Digital Health Governance: Management and Strategy for the 21st Century Digital Economy

Save to myBoK

By Jennifer S. Geetter and Dale C. Van Demark

Digital health technologies, solutions, and approaches to decision-making are transforming the delivery of healthcare, reshaping patient (and health consumer) expectations, and presenting health plans, health systems, informatics companies, and other stakeholders with a dizzying array of digital health solutions and products. The promise of telemedicine, remote monitoring and wearable health devices, and other technologies in healthcare is real—but potential customers must still contend with how best to assess the seemingly ever-expanding digital health options available or being introduced to them to distinguish the gimmick from the game changer. At the same time, state and federal regulation, mandated quality data reporting, and healthcare transaction coding sets, are challenging the capacity of health information managers and the ability of organizations to appropriately coordinate their management and strategic plans relative to these existing and potential assets.

While HIPAA-covered entities and business associates have long worked within the environment of health data privacy and security protections, identifying all possible digital health options, assessing them in the context of existing digital health tools and IT infrastructure, and integrating them into workforce workflow goes well beyond this privacy experience base. Rather, organizations will need to design and implement "digital governance" structures that build upon this privacy and security commitment, but include additional components and organizational stakeholders, in order to meet the business and strategic demands of the digital health revolution. This diversified portfolio of perspectives would include health information management personnel, risk management, communications/public relations, legal, business and reimbursement experts, and other strategic personnel.

Digital governance, then, contemplates at least three concepts. First, the data obtained, generated, and/or maintained by the company is an asset (the value of which may be apparent or subject to development) that requires an appropriate infrastructure. Second, data and analytics are not enough—the data and analytics must operate in a coordinated matter to create actionable, end-to-end process changes, using digital health tools, operational changes, culture shifts, incentives, and other process improvements, to measurably improve outcomes. Third, vetting and implementing digital health solutions is not only integral to the fiscal health of the enterprise but requires a comprehensive, retooled approach distinct from past purchasing processes.

There must be a strategy, in other words, implemented by integrated tactics. For example, such an integrated strategy would draw insight from an institution's data governance and information governance initiatives. AHIMA's Information Governance Principles for Healthcare describe data governance as the process to ensure the availability, usability, integrity, and security of the data held by an organization and describe information governance as the organization's framework to safeguard and harness information across its lifecycle and to ensure that the organization's strategy, operations, regulatory, legal, risk, and environmental requirements are met.

Any effective approach must be proactive and comprehensive on the front end to avoid costly unwinds of problematic systems. Further, the approach needs to be comprehensive, recognizing that various departments may need to be involved in an appropriate review and integration planning for potential digital health tools. At the same time, these systems have to be efficient themselves in order to effectively address the issues and not burden an organization with excess layers of bureaucracy.

Coordination across Disciplines and Business Units

Achieving this goal is no easy task and requires an organizational commitment to a clear mission.

As noted above, effective digital health governance requires recognition of the new digital dynamic in which healthcare organizations operate. Because digital health tools typically interact with enterprise-wide IT and data infrastructure, and often support mission-critical functions such as clinical operations and quality monitoring, licensing a lemon can have ripple effects far beyond the financial consequences of a poor SaaS decision. The digital governance process must have the authority and clarity of purpose to be understood within the entirety of the organizational structure as a key strategic priority for the company, not as a bureaucratic hurdle placed in front of the purchasing team. A set of clear goals and an established mission and scope help to establish this governance structure as an extension of the strategic priorities of the organization's leadership.

Digital governance looks at the adoption and deployment of digital health solutions across an enterprise. Even when a digital health solution or other data-driven activity will principally impact a particular clinical area, department, or function, the decision still impacts other stakeholders. Adoption of a new technology, for example, may require system configurations that could complicate or facilitate digital health adoptions elsewhere in the enterprise. Or, alternatively, an enterprise may have an existing contract with a vendor for one purpose in area A of the business but that vendor offers a competitor product for area B; but area B has been approached by a different vendor.

Of course, enterprises make informed purchasing decisions every day. But coordinated digital health decision making presents new twists because of the need for end-to-end data and analytics integration with actionable solutions and to coordinate with overall data and information governance ongoing efforts. For example, different digital health solutions may generate and/or digest different data, cleanse and curate that data differently, and generate different insights. Without an overarching, comprehensive strategy, this can result in missed and mixed directives. In addition, the solutions may be different but the covered entity or business associate needs to protect its health data to a consistent standard. Solution vulnerabilities not only impact the particular business line but the IT system broadly. In addition, purchasers need to consider interoperability challenges and the ability of potential solutions to integrate well with existing system platforms plus future solutions.

Further, many digital health solutions are not subject to US Food and Drug Administration (FDA) oversight. Standard provider purchasing involves FDA-regulated products with the built-in safeguards that FDA review of safety and effectiveness provide. Without FDA review, developers will decide for themselves how to validate their products and corresponding commercial claims. Savvy purchasers need to look under the hood and establish consistent vetting standards that:

- Ask for research-quality evidence to support claims
- Provide reassurance that any research involving individuals, including just identifiable data, was conducted in accordance with laws and norms applicable to research involving human subjects

Although there are different possible structures for digital governance, some of which are described below, a common critical feature is that the governance is informed by diverse compliance and business stakeholders. Digital governance is not privacy and security under a new name. It is an integrated approach that looks at financial, compliance, legal, technological and strategic objectives and considerations in making digital health decisions. Representatives from these disciplines should be included, alongside clinical colleagues.

Possible Structures

There is no one necessary structure for a successful digital governance process. The right structure will take into account the size, complexity, and business plan of the entity, as well as its own particular culture. In thinking about a digital governance strategy, entities may want to consider the following possible approaches (which may be implemented alone or together):

Single leader (DH coordinator) supported by ad hoc staff

For an organization that may have fewer digital health governance demands and a need to pull together different stakeholders for different assessment but only as needed, a single leader with ad hoc staff and support may be the right scale. Technical expertise, while helpful, may not be necessary for the individual filling this role; rather, excellent management skills, the ability to garner both individual and institutional support, and a dedication to the effort may be the most important attributes of this individual.

The advantages with this approach may include:

- Single coordinator may result in stronger sense of responsibility and create clear path of accountability
- Streamlined process can result in rapid decision making
- Departments remained unburdened by additional "committee" assignments

The disadvantages with this approach may include:

- Potential for lack of interest/development of expertise within different operating divisions
- Increased likelihood of an issue being missed by a single coordinator
- Lost opportunity for cross-learning among departments

Digital Health committee

For an organization whose size, internal politics, and/or complexity suggest that digital health evaluation and implementation issues will be under consideration on a regular basis and will touch on the portfolio of diverse stakeholders, a standing committee may be best. At a minimum, committee members should represent those who will deploy digital health solutions in operations. Regardless, the combination of committee members and support staff should represent as many stakeholders as reasonably possible and should be capable of providing strategic, operational, technical, and legal perspectives.

The advantages with this approach may include:

- Increased likelihood that cross-department collaboration and learning will improve digital health literacy across the organization
- Comprehensive "issue spotting" and "issue resolution" will occur with every opportunity under consideration
- Increased cross-departmental awareness of organizational needs

The disadvantages with this approach may include:

- Potential for slower decision-making and difficulty getting to "yes"
- Potential for diminished commitment if committee structure proves slow or burdensome
- Shared responsibility may reduce sense of individual responsibility

Board subcommittee oversight

For organizations not ready to commit to actively managing digital health opportunities from a system perspective, or wishing to exercise more significant board oversight of digital health opportunities and initiatives, a board subcommittee may be appropriate.

The advantages with this approach may include:

- Board subcommittee oversight can ensure appropriate board-level attention and focus
- Board-level education regarding digital health matters becomes easier

The disadvantages with this approach may include:

- Without an operating or management structure in support, the board subcommittee may have incomplete or imperfect information
- Without active management by a dedicated team, subcommittee directives may not be as effectively carried out

Roll-Out

Digital governance may come with some growing pains for an organization as it necessarily brings into closer coordination departments that may have historically operated somewhat independently from one another, perhaps even by design. Since digital governance may be new for the participants and the organization, a thoughtful roll-out and implementation process is key. In designing your roll-out process, you may want to consider including these staples for success:

1. Clear and concise charter, policies, and procedures that take into account the complimentary responsibilities of existing business and compliance committees and departments.
2. Education of team, senior leadership, and the board.
3. Thorough and system-wide education, together with the setting of clear expectations regarding cooperation and collaboration.
4. Recognition that evolution of the structure may be appropriate over time.

Digital health solutions may be introduced to individual physicians, clinical service line administrators, information technology staff, or any of a vast number of additional access points to a health system. In many instances the complicating results of adoption may not be readily apparent to the touch point within the system, complicating the efforts of health information management stakeholders. Adoption of a simple telemedicine program to expand behavioral health capabilities, for example, may utilize systems that are incompatible with the existing IT platform and make the protection of highly sensitive information more complicated. Worse, a seemingly simple digital health solution could result in nuanced compliance risk not recognized by the adopter. Multiple digital health solutions running in multiple locations within a system can create dramatic inefficiencies and, importantly, lost opportunities if interoperability issues are not addressed on the front end or the solution does not adhere to the organization's strategic direction. A digital governance program can recentralize important data-driven and solution-drive decision making, concentrate responsibility, and accelerate expertise building, avoid false starts, and result in consistent standards that vendors hoping to partner with you, and your own team members, need to meet.

Jennifer S. Geetter and Dale C. Van Demark, partners in the health law practice at international law firm McDermott Will & Emery, counsel clients on a wide range of issues related to the development and use of digital technology in healthcare delivery.

Original source:
Geetter, Jennifer S; Van Demark, Dale C. "Digital Health Governance: Management and Strategy for the 21st Century Digital Economy" (Journal of AHIMA website), August 01, 2017.

Driving the Power of Knowledge