Getting the Right Information to the Right Health Care Providers at the Right Time

A Road Map for States to Improve Health Information Flow Between Providers
Acknowledgements

Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers ("road map")—written by Kate Johnson, Chelsea Kelleher, Lauren Block and Frederick Isasi—is the result of the National Governors Association Center for Best Practices (NGA Center) Health Division's ongoing work on data and analytics. The NGA Center would like to thank the many state officials and national experts who lent their guidance and insights in the development of the road map. The NGA Center would also like to acknowledge the Office of the National Coordinator for Health Information Technology (ONC) for its generous support in the development of the road map through Cooperative Agreement No. 90AX0003/01. The contents of the road map are solely the responsibility of the authors and do not necessarily represent the official views of ONC.


About the National Governors Association

The National Governors Association (NGA) is the nation’s oldest organization serving the needs of governors and their staff. The NGA Office of Government Affairs serves as the collective voice of the nation’s governors in Washington, D.C., while the NGA Center for Best Practices (NGA Center)—a separate 501(c)(3) organization—functions as a combination think tank and consultancy to help states advance policy objectives by implementing evidence-based best practices. The Health Division—which produced this publication—is located within the NGA Center.

Legal Disclaimer: The analysis provided in this road map is for informational purposes only and is not intended to be legal advice. You should contact your attorney to obtain advice with respect to any particular issue or question described herein.
### Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACO</td>
<td>Accountable Care Organization</td>
</tr>
<tr>
<td>ADT</td>
<td>Admission, Discharge and Transfer</td>
</tr>
<tr>
<td>CCD</td>
<td>Continuity of Care Document</td>
</tr>
<tr>
<td>CCO</td>
<td>Coordinated Care Organization</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CHIP</td>
<td>Children’s Health Insurance Program</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare &amp; Medicaid Services</td>
</tr>
<tr>
<td>DHIN</td>
<td>Delaware Health Information Network</td>
</tr>
<tr>
<td>DS4P</td>
<td>Data Segmentation for Privacy</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>FFS</td>
<td>Fee-for-Service</td>
</tr>
<tr>
<td>HIO</td>
<td>Health Information Organization</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH Act</td>
<td>Health Information Technology for Economic and Clinical Health Act</td>
</tr>
<tr>
<td>HITOC</td>
<td>Health Information Technology Oversight Council</td>
</tr>
<tr>
<td>ICD-10</td>
<td>International Classification of Diseases, Tenth Revision</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KHIN</td>
<td>Kansas Health Information Network</td>
</tr>
<tr>
<td>MCO</td>
<td>Managed Care Organization</td>
</tr>
<tr>
<td>NCQA</td>
<td>National Committee for Quality Assurance</td>
</tr>
<tr>
<td>NGA</td>
<td>National Governors Association</td>
</tr>
<tr>
<td>NGA Center</td>
<td>National Governors Association Center for Best Practices</td>
</tr>
<tr>
<td>NPRM</td>
<td>Notice of Proposed Rule Making</td>
</tr>
<tr>
<td>OHA</td>
<td>Oregon Health Authority</td>
</tr>
<tr>
<td>ONC</td>
<td>Office of the National Coordinator for Health Information Technology</td>
</tr>
<tr>
<td>PA 129</td>
<td>Public Act 129</td>
</tr>
<tr>
<td>Part 2</td>
<td>42 Code of Federal Regulations Part 2</td>
</tr>
<tr>
<td>PCPCH</td>
<td>Patient-Centered Primary Care Home</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>Road map: Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers</td>
<td></td>
</tr>
<tr>
<td>VBP</td>
<td>Value-Based Purchasing</td>
</tr>
<tr>
<td>VITL</td>
<td>Vermont Information Technology Leaders</td>
</tr>
</tbody>
</table>
The Problem
Due to a variety of legal and market-based barriers, exchange of clinical health information between providers either does not occur or occurs in a manner that does not allow for meaningful use of data to support optimal patient care.

The Road Map
The road map was developed to help states evaluate and implement changes to achieve better health, better care and lower costs by increasing the flow of clinical health care information between health care providers while protecting patient privacy as a step toward nationwide interoperability.

Steps States Can Take to Increase Information Flow Between Health Care Providers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assemble Core Team</td>
</tr>
<tr>
<td>2</td>
<td>Conduct Legal and Market Analyses</td>
</tr>
<tr>
<td>3</td>
<td>Determine Primary Barriers</td>
</tr>
<tr>
<td>4</td>
<td>Select Strategies</td>
</tr>
<tr>
<td>5</td>
<td>Implement and Evaluate</td>
</tr>
</tbody>
</table>

State Strategies to Address Legal and Market Barriers and Increase Information Flow Between Health Care Providers

**State Strategies to Address Legal Barriers**

- **Fully Align State Privacy Laws With HIPAA**
  Pass a law that supersedes all more restrictive state privacy laws to allow providers and hospitals to exchange information in accordance with HIPAA.

- **Partially Align State Privacy Laws With HIPAA**
  Amend select statutes to allow certain types of information, such as information exchanged electronically, to be exchanged in accordance with HIPAA.

- **Create Standardized Consent Forms**
  Create a standardized consent form that provides a “one stop” approach to gaining patient permission for sharing information.

- **State Guidance and Education**
  Issue guidance and provide education to providers about how to comply with state and federal law, including clarifying legal intent and addressing common misconceptions.

**State Strategies to Address Market Barriers**

- **Create Meaningful Economic Interests That Encourage Exchange of Health Information**
  Create or adjust payments to incentivize exchange of health information or penalize lack of exchange.

- **Use Legislative, Regulatory and Contracting Authority to Bolster Exchange of Information**
  Pass laws or issue regulations that expressly prohibit information blocking or require information exchange.

- **Set the Vision and Hold People Accountable**
  Set statewide vision for interoperable exchange of health information and use bully pulpit to elevate best practices and place pressure on those lagging behind.

- **Serve as Convener**
  Bring key stakeholders to the table to work together toward interoperable exchange of health information.

In the Appendices: Understanding How Providers Exchange Health Information - Background on the Legal Landscape Pertaining To Exchange of Health Information - Background on the Market Landscape Pertaining To Exchange of Health Information - Evaluation of State Strategies
Introduction
Introduction

The road map was developed to help governors, their senior health policy officials, state lawmakers, state health information technology (IT) officials and state legislative counsel to evaluate and implement changes to achieve better health, better care and lower costs, by increasing the flow of clinical health care information between health care providers while protecting patient privacy, as a step toward nationwide interoperability. The path to interoperability is not linear; every state is starting from a different statutory, market and infrastructure standpoint and will have different goals to achieve and obstacles to overcome. As a result, each state can adapt the steps in the road map to meet its individual needs.

What to Expect

The road map is organized into four sections. It includes:

- Background information outlining the current state of clinical health information sharing between providers in the United States;
- Steps state policymakers can take to evaluate their state’s current environment and make changes to increase the interoperable flow of data between health care providers, including assembling a core team, conducting landscape analyses, identifying barriers within the state, selecting strategies to overcome challenges and implementing and evaluating strategies;
- Examples of states that have implemented strategies to overcome barriers to clinical information flow between providers; and
- Supplemental information about how clinical information is exchanged between health care providers today and the challenges and opportunities states face in seeking to enhance interoperable exchange of information between health care providers.
Ultimately, nationwide interoperability will allow providers inside and outside of health care to share information critical to health and social welfare, including clinical, claims and social services data at the individual level as well as for overall population health and research. The road map, however, is not a comprehensive guide for every aspect of statewide or nationwide interoperability; rather, it is intended to highlight the policies and processes states can consider to increase the flow of clinical information between providers as one component of interoperability.

How the Road Map Was Developed
The NGA Center interviewed more than 90 state officials, health information organizations (HIOs), health care providers, health systems, health IT vendors, researchers and other national experts to inform development of the road map. In addition, the NGA Center conducted an experts roundtable that brought together more than 30 experts from across the country to discuss strategies available to states to move the needle on health care provider information sharing. The road map reflects the insights and experience of the many experts consulted during its development.
Background
Background

The United States has experienced significant advancements in medical diagnostics and treatments for complex health problems in recent years, but significant gaps remain in electronic information sharing between individual health care providers to inform such care.²

A patient’s protected health information (PHI) may exist in any number of formats and across a variety of care settings.³ Facilitating exchange of clinical health information is critical to ensuring that providers have the best information possible when making decisions about patient care, minimizing repetition and errors, ensuring high-quality transitions of care and lowering costs.⁴ The confluence of increasing pressure to achieve better health care outcomes at lower costs and robust technological advances in health IT should support increased information flow between providers, but significant barriers remain to widespread and meaningful provider adoption. After carefully analyzing and addressing patient privacy concerns, these barriers must be addressed to achieve interoperability.

Factors that Limit Exchange of Clinical Information Between Health Care Providers

Exchange of clinical health information either does not occur or occurs in a manner that does not allow for meaningful use of data to support optimal patient care.
Federal and State Legal Framework for Sharing Health Information

The federal Health Insurance Portability and Accountability Act (HIPAA) is the law that sets the floor for national privacy standards for the use and disclosure of personally identifiable health information, also referred to as “protected health information.” The law includes broad provisions that allow for exchange of information between entities pertaining to treatment, payment and health care operations without patient consent. Federal laws and regulations governing exchange of information related to substance abuse treatment are more stringent than the requirements under HIPAA. Federal regulation regarding confidentiality of alcohol and drug abuse patient records—42 CFR Part 2 (“Part 2”)—requires strict protections for sharing individually identifiable substance abuse treatment information. Part 2 restrictions limit providers’ ability to easily access and review complete patient information or improve care coordination for patients unless they have sophisticated technological capabilities.

Moreover, many states have privacy laws pertaining to health information that are more protective than HIPAA, restricting disclosure of specific categories of information deemed to be sensitive, such as mental health and communicable disease information, without explicit consent from the patient. Further, hospital systems and provider groups are responsible for setting their own privacy policies, which vary and in some cases are more restrictive than federal or state laws based on narrow legal interpretation. Hospital systems and provider groups may apply a more restrictive interpretation of the law to avoid legal risks associated with improperly sharing patient information. The variable nature of hospital and other provider policies creates a further layer of complexity on top of federal and state laws and can be an additional barrier to sharing patient information.
Influence of Market Incentives on Exchange of Health Information

The primary mode of payment for health care in the United States is the fee-for-service (FFS) model, which many experts argue incentivizes providers to focus on increasing the volume of services they provide over quality and efficiency of care. In recent years, both the federal government and states have taken steps to move away from FFS toward paying providers for health outcomes through value-based purchasing (VBP) initiatives. The shift to VBP, where payment to providers depends on the value of care they deliver, should incentivize providers to adopt more coordinated, team-based approaches to care that necessitate information sharing, in order to improve outcomes while lowering costs; despite some advances, however, the FFS model remains the dominant mode of payment.

Under the FFS model, many experts posit that providers almost always lack strong financial incentives to share information to achieve efficiencies, such as reducing the number of unnecessary services and better coordinating care. For example, health care providers may have concerns that sharing their patients’ health information could facilitate competitors “stealing” patient volumes, which could affect profitability. Other health care entities view their patients’ health information as proprietary and have business interests in commodifying its use. Similarly, there are challenges related to IT vendors’ willingness to share data because of its value for market leverage as companies enter new business areas.

In addition to provider payments for care delivery, other funding and incentive mechanisms can significantly influence the market landscape for exchange of health information. In recent years, there has been significant federal investment to encourage the adoption and use of health IT to promote clinical information sharing. In 2009, the federal government passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act. The HITECH Act provided incentives and penalties for certain providers to adopt and meaningfully use electronic health records (EHRs) as well as significant funding to states and territories to enable exchange of health information. Although the law provided important incentives to certain providers, it excluded many other providers from eligibility to receive funds and focused funding on infrastructure and startup costs without additional support for ongoing maintenance of systems. The Centers for Medicare & Medicaid Services (CMS) recently issued guidance authorizing new federal Medicaid matching payments to a broader group of providers to facilitate interoperable data exchange, which may help additional providers adopt new technology and participate in information exchange.

Even with the right economic signals and provider buy-in, significant work remains to optimize the way in which information is shared between providers and improve the utility of the information exchanged. While some data standards do exist, and efforts are underway by private organizations to create clearer and more cohesive standards, there are currently no uniform national standards for exchange of health information.
Exchange of Health Information as a Component of Governors’ Vision for Better Health, Better Care and Lower Costs

Governors have powerful levers they may use to influence the legal and market dynamics that shape health care provider choices. In the current national health care environment, costs continue to rise; health care outcomes continue to fall behind other, similarly situated nations; and much of the information necessary to coordinate care and improve outcomes is not being meaningfully shared between providers. The vision of the road map is to help drive forward state policies that support the seamless flow of clinical patient health care information between providers while protecting patient privacy.
Key Steps for States
States can use several strategies to address the legal complexities and market dynamics that limit exchange of health information. Which strategies will work best for a state depends on the state’s unique environment and challenges. As states prepare to address the wide range of potential issues impeding information flow, there are five key steps that will help ensure selection and successful implementation of the most effective strategies.

1. Assemble Core Team
2. Conduct Legal and Market Analyses
3. Determine Primary Barriers
4. Select Strategies
5. Implement and Evaluate
Step 1: Assemble a Core Team

States should assemble a core team to take ownership of strategic decision making.

Team members must buy into and commit to goals and objectives to maximize the potential gains of information flow. From within government, the core team should, at a minimum, include representation from the governor’s office, Medicaid—including privacy counsel, senior policy officials and health IT leadership—the state health IT coordinator, public health, the attorney general’s office and the agency that administers state employee health benefits. It is important that core team members include senior state officials who have authority to make decisions on policy and strategy.
In addition to state officials, states should engage external stakeholders through additional workgroups, advisory boards or committees established to support the core team’s work and make recommendations to the state. External stakeholders should include health care practitioners, health systems, privacy and consumer advocates, HIOS and academic experts. External participants can serve as an initial sounding board for the state and help garner broader buy-in from other stakeholders. Advisory groups can be established by legislative mandate or through gubernatorial authority.

Stakeholder champions and entities that are likely to serve as early adopters in the provider community are also a crucial group to involve in efforts to increase exchange of health information. When large hospital systems responsible for significant patient populations demonstrate their commitment to a policy or cultural change, others may feel more comfortable following their lead.

State medical societies and hospital associations also can be important allies because they are a trusted source of information and advice for many providers. For example, in Kansas, the state medical society and state hospital association were integral to the development and governance of the Kansas Health Information Network (KHIN), an HIO serving most of Kansas. The two societies served as champions for widespread participation among the provider community.
Step 2: Conduct Legal and Market Analyses

Before selecting strategies to increase exchange of health information, states should conduct a landscape analysis to fully understand primary challenges and opportunities related to legal and market issues. Landscape analyses can be conducted using data reviews, focus groups, surveys and informal interviews.

Legal Analysis
With regard to the legal privacy environment, analysis should include review of existing state privacy laws, primary privacy barriers for the provider community, perspectives of health care privacy advocates, patient preferences and the appetite for change among these key stakeholders.

See Appendix B on page 55 for additional background on the legal landscape pertaining to information exchange.

Key Questions for Legal Analysis

State legal landscape:

- Yes Does the state have health care privacy laws that are more restrictive than HIPAA with regard to:
  - Mental health treatment information;
  - Substance abuse treatment information (beyond Part 2);
  - HIV/AIDS-related information;
  - Genetic information;
  - Treatment information for minors; or
  - Any other aspect of treatment, payment or operations?

- Is there an appetite or desire for changes to state law?
Health care community needs:

✓ Have providers identified state laws as a barrier to sharing information to coordinate patient care?

✓ Have providers identified confusion about federal law (Part 2 and HIPAA) or state law as a barrier to sharing information to coordinate patient care?

✓ Is there a desire among health care providers to simplify consent processes for treatment?

✓ Are there any providers that would act as champions or early adopters for a policy?

Patient needs:

✓ Are patients satisfied with the quality of care they are receiving, including the level of coordination between providers?

✓ Are there consumer advocacy groups that oppose or support changing state privacy laws or policies?

Privacy community needs:

✓ Does the privacy community view exchange of health information as in the interest of patients or as a threat to patient privacy?

✓ Is there strong resistance to change among key stakeholders in the privacy community?
Market Analysis
From a market perspective, analysis should include review of existing payment structures across the state’s dominant public and private health insurers (including Medicaid and state employees), appetite for change among key stakeholders, the IT vendor landscape, existing infrastructure for exchange, the level of provider participation in exchange, the type of information being exchanged, use of the information that is flowing and the level of provider and vendor information blocking that may be occurring.

See Appendix C on page 62 for additional background on the market landscape pertaining to exchange of health information.

Key Questions for Market Analysis

Medicaid payment:
✓ What are the state’s existing payment structures for Medicaid, state employees and other predominant health insurers in the state?
✓ To what degree do payment systems incentivize exchange of health information either directly (for example, through explicit metrics that require exchange) or indirectly (for example, by developing new risk-bearing entities that necessitate care coordination and intensive communication between providers and provider entities)?
✓ What are the current dynamics for shifting to VBP models?
✓ Is there strong resistance to change among key stakeholders?

IT vendor landscape:
✓ What is the current IT vendor landscape in the state?
✓ How many EHR vendors and HIOs are in the state, and what is their market share?
✓ Have vendors been resistant or cooperative in past efforts to increase exchange of health information?
Provider exchange of health information:

✓ What is the current level of provider participation in exchange of health information?

✓ What health information is currently being exchanged, and how often is the exchanged information used in the delivery of health care?

✓ What is the existing infrastructure for exchange of health information between providers?

✓ What is the primary reason providers are not participating in exchange of health information?

Information blocking:

✓ Do key stakeholders report that information blocking is occurring among providers, health insurers or IT vendors?
Step 3: Determine Primary Barriers

Once the core team has analyzed the legal and market landscape, it should determine the most critical barriers to address to advance exchange of health information in the state. States can consider ranking barriers according to priority levels, with those that are essential to progress as the highest priority.

Categorizing barriers may be a particularly helpful exercise as states work to map potential strategies to existing barriers. For instance, a state may discover that a particular strategy that addresses a high-priority barrier may work to solve a lower priority barrier, as well.

Table 1 on page 22 lists the primary legal and market-based barriers identified by the NGA Center based on interviews with state and national experts as well as literature review.
Table 1: Legal and Market-Based Barriers to Exchange of Health Information

<table>
<thead>
<tr>
<th>Legal Barriers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legal Restrictions on Information Exchange</strong></td>
</tr>
<tr>
<td>Federal and state privacy laws pertaining to health information that are more</td>
</tr>
<tr>
<td>protective or restrictive than HIPAA can significantly limit information flow</td>
</tr>
<tr>
<td>between providers by either fully prohibiting exchange for certain categories</td>
</tr>
<tr>
<td>of information or adding burdensome requirements that make exchange more</td>
</tr>
<tr>
<td>difficult. More protective laws prohibit or restrict disclosure of specific</td>
</tr>
<tr>
<td>categories of health information deemed sensitive—such as substance abuse,</td>
</tr>
<tr>
<td>mental health or communicable disease information—without explicit patient</td>
</tr>
<tr>
<td>consent.</td>
</tr>
<tr>
<td><strong>Perceived Restrictions to Information Exchange</strong></td>
</tr>
<tr>
<td>The intent of federal and state privacy laws is often confusing to providers.</td>
</tr>
<tr>
<td>Hospital systems and provider groups are responsible for setting their own</td>
</tr>
<tr>
<td>privacy policies, which can vary based on their interpretation of the law.</td>
</tr>
<tr>
<td>These entities may apply a more restrictive interpretation of the law in</td>
</tr>
<tr>
<td>setting their privacy policies because they are confused about the true</td>
</tr>
<tr>
<td>intent of the law or are intentionally seeking to avoid legal risks</td>
</tr>
<tr>
<td>associated with improperly sharing patient information. Restrictive</td>
</tr>
<tr>
<td>interpretation adds unnecessary burden to information sharing between</td>
</tr>
<tr>
<td>providers and limits information flow.</td>
</tr>
<tr>
<td><strong>Burdensome Consent Requirements</strong></td>
</tr>
<tr>
<td>The requirement to obtain and document patient consent can be difficult for</td>
</tr>
<tr>
<td>providers, who may not feel comfortable explaining consent to patients and</td>
</tr>
<tr>
<td>may not have sufficient time to ensure that information is being shared in</td>
</tr>
<tr>
<td>accordance with the law. In some cases, providers will decide not to</td>
</tr>
<tr>
<td>exchange health information rather than engage in a burdensome consent</td>
</tr>
<tr>
<td>process.</td>
</tr>
<tr>
<td><strong>Variability Across States</strong></td>
</tr>
<tr>
<td>Varying state laws add a level of complexity for exchange of health</td>
</tr>
<tr>
<td>information across state lines. In situations where provider and hospital</td>
</tr>
<tr>
<td>systems operate in multiple states that have conflicting privacy laws, they</td>
</tr>
<tr>
<td>may adopt policies that adhere to the more protective laws to minimize risk</td>
</tr>
<tr>
<td>and avoid administrative and technical complexity. Adhering to the most</td>
</tr>
<tr>
<td>restrictive laws across multiple states results in a situation where optimal</td>
</tr>
<tr>
<td>information flow does not occur.</td>
</tr>
</tbody>
</table>
Table 1: Legal and Market-Based Barriers to Exchange of Health Information

## Market-Based Barriers

### Fee-for-Service Economics

The FFS payment model incentivizes providers to deliver high volumes of individual services as opposed to the most efficient and effective care. Under the FFS model, many experts posit that providers almost always lack strong financial incentives to share information to achieve efficiencies, such as reducing unnecessary services and better coordinating care. Without strong incentives, providers are unlikely to share data, particularly when doing so requires significant investment in systems and services, as well as workflow integration.

### Lack of Uniform Data Standards

Data standards for exchange of health information do exist, but there are no uniform national standards to which all health systems and providers adhere. The lack of national data standards allows IT vendors to develop systems and solutions according to their own design interests, which creates significant variability across systems and service platforms. Vendors are then able to charge additional fees to enable connections between systems.

### Information Blocking

In the current market environment, IT vendors and providers can benefit from limiting access to data as opposed to facilitating or participating in exchange of health information. By limiting access to data, vendors and providers can retain proprietary control over the data, which they can then use to extend lines of business or prevent patients from leaving their provider network. In some instances, efforts to limit access to data may be reasonable responses to existing economic incentives or legitimate controls to protect patient privacy or safety. In other instances, however, efforts to limit access to data are unreasonably and knowingly executed to block exchange of health information.
Step 4: Select Strategies

Once the core team has determined its primary challenges related to exchange of health information, it must select specific strategies the state can implement to address those challenges.

In many cases, a state may need to employ multiple strategies to maximize effectiveness. For instance, a state may fully align its laws with HIPAA, but if the provider community is unaware of this change or misconceptions about HIPAA remain, this strategy will not improve exchange of health information. Similarly, a state may create economic incentives for information exchange through Medicaid payment and quality mechanisms, but if many providers in the state do not have the resources to acquire technology or the infrastructure needed to support such exchange, those incentives may not be effective.

The strategies and key considerations presented in this section are meant to help states think through the optimal approach in their unique environment. Strategic decision making about legal and market issues should occur in tandem to ensure the development of a comprehensive approach. Any strategic approach must include an outreach and education component to raise awareness of existing opportunities for improving the flow of information, as well as new opportunities afforded through policy and programmatic changes.

Each strategy presented in this section includes key considerations for states as they think through value and ease of implementation. It also includes a high-level assessment of the effectiveness of each strategy. Effectiveness is ranked according to the following scale:

- ★★★★ = Very Effective
- ★★★ = Somewhat Effective
- ★★ = Minimally Effective
State Strategies to Address Legal Barriers and Increase Information Flow Between Health Care Providers

Strategy 1: Fully Align State Privacy Laws With HIPAA Through Legislative Change

Several states have fully aligned their laws with HIPAA to simplify privacy laws and promote the streamlined exchange of health information. In recent years, states—including Hawaii, Kansas, Wisconsin and Utah—have passed legislation to allow providers and hospitals to exchange patient information in accordance with HIPAA, superseding all existing, more restrictive state privacy laws. Hawaii and Kansas had a patchwork of 50 and 200 state laws, respectively, before aligning with HIPAA. See page 37 for additional information on Kansas’ approach to full alignment with HIPAA.

Considerations for Full HIPAA Alignment

Although legislative alignment significantly simplifies a state’s legal framework, a potential drawback to pursuing HIPAA alignment is the difficulty in receiving buy-in from stakeholders. First, alignment with HIPAA may improve the flow of information, but it may not reflect the preferences of patients and privacy advocates in a state. These stakeholder groups may be concerned that alignment with HIPAA will undo the state’s previous safeguards against sharing of sensitive health information and lead to situations in which information will be shared against a patient’s will. Many laws that are intended to protect patient privacy were created to increase patient trust and engagement with the health care system, and some advocates fear that removing patient control will damage that trust.

Stakeholder groups should be brought into discussions about the proper way to use data to improve care and outcomes while protecting patient rights and ensuring trust. Appropriate education is critical in enhancing advocates’ understanding of HIPAA as well as the new opportunities associated with exchange of health information to improve patients’ lives. Discussions should focus on the shared goal of better patient care and how improving the flow of information between providers is critical to preventing errors, misdiagnoses and complications.

It is important to note that although HIPAA alignment can help solve barriers related to state privacy laws, it will not reduce confusion or difficulty surrounding Part 2. States
considering full HIPAA alignment should couple this strategy with educational efforts to help providers understand not only the specific impact of legislative change to state privacy laws but also the legal landscape more broadly, including what is allowable under Part 2.

**Strategy 2: Partially Align State Privacy Laws With HIPAA Through Legislative or Regulatory Change**

| ★★★ Leads to Less Restrictive Legal Environment | ★★★ Reduces Confusion Around Laws | ★★★ Reduces Fear of Liability |

In states where there is not sufficient interest in fully aligning with HIPAA, state leaders may consider a more targeted strategy of aligning only certain laws with HIPAA. The following are examples of approaches to partial HIPAA alignment.

**HIPAA-Based Electronic Exchange**

Some states have sought to reduce legal barriers by having different disclosure standards for electronic information versus paper records, phone calls and fax. In 2007, Nevada changed its public health and safety code to exempt HIPAA-covered entities from the state’s more stringent health information privacy laws when electronically exchanging information (if the electronic exchange complies with HIPAA). See page 38 for additional information on Nevada’s approach to partial alignment with HIPAA. Ohio also has adopted this approach, amending its state code to ensure that information exchanged electronically, with certain exceptions, is not subject to any pre-existing state law based on confidentiality, privacy, security or privilege status provisions that are more stringent than HIPAA.

**Amendment of Select State Privacy Laws**

In lieu of state legislation that explicitly overrides all state privacy laws to align with HIPAA, states can create legislation that amends language in specific laws to meet the HIPAA standard for certain categories of information. For instance, Colorado amended the Mental Health Practice Act in 2011 to exempt HIPAA-covered entities and their associates from the state’s previous statute requiring consent for any disclosure of mental health treatment information.

**Considerations for Partial HIPAA Alignment**

Partial HIPAA alignment will not address all state laws or types of information sharing, but it can offer a solution to some pressing challenges inhibiting information flow. For instance, partial alignment that establishes less restrictive disclosure standards
for electronic information sharing that align with HIPAA, as done in Nevada, may be an effective strategy for states given that providers commonly document and share information in an electronic format. Similarly, partial alignment that involves the amendment of a state law governing a primary category of health information—such as mental health information—may be impactful in improving information flow that facilitates more coordinated, whole-person care. It is important to keep in mind that, like full HIPAA alignment, partial alignment may raise concerns among privacy advocates and patients who feel that it reverses the safeguards that a particular state privacy law ensures. Engaging key stakeholders early and often can help mitigate such concerns.

**Strategy 3: Create Standardized Consent Forms**

Standardized consent forms have the potential to reduce provider confusion about what they can share under the law and help clarify patient rights and provider responsibilities. They minimize the burden on providers, who may currently be responsible for creating their own consent forms for information sharing, and can help reduce the significant variability in forms from practice to practice. A standardized consent form provides a “one-stop” approach to obtaining patient consent that is good for a certain period of time and that other providers will accept. In addition to reducing the burden on providers, this standardization can improve patient understanding of consent if the form clearly explains to patients what their consent means.

The creation of a standardized consent form requires input and buy-in from a diverse set of stakeholder groups, and the process can help foster greater trust in the information being shared. **New York** has created a standardized consent form to allow providers to obtain a one-time consent for information categories more protected than HIPAA.27 Similarly, **Michigan** has created a standardized consent form for sharing behavioral health information.28 See page 39 for additional information on Michigan’s approach to standardized consent forms.

**Considerations for Standardized Consent Forms**

Currently, no state mandates the use of a consent form, so provider buy-in is essential to ensuring that the form is actually used. If providers and their legal counsel are reluctant to adopt the form, relying instead on their own consent forms, there will still be issues with disparate consent forms and multiple consents. Michigan’s Department of Health and Human Services, which houses the state’s consent form on its website
and promotes its use, has noted that an important strategy in reaching providers and legal counsel is emphasizing the value of information sharing for improved patient care. Stakeholders may have concerns about minimizing their risk, but ultimately the need to improve patient care was a unifying message.

**Strategy 4: State Guidance and Education**

One of the main obstacles to exchange of health information is concern among providers and legal counsel about what is allowed under federal and state law and associated fear of liability, particularly with regard to HIPAA (for further discussion of HIPAA, see Appendix B on page 55.)

States can consider issuing guidance to address such concerns and help providers better understand privacy laws. Such guidance could include frequently asked questions (or FAQs) or case studies that provide clarity on specific scenarios and areas of common confusion related to permissible exchange. For example, the New York State Department of Health posts a comparison chart on its website to show where HIPAA and state law differ and which law prevails. Guidance could also take the form of a letter from the state secretary of health to providers, hospital IT officers or hospital privacy counsels explaining the legal parameters of certain types of data exchange, such as ICD-10 codes or narrative notes. In addition, state agencies can conduct provider surveys and interviews so that they can better understand the challenges providers face, to focus guidance appropriately and provide examples based on actual questions.

Some state agencies have taken steps to connect providers to a wider array of resources and training materials. The Oregon Health Authority (OHA) has created a Behavioral Health Information Sharing Advisory Group that aims to help providers better understand what information sharing is allowed under federal and state law. See page 39 for additional information on Oregon’s approach to guidance and education.

Private or state-designated entities can facilitate education efforts, as well. In Kansas, the private HIO KHIN employed an extensive direct communication strategy to educate providers, hospitals and health networks about KHIN participation and best practices and to debunk incorrect assumptions and misconceptions about what can be shared
under federal and state law. As another example, Arizona’s Health e-Connections HIO developed a toolkit to help providers understand the parameters of participation in the HIO as well as rules and regulations for sharing patient information.

**Considerations for State Guidance and Education**

When conducting outreach and education, it is crucial to reach multiple branches of a provider organization or hospital’s leadership because of the varying priorities and responsibilities within a given organization that must come together to achieve the overall mission. Decision making and education efforts should, at a minimum, engage the organization’s chief information officer, legal counsel and head of population health efforts, all of whom have unique and important perspectives. If, for example, information sharing decisions were made exclusively by a privacy and compliance officer, that individual may prioritize privacy considerations above the ability to make accurate and timely health care decisions, which could significantly limit the ability to share information within and across systems, aggregate data for quality improvement and population health planning or meaningfully participate in VBP initiatives. Ultimately, the need to ensure the privacy and security of health information must be balanced with the need for adequate information flow to deliver the highest quality care, which requires the engagement of multidisciplinary teams in an organization, from physicians to staff registering patients at admission.
State Strategies to Address Market Barriers and Increase Information Flow Between Health Care Providers

Strategy 1: Create Meaningful Economic Interests That Encourage Exchange of Health Information

Longer-Term Strategies
One of the main obstacles to exchange of health information between providers is the lack of appropriate and strong economic incentives for exchange. The primary way a state can create economic interest for information exchange is through its larger efforts to change the way health care is paid for, delivered and measured. Governors can use their regulatory and oversight authority through Medicaid, the Children's Health Insurance Program (CHIP), state employee health benefits, state retiree health programs and health insurance marketplaces to encourage change. Reforms that move away from FFS volume-based payments toward aggregated risk and population health, such as accountable care organizations (ACOs), can create meaningful economic incentives to facilitate information exchange between providers.35

Shorter-Term Strategies
In addition to longer term payment and delivery system reforms, states can pursue shorter term payment and incentive strategies to encourage procurement of interoperable EHR systems and meaningful information exchange. These strategies include:

- Developing and linking Medicaid payments to performance metrics that tie directly to the exchange of health information (for example, the Oregon Health Authority has established “emergency department information exchange” as a quality metric for incentive payments to hospitals.36 See page 40 for additional information on Oregon’s approach to creating economic interest in exchange);

- Developing and linking Medicaid payments to performance metrics for which information exchange is critical to success, such as reduced number of duplicate tests, lower readmission rates or improved coordination of care for patients who have chronic health conditions;
Creating financial penalties for information blocking (for example, a one-time fee for engaging in information blocking or penalties tied to Medicaid or other insurer payments such as those imposed for hospital readmissions in Medicare);

Using federal funding, such as the expansion of 90 percent matching funds in Medicaid, to support the cost of developing interoperable systems for Medicaid providers;37 and

Providing other financial support to providers or certain categories of providers for expenses related to: purchasing interoperable systems; updating existing systems to be interoperable; establishing EHR connectivity with critical partners (middleware and interface costs); and HIO connectivity.

Considerations for Creating Economic Interest

Shifting to VBP methodologies will take considerable time, and will not be a sufficient strategy on its own if a state is looking to make progress on exchange in the short term. Rather, states should consider such a shift as part of a multipronged approach that has the potential for both short- and long-term success. For instance, many states have included pay-for-performance initiatives in their Medicaid managed care contracts and may see early progress by incorporating performance targets specifically tied to information exchange, or for which exchange of health information is critical to success. For example, if a state requires reduced readmission rates as a performance target tied to payments, providers may be incentivized to participate in an admission, discharge and transfer (ADT) notification system that requires them to send, receive and use data effectively.

Federal investments, such as the 90 percent matching funds in Medicaid, offer a prime opportunity for states to maximize resources. By design, however, these federal investments primarily support infrastructure development and will not sustain ongoing provider costs related to maintenance and operations.

In some instances, states may consider making information blocking illegal and levying fines for such activity. States considering levying financial penalties for information blocking should weigh the time and cost that may be involved in both identifying and enforcing penalties and consider opportunities to leverage existing rules and enforcement mechanisms. For example, Connecticut passed a law that prohibits health care providers and IT vendors from engaging in health information blocking by...
establishing such action as an unfair trade practice. As a result of the law, information blocking is subject to associated trade rules and regulations. See page 41 for additional information on Connecticut’s approach to prohibiting information blocking.

Strategy 2: Use Legislative, Regulatory and Contracting Authority to Bolster Exchange of Health Information

One way governors, state legislators and policymakers can improve information exchange between health care providers is by using their legislative, regulatory and contracting authority to expressly require providers or IT vendors to participate in information exchange or prohibit information blocking. Legislation for increased participation in exchange of health information could also require that providers fully connect to an HIO, or share certain data feeds; it could also require that IT vendors have certified technologies that meet minimum standards for connectivity. States can also use existing or new contracts with managed care organizations (MCOs), state employee health insurance providers or other organizations to impose requirements indirectly. For example, through its managed care contracts, Iowa has stipulated that in order for MCOs to connect to the statewide alert notification system, they must require that providers in their network send ADT feeds to the statewide system.

Considerations for Using Legislative, Regulatory and Contracting Authority to Bolster Exchange of Health Information

Primary considerations for states that seek to use legislative, regulatory or contracting authority to bolster exchange of health information relate to how the stakeholder community will react, the dominance of specific vendors (market share) and whether there is political will to pass or implement such a measure. State efforts will face greater challenges if there is limited support within the legislature or if there is significant pushback from IT vendors, providers or other stakeholders. In pursuing legal changes, states should engage stakeholders to establish buy-in and ensure clarity about definitions of and expectations for information sharing, information blocking, connectivity, certification and other concepts around which requirements or prohibitions are being structured. States will also need to think critically about the specific oversight authority they seek to implement and how it can be effectively enforced, including a review of financial resources, staff and technological capacity to carry out the policy in a meaningful way. Similar to making legislative or regulatory change, to amend contracting arrangements, states will need to engage key stakeholders and establish buy-in and agreement for new contract terms.
Governors have the unique ability to set a statewide vision for interoperable exchange of health information that clearly articulates to key stakeholders and the public its importance and value. The statewide vision may include a high-level mission or series of goals, or may involve detailed strategic objectives. Establishing information sharing as a priority for the governor will help set expectations and allow the state to hold relevant parties accountable for their role in realizing the vision. The governor can then use her or his bully pulpit to highlight best practices. This strategy also allows the state to place pressure on entities that may be blocking information by making their business practices known to the public. For example, Oregon established a health IT oversight council that is responsible for setting a strategic vision and plan for the state; as part of this effort, the state envisions highlighting state entities that are making notable progress in information exchange. See page 41 for additional information on Oregon’s approach to setting the vision.

Considerations for Setting the Vision and Holding People Accountable
In establishing a statewide vision for interoperable exchange of health information, governors and their staff should consider what level of detail to include, who should be responsible for executing the vision from a state perspective and which practices or policies do and do not represent alignment with that vision among key stakeholders. Another primary consideration for states will be how to hold people accountable for alignment with the state vision. States may choose solely to highlight those that are doing an exemplary job aligning with the state vision and working toward interoperable exchange of health information, or they may choose to highlight those that are doing poorly. Stakeholders should be engaged early and often in the development of this strategy.

Strategy 4: Serve as Convener
One of the most important levers governors have is their ability to bring diverse parties together on an issue. By serving as convener, a state can support consensus building among parties that may have differing interests, helping establish common ground and compromise. States can serve as an intermediary or resource for issues or conflicts between specific parties.
Governors and their state leaders benefit from bringing stakeholders to the table to listen to their perspectives and get buy-in on strategies to achieve a solution. The state convener role can also be useful in helping those in the provider community align on specific use cases for information sharing—such as newborn screening or advance directives for end-of-life care—which has proven to be a successful stepping stone toward broader information sharing for some organizations. Defined use cases give providers a better understanding of the value of information sharing to their specific business unit from both a process and resource perspective and allow for greater control over the management of information exchange.

States can also work with providers and vendors to build model contracts that prevent information blocking. States can play an important role in helping providers prepare to negotiate with EHR vendors by identifying specific criteria for evaluating contracts and establishing clear requirements for interoperability with other systems. For example, Vermont provided assistance to the statewide health information exchange network, providers and EHR vendors by participating in conference calls and other forums to provide clarity on connectivity standards and state law. See page 42 for additional information on Vermont’s approach to serving as convener.

**Considerations for Serving as Convener**

States that serve as a convener must clearly define what they aim to achieve in their convener role and consider the most effective manner by which to achieve that goal. The state may serve as an intermediary or may bring like-minded organizations together to coalesce around key priorities and create new partnerships. States may also consider bringing in outside experts to elevate discussions and serve as unbiased intermediaries. Importantly, serving as convener does not require that states direct the dialogue but rather allows a chance for facilitated discussion among parties that may not otherwise have the opportunity or impetus to connect with one another.

Serving as convener can be a relatively low-cost strategy that states can use to achieve important consensus building among key stakeholders. States should be sure, however, to dedicate the staff time needed to develop an effective strategy for engagement and manage the process.
Step 5: Implement and Evaluate

Once a state has selected a comprehensive set of strategies to pursue, it must build and execute implementation and evaluation plans.

The implementation plan should include program management components, such as assignment of roles and responsibilities—including designation of a team lead; development of action steps; creation of a timeline; and establishment of a governance structure. Core team leadership should pay careful attention to how timing aligns with a state’s legislative calendar, completion of a governor’s term, procedural barriers and opportunities that may slow down or speed up initiatives—such as procurement processes or timing of Medicaid contract updates. Additionally, states should carefully weigh the time and resources necessary to carry out multiple strategies concurrently and ensure that tasks and responsibilities are divided accordingly.

States also should develop an evaluation plan to monitor progress. States will need to determine the metrics that will define success for their initiatives and develop a rapid-cycle evaluation process that will allow for continuous performance assessment over the course of implementation and the ability to employ mid-course corrections as necessary. It is important to establish metrics before implementation begins to track progress as part of reporting and management processes. As states begin implementation and evaluation they may need to revisit certain strategies and action steps as new information becomes available, new barriers arise and new solutions become feasible. States should continue to work with their core teams and advisory groups to make changes to the implementation plan as necessary.

Please see Appendix D on page 66 for a list of evaluation metrics states may consider as related to the strategies presented in this road map.
Examples of State Strategies to Increase Information Flow Between Health Care Providers
Examples of State Strategies to Address Legal Barriers and Increase Information Flow Between Health Care Providers

Kansas: Full Alignment With HIPAA

In Kansas, the Kansas Health Information Technology Act of 2011 aligned the state’s laws with HIPAA, superseding the state’s previously existing health privacy laws. The language used in the law is as follows:

KSA 65-6823. Kansas health information technology and exchange act; purpose.

(a) It is the purpose of this act to harmonize state law with the HIPAA privacy rule with respect to individual access to protected health information, proper safeguarding of protected health information, and the use and disclosure of protected health information for purposes of facilitating the development and use of health information technology and health information exchange.

65-6825. Same; use and disclosure of protected health information.

(a) No covered entity shall use or disclose protected health information except as follows:

(1) Use and disclosure of protected health information consistent with an authorization that satisfies the requirements of 45 C.F.R. 164.508;

(2) use and disclosure of protected health information without an authorization as permitted under 45 C.F.R. 164.502, 164.506, 164.508, 164.510 and 164.512; or

(3) use and disclosure of protected health information as required under 45 C.F.R. 164.502.
Nevada: Partial Alignment With HIPAA for Electronic Exchange

In 2007, Nevada changed its public health and safety code to exempt HIPAA-covered entities from the state’s more stringent health information privacy laws when exchanging information electronically as long as the electronic exchange complies with HIPAA. The following is an excerpt of the Nevada statute:

NRS 439.538 Electronic transmission of health information: Exemption from state law concerning privacy or confidentiality of certain health information; ability of person to opt out of electronic disclosure of certain health information.

1. If a covered entity transmits electronically individually identifiable health information in compliance with the provisions of:
   (a) The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and
   (b) NRS 439.581 to 439.595, inclusive, and the regulations adopted pursuant thereto, which govern the electronic transmission of such information, the covered entity is, for purposes of the electronic transmission, exempt from any state law that contains more stringent requirements or provisions concerning the privacy or confidentiality of individually identifiable health information.

2. A covered entity that makes individually identifiable health information available electronically pursuant to subsection 1 shall allow any person to opt out of having his or her individually identifiable health information disclosed electronically to other covered entities, except:
   (a) As required by the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
   (b) As otherwise required by a state law.
   (c) That a person who is a recipient of Medicaid or insurance pursuant to the Children’s Health Insurance Program may not opt out of having his or her individually identifiable health information disclosed electronically.

3. As used in this section, “covered entity” has the meaning ascribed to it in 45 C.F.R. § 160.103.
Michigan: Standardized Behavioral Health Consent Form

Michigan created a standardized consent form for sharing behavioral health information. The form allows patients to designate which providers are allowed to share their information and which information should not be shared as well as allowing patients to withdraw consent. It was created to address administrative difficulties resulting from providers and hospitals across the state requiring the use of varied, individual consent forms. In 2014, the Michigan legislature passed Public Act 129 (PA 129) as an amendment to the state’s mental health code. PA 129 required both the development of a standardized form that would comply with relevant state and federal law and that behavioral health providers honor the form if a patient or another provider uses it. Michigan is also working to create an electronic version of the consent form that providers can incorporate into their EHR interfaces so that it fits more easily into their workflow.

Oregon: State Guidance and Education

The OHA has created a Behavioral Health Information Sharing Advisory Group that aims to “assist providers in determining when behavioral health information can be shared without consent, and work to clarify misconceptions and confusion about applicable state and federal privacy laws that may currently limit information sharing.” The advisory group shares publications and hosts webinars to clarify what kind of information sharing is allowed under state and federal law, with the goal of further enabling the electronic exchange of patient data for improved physical and behavioral health care coordination. The group has also partnered with the state’s department of justice in order to ensure correct interpretation of the law and to create webinars communicating allowable exchange of information.
The state of Oregon has implemented several incentives for exchange of health information as part of its health care payment and delivery reforms. In 2011, Oregon House Bill 3650 established coordinated care organizations (CCOs), or local health entities, to deliver health care and coverage for the state’s Medicaid population. The state is using quality measures and associated payments to hold CCOs accountable for the health outcomes of the population they serve. Seventeen CCO incentive measures have been developed, three of which are clinical quality measures for meaningful use of EHRs. Payments are awarded to CCOs based on their annual performance on these measures.

The state of Oregon is also encouraging exchange of health information through its hospital incentive measures. As directed by the 2013 Oregon House Bill 2216, the state has developed 11 quality measures that are tied to hospital payments. One of the 11 incentive measures directly requires that hospitals participate in exchange by sharing emergency department visit information with primary care providers and other hospitals through the state’s Emergency Department Information Exchange initiative. Numerous other hospital incentive measures indirectly encourage exchange of health information, including reducing all-cause readmissions and ensuring appropriate follow up after hospitalization for mental illness.

Finally, Oregon is incentivizing exchange of health information through its Patient-Centered Primary Care Home (PCPCH) program. Clinics in the state can apply to be recognized as a PCPCH, and those recognized are eligible for incentive payments according to the types of measures they meet. PCPCH measures related to exchange of health information include sharing clinical information electronically with other providers and care entities, meeting Meaningful Use standards for EHRs and being able to provide patients with their medical record electronically upon request.
Connecticut signed into law a bill—Conn. PA No. 15-146—that prohibits hospitals, health systems and EHR providers from “health information blocking.” The legislation establishes that such action is an unfair trade practice. Health information blocking is defined in the statute as:

“(A) knowingly interfering with or knowingly engaging in business practices or other conduct that is reasonably likely to interfere with the ability of patients, health care providers or other authorized persons to access, exchange or use electronic health records, or (B) knowingly using an electronic health record system to both (i) steer patient referrals to affiliated providers, and (ii) prevent or unreasonably interfere with patient referrals to health care providers who are not affiliated providers but shall not include legitimate referrals between providers participating in an accountable care organizations or similar value-based collaborative care models.”

Oregon: Set the Vision and Hold People Accountable

In 2009, the state of Oregon was charged with a legislative mandate to establish a strategic plan for health IT. Out of this mandate and subsequent legislative direction in 2015 the state established the Health Information Technology Oversight Council (HITOC), which is responsible for “setting goals and developing a strategic health IT plan for the state, as well as monitoring progress in achieving those goals and providing oversight for the implementation of the plan.” The HITOC members represent diverse sectors of the health industry and serve as the organizing body for Oregon’s efforts to advance adoption of EHRs and a statewide system for electronic exchange of health information.

As part of its efforts to facilitate exchange of health information in Oregon, HITOC is updating its strategic plan and accelerating efforts to bring new governance and funding to Oregon’s health information exchange environment. The OHA and HITOC are partnering with the Oregon Health Leadership Council (a collaborative group of commercial health plans), hospitals, health systems and others to develop a statewide health IT utility governance model that will seek agreement for universal data sharing across entities and bring public and private support to Oregon’s health IT infrastructure. As part of its work, OHA also envisions reinforcing the concepts of ONC’s interoperability pledge through participation in the new health IT utility model and highlighting state entities that are making particularly notable progress in information exchange.
Vermont: Serve as Convener

In an effort to facilitate exchange of health information and prevent barriers such as information blocking, in 2009, the state of Vermont passed a law that established a statewide health information exchange network—Vermont Information Technology Leaders (VITL). In 2012, additional authority was added to allow VITL to establish connectivity criteria for providers using the state HIO.52

The criteria VITL established included four incremental stages designed to achieve full interoperability among providers by stage 4. By establishing defined criteria, the state created leverage for providers who were newly acquiring, updating or replacing EHR systems to ensure that those systems had the functionality necessary to allow participation in exchange and achieve full interoperability.53 In addition to establishing connectivity criteria, the state of Vermont provided assistance to VITL, providers and EHR vendors by participating in conference calls and other forums to provide clarity on connectivity standards and state law.
## Appendices - Table of Contents

1. **Appendix A: Understanding How Providers Exchange Health Information**
   a. **Vehicles for Exchange of Health Information**
      i. **EHRs**
      ii. **Facilitating Entities**
   b. **Methods of Exchange of Health Information**
      i. **Directed Exchange**
      ii. **Query-Based Exchange**
   c. **HIO Architecture and Consent**
      i. **HIO Architecture**
      ii. **HIO Consent**

2. **Appendix B: Background on the Legal Landscape Pertaining To Exchange of Health Information**
   a. **Federal Privacy Laws**
      i. **HIPAA**
      ii. **Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2)**
   b. **Part 2 Challenges**
      i. **Confusion About Part 2**
      ii. **Technical Barriers to Sharing Part 2 Information**
   c. **State Privacy Laws**
      i. **Mental Health Information**
      ii. **HIV/AIDS Information**
      iii. **Genetic Information**
      iv. **Information About Minors**
      v. **All Health Information**
   d. **State Law Challenges**
      i. **Burdensome Consent Requirements**
      ii. **Confusion, Misinterpretation and Restrictive Interpretation of Laws**
      iii. **Complicated Technology**
      iv. **Interstate Data-Exchange Issues**
3. **Appendix C: Background on the Market Landscape Pertaining To Exchange of Health Information**
   a. **Federal Funding Supporting Exchange of Health Information**
   b. **Fee-for-Service Economics**
   c. **Resource and Workflow Challenges**
   d. **Lack of Uniform Data Standards**
   e. **Information Blocking**

4. **Appendix D: Evaluation of State Strategies**
   a. **Data Sources**
   b. **Process Measures**
      i. **Measures to Assess Progress in Addressing Legal Barriers**
      ii. **Measures to Assess Progress in Addressing Market Barriers**
   c. **Short-Term Outcome Measures**
      i. **Information Exchange Measures**
      ii. **Provider Adoption and Perception Measures**
      iii. **Delivery System Reform Measures**
   d. **Long-Term Outcome Measures**
      i. **Quality and Appropriateness of Care Measures**
      ii. **Cost Measures**
Appendix A: Understanding How Providers Exchange Health Information

Although exchange of health information has advanced over the past two decades, with the most significant progress occurring in the past eight years—primarily related to passage of the HITECH Act of 2009 and subsequent increased adoption of EHRs—health care still lags far behind other sectors of the economy in the exchange of information to improve efficiency.54

Historically, providers shared information by facsimile, mail, or phone. New technologies have created a space for greater innovation and coordination within and across health care settings. Starting with secure messaging, increasingly sophisticated technologies have allowed for real-time information sharing across EHR systems. Public and private HIOs have formed in many states and cities to facilitate exchange of information between EHR platforms and across hospital and provider systems. At the same time, standards such as Fast Healthcare Interoperability Resources have enabled new application programming interfaces that have the potential to streamline the flow of information across providers throughout the nation.55 In addition to real-time information flow, EHR and other IT vendors have developed analytical tools to maximize the utility of the data now available, helping providers and health systems track patients at individual and population health levels. Technology advancements also create new opportunities to address important patient privacy issues through data segmentation and consent management tools that can maximize information flow for optimal care while adhering to patients’ privacy preferences.

Electronic exchange of health information can occur in many ways and be led by a variety of entities, including federal, state and local government; private institutions; or a cross-section of such entities. Electronic exchange of health information can be targeted or broad in scope with respect to the amount and kind of information shared and the number of entities participating in exchange. For instance, exchange can occur between a small network of providers, such as a community hospital and ambulatory care clinics; it may be targeted for a specific use case by a large network of providers, such as ADT alerts between hospitals and primary care physicians across a state; or it may involve a central clinical data repository through which all providers in a particular region can access the majority of a patient’s health information.

This section provides an overview of how exchange of health information occurs today and the vehicles and methods for such exchange.
Vehicles for Exchange of Health Information

- **EHRs**
  Exchange of health information across EHRs can occur within a health system or network of providers, such as an ACO, that have affiliated providers who operate different EHR systems as well as between unaffiliated providers. This type of exchange requires interfaces and transport services to facilitate sharing between unique systems. Information exchange across EHR systems may be simpler to employ if providers are using the same EHR vendor or similar technologies.

This road map does not delve into the many characteristics that define a well-organized EHR that is able to effectively exchange data; however it is important for state leaders to recognize the enormous variability in the manner in which providers are capturing, sending, receiving, and using data. Many clinical data systems have significant limitations that restrict the utility of data for the purposes of patient care. The National Committee for Quality Assurance (NCQA) provides an illustrative example of a framework for clinical data systems, which includes the ability to: capture patient care in a structured, electronic format; be maintained over time; include some or all key clinical data relevant to care; facilitate bidirectional, automated sharing of information; and be accessible by the health care team at the point of care. For additional information on NCQA’s framework, please visit: http://www.ncqa.org/hedis-quality-measurement/ecds.

- **Facilitating Entities**
  Exchange of health information can occur through a facilitating entity that manages the transport of information and, in some cases, stores information across multiple providers. Facilitating entities can offer a range of services and accompanying infrastructure to support exchange.56

Because there are no uniform national standards for exchange of health information across EHR platforms and health systems, facilitating entities such as HIOs may be perceived as the most obvious solution to accommodate information exchange between providers.57 An HIO can help individual providers or hospital systems avoid establishing unique connections to all other providers with whom they might want to exchange information, but if and when uniform standards are agreed upon, direct provider-to-provider information sharing may become easier and more commonplace.
Methods of Exchange of Health Information

- **Directed, or “push,” exchange.**
  In directed exchange, information is sent and received electronically through direct secured messaging. Information can be sent in many formats, including basic notes, PDF-like attachments or standard message formats—such as ADT feeds and continuity of care documents (CCDs).

- **Query-based, or “pull,” exchange.**
  In query-based exchange, patient information is searched for or requested, and then subsequently shared through standard message formats (such as ADT and CCD).

No single best practice defines the manner or method by which to achieve interoperable exchange of health information between providers. With the appropriate infrastructure, direct EHR-to-EHR exchange and exchange through facilitating entities provide similar information-sharing capabilities, but they can differ in administrative complexity, workflow integration, data aggregation capability and cost.

With the infusion of federal dollars to support exchange of health information and HIO development through the HITECH Act, many states have pursued HIOs as a vehicle by which to facilitate exchange of health information across health care providers and, in some cases, multi-provider or state-level data aggregation for reporting, research and analytics purposes. In 2015, the Robert Wood Johnson Foundation conducted a survey identifying the types of exchange efforts underway across the country. The most commonly identified efforts were HIOs and state health information exchanges. (Note that HIOs are commonly referred to as “health information exchanges.”) Table 2 below provides an overview of exchange efforts currently underway.

### Table 2: Health Information Exchange Efforts Underway in the United States

<table>
<thead>
<tr>
<th>Type of Organization</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health information organization</td>
<td>65</td>
</tr>
<tr>
<td>State health information exchange or state-designated entity</td>
<td>32</td>
</tr>
<tr>
<td>Health care delivery organization (e.g., hospital, integrated delivery network, individual practice association and ambulatory practice)</td>
<td>17</td>
</tr>
<tr>
<td>Community-based organization</td>
<td>11</td>
</tr>
<tr>
<td>Nongovernmental organization or policy/advocacy group</td>
<td>7</td>
</tr>
<tr>
<td>Public health department or agency</td>
<td>6</td>
</tr>
<tr>
<td>Technology vendor</td>
<td>6</td>
</tr>
<tr>
<td>State Medicaid agency</td>
<td>3</td>
</tr>
<tr>
<td>Academic institution</td>
<td>3</td>
</tr>
<tr>
<td>State government (other than state Medicaid or public health)</td>
<td>2</td>
</tr>
</tbody>
</table>
Previous infrastructure investments and the potential for population-based data aggregation and analysis that HIOs afford have made them an attractive prospect for many states. Even though they can add value to efforts to increase interoperable exchange of health information between providers, stand-alone HIOs face significant challenges related to their business model and long-term financial sustainability. The greatest challenge facing stand-alone HIOs, as opposed to those developed internally to an organization such as a health system or ACO, is that too few providers participate and subscription fees are intended to generate revenue. Providers often refrain from participation because they do not see the value in doing so, which may then result in gaps in clinical data that make HIO services even less appealing. In addition, because HIOs receive limited funds from provider sign-up and subscription fees, they often rely on grant funding as a primary source of revenue—an often unstable funding stream. Providers may not participate in HIOs because they do not believe it aligns with their business interests, particularly when balanced against other resource priorities more directly linked to revenue generation (for example, new inpatient facilities and well-reimbursed diagnostic tools).

**HIO Architecture and Consent**

HIO architecture, governance and the process by which patients consent to sharing information can have significant implications for participation rates, the value of the information being exchanged and the ultimate success of HIOs. Therefore, states considering developing new HIOs or reconfiguring existing operations should consider the pros and cons associated with different HIO architecture and consent models.

**HIO Architecture**

HIOs typically have one of three primary architectures:

- **Decentralized HIO.** A decentralized HIO facilitates data sharing and exchange among independent databases. It does not store information but rather facilitates the transfer of information between providers without the need for multiple interfaces.

- **Centralized HIO.** A centralized HIO facilitates data sharing and exchange by collecting and storing information from diverse databases in a central repository. Under the centralized model, data are stored according to defined standards and allow for population-based analytics of shared information.

- **Hybrid HIO.** A hybrid HIO incorporates variations of decentralized and centralized architectures.
Centralized Repository Model

Data flows from all participating entities with clinically relevant data (such as a hospital or provider group) to a central CDR. Data are stored in the CDR and authorized users can access data as determined by security and consent policies.

EHR Data: Demographics, Orders, Results, Diagnosis, Allergies, Treatments, Notes, Lifestyle Habits, etc.
Eligibility Data: Plan effective dates and coverage
Immunization Registry: Dates immunized
Claims: Procedures, Diagnosis, Prescriptions
Personal Health Data: Procedures, Diagnosis

Decentralized (Federated) Model

Decentralized

Participating entities with clinically relevant data (such as a hospital or provider group) can request data from other participating entities. Data are transferred upon request to authorized users as determined by security and consent policies via a record locator service.

EHR Data: Demographics, Orders, Results, Diagnosis, Allergies, Treatments, Notes, Lifestyle Habits, etc.
Eligibility Data: Plan effective dates and coverage
Immunization Registry: Dates immunized
Claims: Procedures, Diagnosis, Prescriptions
Personal Health Data: Procedures, Diagnosis

Getting the Right Information to the Right Health Care Providers at the Right Time

Hybrid Model

Hybrid
Some data are held in centralized CDR and other data are held by the system in which they are created. Clinically relevant data are pulled directly from the CDR or via the record locator service when requested.

EHR Data: Demographics, Orders, Results, Diagnosis, Allergies, Treatments, Notes, Lifestyle Habits, etc.
Eligibility Data: Plan effective dates and coverage
Immunization Registry: Dates immunized
Claims: Procedures, Diagnosis, Prescriptions
Personal Health Data: Procedures, Diagnosis

HIO Consent
States and organizations may adopt opt-in or opt-out laws or policies for HIOs to collect patient consent before providers exchange electronic health information. Such laws and policies affect the ease by which providers can share information. Opt-out policies tend to increase the amount of information being exchanged because no patient action is required for data that are not subject to Part 2 or more restrictive state laws to flow, while opt-in policies tend to limit information flow because they require affirmative patient consent to exchange data.61

Some HIOs have implemented technological solutions to allow for granular choice, or the ability for patients to individually select the data they do and do not want shared, and have that choice reflected in what providers can view. In addition, states and HIOs sometimes distinguish between “consent to share” information and “consent to view” information. In other words, some HIOs may have one consent policy that governs the basic flow of information to a centralized data warehouse or cloud-based system and another consent policy that governs which providers can access or view data under what circumstances.63 Descriptions of the major types of consent policies that may be required by HIOs, or by states in governing HIOs, as well as examples of states and organizations that have such policies, are discussed below.

No-Consent (i.e. HIPAA Protections Control)
A “no-consent” HIO model abides by the HIPAA standard and automatically shares or stores patient information without obtaining patient consent for participation.64 Delaware’s HIO, the Delaware Health Information Network (DHIN), has a no-consent policy for storing patient information. All patient laboratory data, radiology reports, primary care clinical data and hospital ADT data are uploaded to the system without patient consent, but DHIN allows patients to opt out of allowing providers to view their clinical data—including emergency department providers—by completing a written opt-out request (which can later be rescinded at a patient’s request). 65

Full Opt-Out
In a full opt-out model, patients’ information is included in the HIO by default and is available for providers to share unless the patient proactively opts out. Under the full opt-out model, if a patient does not opt out, all of his or her health information that is not subject to special protections under existing law, such as Part 2, will be available to share across treating providers. If the patient does opt out, none of his or her information will be available for exchange. It is an “all-or-nothing” proposition. Virginia’s ConnectVirginia HIE, Inc. is an example of a full opt-out HIO in that all patient information is available for exchange unless patients specifically request through the opt-out process that their data not be shared. 66

Opt-Out With Exceptions
Some HIOs that use opt-out consent models have implemented technological solutions to offer some level of granular choice. Under this model, data are automatically included in the HIO, but patients must be offered the option to fully or partially opt out. Partial opt-out, or opt-out with exceptions, allows patients
to limit what is shared or the specific circumstances under which information is shared. For instance, patients may be able to opt out of participation for all information except their medication summaries, or they may be able to stipulate a set of select providers who can view their information while denying access to all others. Alaska’s HIO, the Alaska eHealth Network, has an opt-out with exceptions policy that allows patients to opt out completely, in which case their information is not stored and cannot be accessed, or to partially opt out, in which case their information is stored and available only in an emergency (commonly referred to as a “break the glass” policy).67

**Opt-In With Restrictions**

An opt-in with restrictions model requires patients to proactively consent to allow their health care providers to share their information with an HIO and gives some choice as to who can access their information. For example, in Rhode Island, by law, participation in the statewide HIO is voluntary. Individuals must enroll to have their information shared with Rhode Island’s HIO, the Rhode Island Quality Institute. In addition, patients can choose to allow all organizations involved in their care to access the information, authorize only certain providers or organizations or only allow access to their information in the event of an emergency.

**Full Opt-In**

In a full opt-in model, patients must consent to having any information available for sharing between providers, and there is no granularity of choice for which information is shared. Just as with full opt-out policies, it is an all-or-nothing model. Massachusetts is an example of a state that has a full opt-in model. In Massachusetts, patients must sign a consent form opting in before any information is stored or shared in the statewide HIO, the Mass HIway. After a patient opts in, all information about that patient can be stored and shared in the HIO.68
Appendix B: Background on the Legal Landscape Pertaining To Exchange of Health Information

Legal Disclaimer: The analysis provided in this road map is for informational purposes only and is not intended to be legal advice. You should contact your attorney to obtain advice with respect to any particular issue or question described herein.

Federal law, state law and individual organization-level policies govern the exchange of health information. HIPAA sets the floor for national privacy standards, but Part 2 and other federal privacy laws add layers of requirements for sharing information. In addition, states have the ability to set their own laws with regard to health information privacy; when these laws are more stringent than HIPAA, the state laws prevail.

This appendix provides background information about HIPAA, Part 2 and state laws as well as related key challenges.

Federal Privacy Laws

HIPAA

HIPAA, which Congress passed in 1996, governs the sharing of personally identifiable health information. HIPAA is intended to allow the flow of PHI while safeguarding patients’ rights and protecting their privacy. HIPAA applies to health information shared by “covered entities,” which include health plans, health care clearinghouses and health care providers and their business associates. The U.S. Department of Health and Human Services defines a “business associate” as a “person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.” Examples of business associates under HIPAA include agents, contractors or other entities hired to help covered entities serve their patients and that may have access to PHI.

HIPAA includes broad provisions that allow for exchange of information between entities pertaining to treatment, payment and health care operations without requiring patient consent. Providers and organizations can exchange PHI without patient permission provided that the information is necessary for one of those purposes. The one category of patient information HIPAA excludes from its normal provisions for treatment, payment and operations is psychotherapy notes. Psychotherapy notes must be kept separate from a patient’s medical record and patient consent is required before they can be shared.
Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2)

The federal rules governing exchange of information related to substance abuse treatment are more stringent than the rules governing health information under HIPAA, in part because of concerns about potential discrimination against patients whose recovery status is exposed. The Part 2 rule requires strict protections for sharing individually identifiable substance abuse treatment information as well as for the storage and destruction of treatment files.

Part 2 applies to federally-assisted drug and alcohol programs. In this context, “federal assistance” is defined broadly to include the receipt of Medicaid or Medicare payments, federal grants or other federal financial support. A “drug and alcohol treatment program” is defined as “any person or entity that holds itself out as providing, and provides, drug abuse diagnosis, treatment, or referral for treatment.” Information can be shared only when written patient consent is provided. Currently, the Part 2 consent form must contain the following information:

- Patient’s name;
- Name or designation of the person or program permitted to disclose the information;
- Recipient of the information;
- Purpose of the disclosure;
- Quantity and type of information to be disclosed;
- Right of the patient to revoke consent at any time;
- Date the consent expires; and
- A note prohibiting re-disclosure of the information.

Part 2 disclosure requirements add a layer beyond HIPAA to preserve the privacy of patients undergoing treatment for substance abuse, but also limit the ability of providers to easily access and review complete patient information. Approximately 8 million adults in the United States have co-occurring mental health conditions and substance use disorders; the care these individuals receive is fragmented among mental health, substance abuse and physical health systems, resulting in poor-quality care and higher costs. According to the Medicaid and CHIP Payment Access Commission, in 2011, “one in five Medicaid beneficiaries had behavioral health diagnoses but accounted for almost half of total Medicaid expenditures, with more than $131 billion spent on their care (including physical, behavioral, and other Medicaid-covered services).” With new system transformation efforts focusing on better coordination of care for high-need patients, there is a growing need for providers to be able to seamlessly exchange health information.

Because of the Notice of Proposed Rule Making (NPRM) that the Substance Abuse and Mental Health Services Administration issued in March 2016, changes are expected to the Part 2 rule. The proposed changes would largely apply to what is contained in the Part 2 consent form. The NPRM clarifies certain definitions within the law but, more importantly, allows a general designation in the “to whom” field of the form, letting a patient designate a general entity—such as an HIO, ACO or “all of my treating providers”—receive his or her treatment information. The proposed change could improve the ability of providers to exchange Part 2-covered information.
Part 2 Challenges

Many provider and organizational issues surround Part 2. Two issues that often arise are confusion and technical barriers.

Confusion About Part 2

Providers and organizations are often confused about whether and how they must comply with Part 2. To be subject to Part 2, a provider or organization must be federally assisted and provide alcohol or drug abuse diagnosis, treatment or referral for treatment. As such, a general medical facility or provider that does not hold itself out as a substance abuse provider is not subject to the rule, despite the fact that substance abuse information may be present in a patient’s record. If a program holds itself out as more than one kind of treatment provider, only substance abuse treatment information is subject to Part 2. Part 2 also does not apply to alcohol or drug abuse information from private, commercial insurance or employee benefits that are not federally subsidized.

Given the frequency with which mental health information and substance abuse treatment information overlap, a major misconception is that Part 2 applies to mental health providers as well as substance abuse providers. Mental health providers, however, are not subject to the Part 2 regulation unless they also hold themselves out as substance abuse treatment providers, in which case only the substance abuse information is subject to Part 2. For example, Part 2 does not apply to information about bipolar disorder or schizophrenia unless a federally-assisted drug and alcohol treatment program collected that information.

Technical Barriers to Sharing Part 2 Information

One of the most significant barriers to exchanging information under Part 2 is the fact that EHRs and HIOs are not designed to easily segment access to information. Many EHRs do not have discreet fields in which to enter sensitive information, or information may be in free-text format, making it difficult to distinguish among different types of data. Similarly, many HIOs lack the capability to segment or limit access to sensitive information. Moreover, even if a provider has the ability to segment data, once the information passes to an HIO, most HIOs do not have the ability to limit access to providers named in a Part 2-compliant consent form. Because it is difficult to build or alter systems to segment access to data and because behavioral health providers have not historically been eligible for federal health IT incentive programs, there is relatively low adoption of EHRs among behavioral health providers.
State Privacy Laws
Before HIPAA, no federal law governed the sharing of health information, and states created their own protections against the improper sharing of patient information. As a result, many states have enacted laws intended to protect the privacy and confidentiality of individually identifiable health information. Many of these laws were passed in the 1970s and 1980s, as concerns for health care privacy grew following the release of information about HIV, substance abuse or mental health treatment records of individuals. States created unique consent requirements for disclosure of information related to particular health conditions, such as mental illness, substance use disorder, HIV or other communicable diseases, as well as special populations, such as minors or victims of abuse. The laws vary widely from state to state and may apply to:

- The type of provider disclosing or receiving information;
- Type of institution sending or receiving information;
- When information can be disclosed;
- The amount of information being disclosed; or
- The type of information that can be shared, even with patient consent.

The most common types of information that state privacy laws govern are discussed below.

Mental Health Information
Many states have laws and regulations for the sharing of mental health information. A 2016 legislative analysis of state laws on mental health treatment records found that in 15 states laws were more restrictive than HIPAA and four states had laws that were judged to be a combination of more and less restrictive than HIPAA. For example, many state mental health laws require patient permission for every exchange of data, and prohibit re-disclosure, meaning that even if a patient gives his or her consent to a provider to view the information, the further sharing of information with another provider or entity is not allowed without the patient’s permission.

HIV/AIDS Information
A majority of states have laws related to the disclosure of patient information regarding HIV status. These laws typically apply to anyone who may encounter or obtain information that would reveal the HIV status of a patient, including providers, hospitals and clinics. The definition of “protected information” can differ from state to state. In some states, protected information includes information about medications and treatment; in other states, protected information is limited to test results. For example, Pennsylvania has a law that requires a patient’s written consent for disclosure of any information that could refer to the patient’s confidential HIV-related information and requires the sender to include in the disclosure a specific written statement prohibiting the information’s further disclosure.
Genetic Information

Many states have laws that restrict access to genetic information without patient consent. Genetic information laws are intended to protect individuals against discrimination based on their genetic information from employers, health insurance companies or other entities. Similar to HIPAA, the federal Genetic Information Nondiscrimination Act of 2008 does not override state laws that may be more protective. Most state laws governing genetic information require written consent before disclosure to another entity, including providers and insurers. For example, New York has a law that states that “all records, findings, and results of any genetic test are confidential and may only be disclosed with written authorization from the individual.”

Information About Minors

Under HIPAA, minors who are not emancipated from their parent or guardian require parental consent for treatment and disclosure of health records. HIPAA defines a “minor” as someone under 18 years of age; the minor’s parent, guardian or person acting in loco parentis (as a parent) must consent to their treatment and can access his or her health information and make disclosure decisions. HIPAA allows for exceptions based on state law, however. Many states have laws that allow minors under 18 years of age to consent to certain types of treatment and simultaneously gives minors full power over disclosure of related health information, including to their parent or guardian. Minor consent laws are intended to encourage minors to seek treatment for conditions that they may be otherwise reluctant to disclose to parents or guardians and typically pertain to sensitive categories of health information such as sexually transmitted diseases, reproductive health or substance abuse. For example, in California, minors as young as 12 years of age can consent to treatment for mental health, substance abuse or reproductive health care and thus can choose whether to disclose information related to that treatment. Given this dynamic, electronic sharing of a minor’s information can be challenging because of the difficulty of creating data systems able to share only particular aspects of a health record based on patient age and consent status.

All Health Information

Many states have laws related to disclosure of health information for specific populations or conditions, but a few states require consent for information sharing for treatment, payment and health care operations. Both New York and Minnesota require that providers obtain patient consent before sharing any patient’s health information except in the case of emergencies. The law in Minnesota states that:

“A provider, or a person who receives health records from a provider, may not release a patient’s health records to a person without: a signed and dated consent from the patient or the patient’s legally authorized representative authorizing the release; specific authorization in law; or a representation from a provider that holds a signed and dated consent from the patient authorizing the release.”
State Law Challenges
The variety of state health privacy laws that layer on HIPAA can add complexity and create confusion about the sharing of health information within states and among providers. State laws governing the sharing of health information exist as a patchwork, differing from one state to the next, whereby information sharing may not take place because providers or HIOs do not feel they can abide by all the laws pertaining to exchange or information sharing occurs but at great cost and complexity, using resources that could otherwise be devoted to other purposes. Specific challenges are discussed below.

Burdensome Consent Requirements
Even when patient information can legally be shared with patient consent for purposes of improving the quality and efficiency of care, the requirement to obtain and document patient consent can be difficult for providers, who may not feel comfortable explaining consent to the patient and may not have time to ensure that the information is shared in accordance with the law.94

Confusion, Misinterpretation and Restrictive Interpretation of Laws
The intent of state health privacy laws is often a source of confusion for providers and organizations. State laws may include terms that are left undefined and unclear. For example, state laws may allow the sharing of information without patient consent “when necessary for treatment”95 or “when it is in the best interest of the patient.”96 Such terms can be ambiguous and may be difficult to interpret, particularly if that interpretation occurs on a case-by-case basis by hospitals and providers without reliance on IT systems that can automatically adhere to the patient’s predefined consent preferences. Furthermore, generalized terms are especially challenging to interpret when operationalizing electronic information systems.97 There may be confusion about whether legal language covers different components of the medical record, such as prescription drug codes or codes showing a referral to a behavioral health practitioner. HIPAA, in contrast, clearly defines the exception it creates for “psychiatric notes separately maintained.” Hospital systems and provider groups are responsible for setting their own privacy policies, which can vary based on their interpretation of the law. These entities may apply a more restrictive interpretation of the law to avoid legal risks associated with improperly sharing patient information. The variable nature of hospital policies creates a further layer of complexity on top of federal and state laws and can be an additional barrier to sharing patient information.

Complicated Technology
Creating health information systems that are compatible with the intricacies and variability of state laws is difficult and adds costly complexity to establishing an interoperable EHR or HIO platform. Providers and technology are far from achieving the goal of computable privacy, in which technology is able to consistently capture, communicate and process patient choices for where their data should flow while at the same time operationalizing compliance with applicable laws.98
One solution is the creation of data segmentation capabilities in EHRs. “Data segmentation” refers to the use of technological applications, such as electronic labeling or tagging, to allow an individual or entity to share only certain segments of a patient’s record. Given that it is a relatively new mechanism for separating information according to consent preferences, many providers do not yet have the technology required to segment data, although this may change with the introduction of the new optional Data Segmentation for Privacy (DS4P) standard for certified EHRs in 2018. The DS4P standard applies to both sending and receiving data, and EHRs that use this standard would provide the technical capability to enable a sending provider to tag a record and a receiving provider to recognize that tag. The tag would alert the provider to sensitive data in the record and the need to follow appropriate state or federal law when accessing the information. The standard is optional, however, and providers would need to request that their vendor include the capability in their EHR.

**Interstate Data-Exchange Issues**

There are many instances where health information needs to flow between providers in different states. For instance, neighboring states may have residents who live on the state border and travel across state lines frequently to receive care, or individuals may travel to another state, experience a health crisis and require care in that state. In addition, providers and hospital systems that have locations in multiple states and are subject to each state’s laws. In these situations, providers and health systems may adopt policies that adhere to whichever state has the most protective policies to minimize risk and avoid administrative and technical complexity. This approach can significantly restrict the flow of critical information between providers.
Appendix C: Background on the Market Landscape Pertaining To Exchange of Health Information

Purchasing, maintaining, updating and incorporating interoperable data systems and services into provider workflow requires significant investment on behalf of health care providers. Some experts believe that these investments should be assumed as a cost of doing business for health care providers; many providers, however, continue to report a lack of adequate resources and strong financial incentives for participation in exchange. This appendix provides background information about existing incentives for and barriers to exchange of health information shaping current market dynamics.

Federal Funding Supporting Exchange of Health Information

Providers have been successful at securing substantial federal investments to support their adoption of data systems. As mentioned in Section 1, through the HITECH Act, the federal government has made significant investments to support providers in adopting new EHR technology and the development of HIOs to help facilitate exchange of health information. The law included provisions for incentives and penalties for EHR adoption among certain providers—physicians, chiropractors, dentists, optometrists, podiatrists, psychiatrists and most hospitals—and established standards and associated incentive payments for meaningful use of EHR technology.

Since 2011, the federal EHR incentive payment program has provided more than $30 billion to encourage hospitals, office-based physicians and other “eligible providers”—that is, eligible professionals or hospitals—to adopt and meaningfully use EHRs, with the goal of using those limited funds to achieve connectivity. The incentives excluded many other categories of providers, however. In 2016, CMS issued a State Medicaid Director Letter that permits states to request 90 percent enhanced matching funds from CMS to connect a broader variety of Medicaid providers for health information exchange and to encourage the adoption of certified EHR technology.

Subject to CMS prior approval, states can now claim 90 percent HITECH matching funds for expenditures related to connecting eligible providers to other Medicaid providers, including behavioral health providers, substance abuse treatment providers, long-term care providers (including providers operating in nursing facilities), home health providers, emergency medical service providers, public health providers, correctional health providers, community-based providers, pharmacists and providers of laboratory services. The program, however, will only cover costs for other Medicaid providers to connect to eligible providers if that connection will help eligible providers demonstrate meaningful use.

The federal health IT investments are designed as one-time payments to support infrastructure development; they do not support all IT costs that providers incur, such as those related to maintaining and updating systems and services.
Fee-for-Service Economics

Despite general consensus on the value of information exchange in making health care more efficient and effective, the majority of providers are still not exchanging data in a systematic and effective manner.\(^\text{105}\) There has been significant progress in EHR adoption and a shift away from paper records in the past decade. Efforts are also underway to improve exchange of information between providers, but a great deal more must be accomplished to ensure robust data exchange. According to a 2014 study, only 30 percent of hospitals in the United States participate in exchange of health information with unaffiliated providers, although rates can vary significantly across states.\(^\text{106}\) Many experts believe that a primary reason many providers are still not participating in data exchange is that it runs counter to their economic incentives in a predominately volume-driven, FFS payment system.\(^\text{107}\) As discussed in Section 1, despite efforts to move to VBP models that would encourage greater information sharing by tying financial incentives to quality of care, health care providers continue to primarily be paid for each service they deliver. When providers do not receive adequate incentives for care coordination and other activities that lead to more efficient care and better outcomes, the economic value of data exchange is limited and may even work against data sharing.\(^\text{108}\)

For example, if a provider sees a new patient and needs to order an imaging test (which is often highly profitable), data exchange may reveal that another provider recently ordered the same imaging test, eliminating both the need to conduct the test and the additional payment. This financial penalty can easily swamp the marginal economic benefits associated with data exchange facilitating better patient care.\(^\text{109}\) Alternatively, under a VBP model, providers are financially rewarded for minimizing overall costs and improving patient outcomes through efficiencies such as fewer duplicative tests and better coordinated care, which creates an economic incentive for robust information exchange.

Ultimately, most providers strive to deliver optimal care to their patients, but they must do so within the confines of the existing payment structure; many experts believe that we will not reach widespread interoperability among providers unless it yields a meaningful economic benefit.\(^\text{110}\)

Resource and Workflow Challenges

Providers face significant resource and workflow challenges related to participation in exchange of health information that serve as underlying barriers to information flow. Some providers previously invested in EHRs that were not interoperable and now cannot afford or do not see the value in investing in system updates that would enable interoperable exchange.\(^\text{111}\) To exchange information with an HIO or other EHR systems, unique EHRs require software modifications or the purchase of additional middleware.\(^\text{112}\) Some progress has occurred in EHR interoperability across vendors, and there are growing multivendor interoperable networks, but most providers still struggle with the complexity and cost to connect from a technology, governance and workflow perspective. There is no simple “plug-and-play” option whereby providers can easily purchase technology and connect to one another.
Resource limitations may prevent smaller providers from participating in HIOs, which typically require payment of multiple fees. Fees can include an initial connectivity charge and recurring annual membership or subscription fees. In addition, existing data or data formats may not adequately meet provider needs. Data feeds may offer too much, too little, poorly-organized or difficult-to-ingest information. For example, a provider may receive a lengthy care summary in which relevant information is buried.

Another challenge providers face is that EHRs may have poor user interfaces that require extra work and time to operate. For example, providers may be required to log in to multiple portals or work through various tabs to review information about a patient. Additional time required to access and review information may delay providers from seeing more patients (a central concern in FFS-financed delivery systems), interfere with the patient-provider interaction and even affect the morale of providers operating in high-pressure environments.113

Providers also struggle with staff capacity and IT knowledge. They often do not have enough staff or staff with the right expertise to be able to operationalize exchange of health information.114 For instance, a provider may not have a staff member with the IT expertise necessary to procure, implement or troubleshoot new systems and services, or the provider may lack the appropriate number of administrative or clinical coordination staff members necessary to facilitate the workflow adjustments required for meaningful exchange—a particular concern in smaller practices.115

Even if resource and workflow challenges can be overcome, significant institutional or cultural barriers to data exchange may remain. For instance, research indicates that many providers who are near retirement may not be willing to focus on developing and using interoperable data.116 In addition, providers in remote locations may have challenges with connectivity because of lack of or limited broadband availability.117

**Lack of Uniform Data Standards**

Lack of clear, universal technology and data standards is a key underpinning of existing market dynamics related to exchange of health information.118 Some standards for information sharing do exist, such as those developed by Health Level Seven International (commonly known as HL7), which provide a general framework for data sharing between health care applications but allow for a great deal of flexibility in how those standards are implemented.119 Other organizations and alliances have been created in recent years to improve interoperability between providers and systems, including the CommonWell Health Alliance, The Sequoia Project and the Care Connectivity Consortium, but there are no universal standards that all providers observe.120

Because universally accepted national standards do not exist and the standards that do exist allow significant room for interpretation, vendors develop systems and solutions according to their own design interests, typically charging providers additional fees to develop middleware and interfaces that enable connections between systems. If universal standards existed, providers might be able to more reliably procure technology that maximizes interoperability at a lower cost.
Information Blocking

In 2015, at the request of Congress, ONC produced a report on information blocking, including the extent to which information blocking occurs and what a comprehensive federal-level strategy to address information blocking might include. According to the report, information blocking refers to “persons or entities knowingly and unreasonably interfering with the exchange or use of electronic health information.” Information blocking may occur directly, meaning that information is held back or not shared with other entities as a primary business practice, or indirectly, meaning that entities employ creative business practices and policies that make it unreasonably difficult to share information. For example, EHR vendors can indirectly block information through pricing strategies that make it cost prohibitive for providers to purchase interoperable systems or services.

In the current environment, to retain or expand market share of EHR services, health IT vendors may fight to retain market share by asserting that their data cannot be interoperable with competitors’ systems without the creation of complex, often costly interfaces. Vendors may technically adhere to certain standards that allow for exchange on a foundational level (as opposed to syntactic or semantic interoperability) but still provide data in highly inefficient formats. For instance, a provider using vendor X’s EHR who makes a request for information about a patient from a different provider who uses vendor Z’s EHR may receive a single PDF-like file that vendor X’s EHR can generate but cannot fully ingest without manual data entry.

Many IT vendors want to expand their service offerings, particularly by providing analytics services. As EHR and HIO vendors enter the analytics market, those vendors have an additional disincentive to share data with potential business competitors. By limiting access to data, a company can establish leverage as the least complex choice, both operationally and legally, for analytics contracts.

Similarly, providers themselves may refrain from participating in exchange or limit access to their data to retain proprietary control. Under the current economic model, data exchange creates an opportunity for providers to develop market advantages over their competitors that may reduce providers’ willingness to share data. For example, if clinical data are flowing in real time about the services patients are using, competing providers could use such information to attract these patients to their institutions (for example, a competing health system “stealing” patient volumes). Moreover, providers may have proprietary protocols or systems of care that allow them to distinguish themselves within a market, and sharing clinical data may facilitate the “reverse engineering” of such protocols by competitors.

As the ONC report notes, there are many valid reasons why providers and IT vendors may refrain from participating in data exchange, and the distinction between what is valid and what constitutes information blocking can sometimes be difficult to discern. Whether a practice or policy constitutes information blocking is typically determined on a case-by-case basis. Additional work needs to be done to establish a clear threshold or standard for identification and enforcement of information blocking.
Appendix D: Evaluation of State Strategies

The most effective strategies to improve information flow will include continuous monitoring and a strong evaluation plan. This appendix discusses some of the data sources and evaluation measures states can use to assess their progress. It includes process measures that can help states quantify success in meeting the goals of their implementation plans. States also can look to short-term outcome measures related to improving information flow and provider experiences with health information sharing. Finally, states should consider longer-term outcome measures which point to the value of health information sharing in helping improve the quality and efficiency of patient care.

Data Sources

States may consider using the following data sources to evaluate their progress. States may only need or have access to certain data depending on their individual goals and resources. The list presents data sources in order of sequential impact, beginning with providers connecting to EHRs and HIOs, to changes in provider practice and patient care.

- **EHR data** such as direct messages, CCDs and ADTs, to measure increases in the exchange of information
- **EHR Incentive Program data** such as program registration and Meaningful Use attestation data from CMS and ONC, to measure the number of providers adopting EHR technology and meeting Meaningful Use milestones
- **HIO utilization data** such as queries, data submissions, and alert notifications, to measure HIO service use
- **Surveys of providers in the state** such as those conducted by trade associations, provider journals and publications, or state entities, to identify provider use and perceptions of EHRs, HIOs and the overall data sharing environment
- **Surveys of consumers in the state** conducted by consumer organizations, consulting firms, or state entities, to gauge awareness and engagement with health information sharing
- **Claims and encounter data** from Medicaid, Medicare and commercial insurance, to examine changes in clinical practice and health service delivery
Process Measures

The following measures can help states monitor the achievement of specific milestones in their implementation plan related to the legal and market environment. The order of the measures reflects the complexity of the policy changes, starting with the most complex measures requiring the greatest political will, buy-in and financing.

Measures to Assess Progress in Addressing Legal Barriers

- Changes to state law or regulation reducing restrictiveness of legal environment
- Changes to state law or regulation intended to prevent information blocking
- Development and issuance of guidance to clarify state and federal law
- Convenings and webinars to educate health care providers and their support staff on state and federal law
- One-on-one outreach conducted to educate health care providers and their support staff on state and federal law

Measures to Assess Progress in Addressing Market Barriers

- Creation of new VBP arrangements in Medicaid and state employee health insurance
- Adoption of metrics intended to directly or indirectly incentivize exchange of health information through Medicaid MCO contracts or other state purchasing vehicles

Short-Term Outcome Measures

These measures are intended to measure the immediate outcomes of state efforts to improve information exchange, including changes in provider incentives, health information exchange occurring between providers, and provider perception of health information sharing and health care markets. Measures are presented in categories according to the types of outcomes they seek to achieve.
Information Exchange Measures

**Provider to Provider Exchange via EHRs**

- Number and percent of providers in a state that have adopted an EHR by provider type and EHR vendor
  - Including number and percent of behavioral health providers (social workers, community mental health centers, psychiatric hospitals/units, residential treatment centers, psychologists) using an EHR.
- Number and percent of providers in a state exchanging information using an EHR by provider type and EHR vendor
  - Within networks
  - Across networks
- Number and percent of providers participating in EHR Incentive Programs
  - Number and percent of providers meeting Meaningful Use milestones
- Types of data being exchanged (labs, CCDs, ADTs, discharge summaries, imaging reports, referrals, screening assessments, psychiatric evaluations, discharge/transition plans, progress notes)
- Number and percent of admissions, discharges and transfers that have an associated ADT notification going to a provider

**Provider to Provider Exchange via HIOs**

- Number and percent of provider organizations participating with an HIO:
  - Number and percent of providers retrieving data from an HIO via a viewer or portal, including provider success rate for querying and retrieving data on their patients from the viewer or portal
  - Number and percent of providers retrieving data from an HIO through their own EHR
  - Number and percent of providers sending information to HIO(s) on a regular basis
- Number of patients whose data are being exchanged via HIO
- Ability for interstate HIO information sharing
- Volume of information sharing occurring between HIOs across state lines

**Provider Adoption and Perception Measures**

- Ease of EHR technology adoption
- Ease of incorporating EHR technology into health care provider and support staff workflow
- Ability to meaningfully use patient data received through exchange
- Satisfaction with practice transformation efforts related to data exchange
Delivery System Reform Measures
» Implementation of delivery and payment reforms to incentivize value
  » Percent of providers’ revenue tied to VBP arrangements
  » Number and type of VBP arrangements occurring in the state
  » Number and type of providers participating in VBP arrangements
  » Number of patients receiving care under a VBP arrangement

Long-Term Outcome Measures
These measures evaluate the long-term impact of policy and programmatic changes related to health information sharing, including more efficient, higher quality care and lower costs. Because measures evaluating long-term outcomes are dependent on many factors, health information exchange accounts for only a portion of the change. The measures are listed in order of quality and cost impact, beginning with the most impactful.

Quality and Appropriateness of Care Measures
» Reduction in preventable ED visits
» Reduction in ambulatory-sensitive admissions
» Reduction in 30- and 60-day readmission rates after discharge
» Reduction in preventable adverse drug events
» Improvement in medication adherence

Cost Measures
» Reduction in total cost of care
» Reduction in cost of inpatient, ambulatory and emergency visits or admissions
» Reduction in duplicate or unnecessary tests and procedures (such as CT scan, MRI, radiograph, immunization)
» Reduction in pharmaceutical spend resulting from more cost-effective prescribing patterns
Endnotes

1 “Interoperability” in this setting is defined as the ability of two or more systems or devices to exchange and interpret data. For systems to be interoperable, they must be able to exchange information and meaningfully use the information they have exchanged. For more information, see Fridsma, D. (2014). Interoperability vs health information exchange: Setting the record straight. Health IT Buzz. Retrieved from https://www.healthit.gov/buzz-blog/meaningful-use/interoperability-health-information-exchange-setting-record-straight


12 Gilman, D. J., & Cooper, J. C. (2010). There is a time to keep silent and a time to speak, the hard part is knowing which is which: Striking the balance between privacy protection and the flow of health care information. Michigan Telecommunications and Technology Law Review 16(2). Retrieved from http://repository.law.umich.edu/mttl/vol16/iss2/1


Getting the Right Information to the Right Health Care Providers at the Right Time


19 National Governors Association. (2016, February). Interview with Laura McCrary, Executive Director of the Kansas Health Information Network.


33 National Governors Association. (2016, February). Interview with Laura McCrary, Executive Director of the Kansas Health Information Network.


35 National Governors Association. (2016, February). Interview with Laura McCrary, Executive Director of the Kansas Health Information Network.


National Governors Association. (2016, July). Interview with Georgia Maheras, Deputy Director of Health Care Reform for Payment and Delivery System Reform and Director, Vermont Health Care Innovation Project, Agency of Administration, State of Vermont.


National Governors Association. (2016, June). Interview with Susan Otter, State Coordinator for Health Information Technology at Oregon Health Authority.


Getting the Right Information to the Right Health Care Providers at the Right Time


65 Ibid.


76 Ibid.


Introduction

Background

Key Steps for States

State Examples

Appendices


87 Foley & Lardner LLP. (2014). Privacy issues in the sharing of genetic information. Retrieved from https://www.foley.com/files/Publication/7465587b-5df9-4f85-9969-68ce1b4c39af/Presentation/PublicationAttachment/88ba6035-c031-4ff4-b4e2-6ad5030b17d/PrivacyIssuesintheSharingofGeneticInformation.pdf


90 2016 Minnesota Statutes § 144.293. Retrieved from https://www.revisor.mn.gov/statutes/?id=144.293


93 2016 Minnesota Statutes § 144.293. Retrieved from https://www.revisor.mn.gov/statutes/?id=144.293


96 Ibid.

97 Ibid.


100 Ibid.


Wang, T. & Biedermann, S. Running the Numbers on an EHR: Applying Cost-Benefit Analysis in EHR Adoption. AHIMA. http://bok.ahima.org/doc?oid=101607#WCDubMEzVqJ


“Middleware” refers to software that acts as a bridge between two systems to translate data and allow the two systems to interact. In the electronic health records market, middleware has recently been touted as a potential solution to the lack of interoperability between disparate systems, similar to the way this type of technology has been used in the financial and retail industries to bridge gaps between complex software applications. For more information, go to http://bok.ahima.org/doc?oid=107645#V6THrlLqrLc and http://www.healthcarebusinesstech.com/middleware-ehr-interoperability


Ibid.


Health Level 7 International Web site: www.hl7.org


Getting the Right Information to the Right Health Care Providers at the Right Time

124 Ibid.
126 Gilman, D. J., & Cooper, J. C. (2010). There is a time to keep silent and a time to speak, the hard part is knowing which is which: Striking the balance between privacy protection and the flow of health care information. Michigan Telecommunications and Technology Law Review 16(2). Retrieved from http://repository.law.umich.edu/mttlr/vol16/iss2/1
131 Ibid.