HEALTH CARE PROVIDERS NEED EFFECTIVE DATA-SHARING GOVERNANCE

By Ania Labno, Josh Kellar, Janine May, Sophie Ding, and Tom Retelewski

TO REALIZE THE TRANSFORMATIVE potential of big data, health care providers and other stewards of patient information must implement effective data governance. The challenges are significant, however, especially for special categories of data such as protected health information and personally identifiable data. Providers must create an efficient process that concurrently addresses a number of complex privacy, cybersecurity, business, and legal considerations.

What's the solution? The secret is excellence in the mundane: transparent processes and governance that enable more intensive oversight of partnerships when necessary, without creating an overly cumbersome bureaucracy for routine data sharing.

Tackling the Challenges of Effective Governance

As artificial intelligence (AI) and related capabilities mature, providers face growing opportunities to create clinical, operational, and financial value by sharing patient

data with innovative partners. For example, companies such as Flatiron, Tempus, and 23andme have created significant value by applying AI and analytics to patient data. To capture these opportunities, organizations are sharing data across a large number of vendors that provide services to improve patient care.

But these data-sharing arrangements have attracted increasing scrutiny from the public and regulators. Because regulators have imposed very strict standards, providers generally cannot share protected health information without a patient's consent, although there are limited exceptions. A number of recent public controversies—relating to, for example, Ascension's partnership with Google and Memorial Sloan Kettering's engagement with an AI startup—illustrate the importance of implementing effective data governance and cybersecurity.

Strong governance is challenging for many reasons. Business leaders want to swiftly resolve oversight decisions in order to capitalize on the potential for fast-moving

digital innovation, but providing adequate control across multiple organizational functions (such as privacy, cybersecurity, and legal) is complex. Moreover, organizations must develop processes that allow them to fairly assess the value data-sharing arrangements bring to potential partners and ensure that partners receive their appropriate share of that value.

The inability to manage data-sharing governance well can create a backlog of approval requests and long processing times. This results in frustration among business leaders seeking to share data and makes providers less attractive to potential innovation partners.

By capably governing their data sharing, providers can capture the value of data while mitigating the risk. Effective governance allows them to carefully consider data commercialization opportunities, ensure that the business arrangement aligns with their mission to promote community health, and engage with stakeholders in the community. At the same time, it enables compliance with all legal and regulatory requirements and minimizes cybersecurity risk. Successful partnerships between Intermountain and Amgen and Geisinger and Regeneron, for example, have delivered value to both organizations, and more importantly to their patients.

Although details can vary across providers, achieving effective data-sharing governance generally requires:

- A tiered, cross-functional governance structure with well-defined decision rights

- A centralized, highly efficient process for evaluating and monitoring requests for new data-sharing arrangements

- Investment in technologies that support process efficiency and data security

A Balanced Structure

The key to an effective governance structure is balance. Structures that require

senior-leadership involvement in all data-sharing decisions, even routine ones, create bottlenecks and incentives to circumvent the process. Conversely, structures that do not define clear escalation pathways increase risk exposure by failing to provide adequate oversight. Providers with effective governance structures use clear criteria, tied to risk level, to decide when to involve senior leaders.

Escalation to senior management should be triggered when a data-sharing request is accompanied by nonroutine levels of risk—such as when the data shared is more than the minimum necessary for the intended purpose. Other examples include data requests that involve:
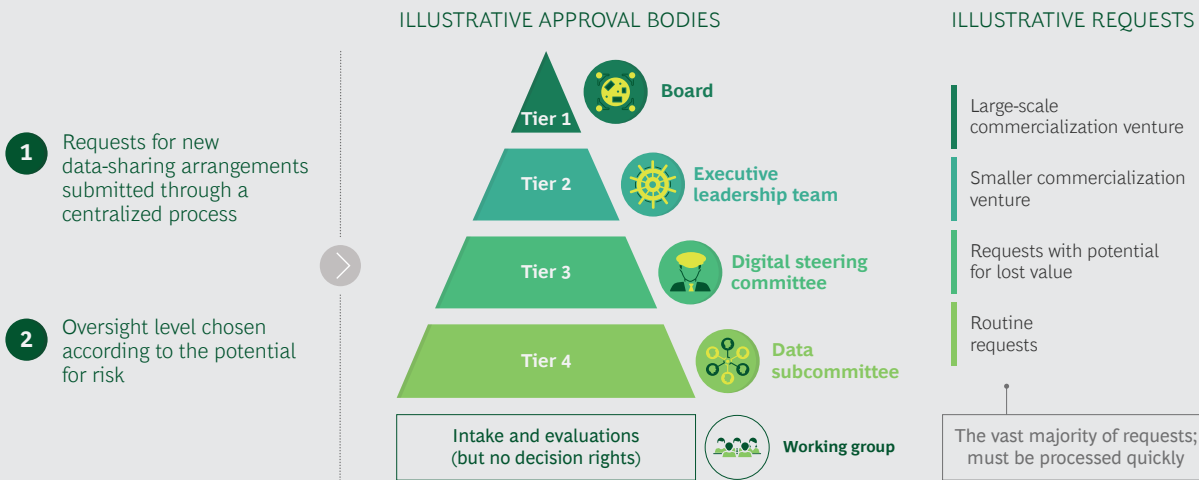
- A possible conflict of interest

- Significant concern regarding the partner's cybersecurity capabilities and practices

- A potential for conflict with the organization's mission or a partnership that raises the possibility of reputational damage

- Concern about secondary uses of the data without appropriate compensation, resulting in lost value

An effective structure has multiple tiers of oversight. (See the exhibit.) Approval by the board or senior management (or both) should be required for rare, high-risk requests, such as large commercial arrangements with significant potential to bring public scrutiny (likely fewer than a handful per year). The vast majority of requests, with lower levels of risk, should be adjudicated by designated data-sharing governance bodies guided by clear policies that ensure appropriate speed.

An Efficient and Transparent Process

The most important characteristic of a data-sharing governance process is efficiency. To effectively manage risk, providers should have a centralized process that

Effective Data-Sharing Governance Requires Tiered Oversight

ILLUSTRATIVE APPROVAL BODIES

Tier 1 — Board

Tier 2 — Executive leadership team

Tier 3 — Digital steering committee

Tier 4 — Data subcommittee

Intake and evaluations (but no decision rights) — Working group

1. Requests for new data-sharing arrangements submitted through a centralized process

2. Oversight level chosen according to the potential for risk

ILLUSTRATIVE REQUESTS

Large-scale commercialization venture

Smaller commercialization venture

Requests with potential for lost value

Routine requests

The vast majority of requests; must be processed quickly

Source: BCG.

---

provides visibility into all sharing that occurs across the organization. It is critical that this process be fully transparent and not become overly bureaucratic or cumbersome, especially for routine requests. The goal is to avoid delays that frustrate business owners who submit requests, which could lead to noncompliance. To hit target turnaround times, organizations need to ensure that the process has the appropriate resources, including dedicated employees and essential technology (described below). These investments will pay for themselves as providers capture greater value from their data.

Providers can foster efficiency by creating a streamlined intake procedure that quickly identifies the level of oversight required and improving coordination among the functions involved in evaluating requests (such as privacy, compliance, cybersecurity, IT, and legal). Additional efficiencies can be realized by maintaining a high level of communication and transparency with business owners on the status of their requests, including rapidly flagging outstanding information required to complete evaluations. A streamlined process also removes redundancies among functional evaluations—the goal is to ask each question only once.

In addition to implementing a clear decision-making and evaluation process,

providers need to develop several supporting programs, including:

- **Training.** Data-sharing governance processes and expectations must be clearly communicated to all stakeholders in order to foster a culture aligned with good governance. It should emphasize the benefit of governance procedures, draw the connection between protecting patient data and the organization's broader mission, and communicate a clear mandate to follow the process.

- **Community Engagement.** Although not necessary for routine arrangements, engagement with external advisory bodies is recommended for high-risk, high-profile arrangements, especially those with a commercial dimension. Ideally, two boards should be established: one consisting of patients and another consisting of people with deep expertise in the ethics, law, and business of data sharing.

- **Strengthened Consent and Privacy Management.** In addition to complying with consent practices mandated by law, providers should strongly consider implementing consent mechanisms for high-profile arrangements, even when not legally required (such as in the case of de-identified data). As public and

regulator concerns about privacy rights grow, offering the ability to opt out—a "right to be forgotten"—will be critical for innovative providers seeking to avoid reputational damage.

Foundational Enablers

Building effective data-sharing governance requires more than well-designed structures and processes—investment in technology is critical to ensuring that the process runs smoothly. Digital tools are needed for consistent, timely, and secure data sharing. They can increase efficiency by enabling automation and helping to operationalize the workflow.

Key technology enablers include:

- Data inventory and catalog tools, which equip data stewards and governance bodies with critical information to inform oversight and decision making.

- Workflow operationalization tools, which sequence and coordinate the end-to-end data-sharing process to increase efficiency and reduce manual dependency.

- Enterprise data platforms, which formalize data management, provide access to consolidated and structured data sets, and enforce centrally managed access controls.

- Data-centric security tools, which are critical to securing data assets—whether on premises or in the cloud—throughout the sharing life cycle. The tools should enable data loss prevention, de-identification, encryption, multifactor authentication, management of access privileges, secure cloud access, continuous monitoring, and alerts, among other capabilities.

- Governance, risk management, and compliance tools, which perform a variety of functions, including management of third-party risk, policies and documents, and legal issues and contracts.

Recently available cloud technologies provide streamlined capabilities for establishing and enforcing data-sharing governance. These technologies provide long-term integrated solutions but require enterprise-wide cybersecurity and data protection policies that cover cloud data management models, as well as the ability to manage cloud infrastructure.

AS TECHNOLOGY TRANSFORMS health care, providers must ensure that patient data is used safely and ethically. Effective data-sharing governance is essential for making this happen. The challenges are significant, including the need for sophisticated coordination across functions, investment in enabling tools, and grappling with ethical considerations at the leading edge of innovation. The first providers to overcome these challenges will be at the forefront of unlocking the potential of big data in health care.

About the Authors

Ania Labno is a partner in the Chicago office of Boston Consulting Group and a core member of the Health Care practice. She has expertise in digital and data and analytics solutions in health care. You may contact her by email at labno.ania@bcg.com.

Josh Kellar is a managing director and partner in the firm's Chicago office. He is a core member of the Health Care and Corporate Finance and Strategy practices, with expertise in advanced analytics, value-based delivery of health care, and the application of new digital technologies in health care. You may contact him by email at kellar.josh@bcg.com.

Janine May is a project leader in BCG's Chicago office and a core member of the Health Care practice. You may contact her by email at may.janine@bcg.com.

Sophie Ding is a manager at BCG Platinion and a core member of the Cybersecurity practice. You may contact her by email at ding.sophie@bcgplatinion.com.

Tom Retelewski is a managing director at BCG Platinion. You may contact him by email at retelewski.tom@bcgplatinion.com.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we help clients with total transformation—inspiring complex change, enabling organizations to grow, building competitive advantage, and driving bottom-line impact.

To succeed, organizations must blend digital and human capabilities. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives to spark change. BCG delivers solutions through leading-edge management consulting along with technology and design, corporate and digital ventures—and business purpose. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, generating results that allow our clients to thrive.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.