the information that was not stipulated in the DUA.</li> <li>○ Ensure that any other parties, including subcontractors, agree to the same conditions as the limited data set recipient in the DUA.</li> <li>○ Not identify the information or contact the individuals themselves</li> </ul> </li> </ul>
Business Associate Agreement (BAA)	<p>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 165.504(e).</p>	<ul style="list-style-type: none"> <li>• Describes the permitted and required uses of protected health information by the business associate.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Participation Agreement (PA)	<p>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.</p>	<p>May include or reference one or more of the above-named agreements.</p>

### 3. Forming Partnerships

#### Data Governance and Data Sharing Agreements *Supplemental Reading*

##### Common governance challenges

Any community collaborative that involves sharing data will almost certainly have to address a range of governance issues, including coming to agreement on whether it is for surveillance or research (see *Distinguishing Surveillance from Research* under *Supplemental Reading in Clarifying Legal and Policy Issues*) and navigating the requirements for using identified, de-identified or sensitive data.

You may also have to manage market-based challenges among your health care partners, including their protecting and withholding data because they view it as intellectual property or a strategic asset or concerns over another entity taking their patients.

Although the lessons learned from the study cited in the article appear simple, in practical application, they are likely to be substantially challenging and time-consuming. The lessons learned include:

- 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

As page nine of the cited article notes, “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 quality improvement 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 [surveillance and] QI objectives.”