COLLABORATIVE TRANSFORMATION

FOCUS ON INNOVATION CENTERS

AVOIDING PITFALLS IN DATA-FOCUSED COLLABORATIONS, VENTURES AND INVESTMENTS

AUTHORED BY JIAYAN CHEN & ED ZACHARIAS

There are myriad opportunities for hospitals and health systems (HHSs) to engage in data-focused collaborations with other stakeholders in the healthcare industry. These collaborations include, to an increasing extent, digital health and technology companies both big and small.

While in certain arrangements the primary role of the HHS is to contribute patient data, this is not the only—or even the most common—role that an HHS can play. Physicians, researchers, data scientists and other entrepreneurial players within an HHS bring valuable expertise and ideas for how data can be leveraged to drive innovation and quality in healthcare. This expertise can fuel research collaborations and joint ventures to develop new tools or products, or investments in start-up digital health companies that harness data to produce insights, analytics, or other solutions or services.

As both users and contributors of data in these endeavors, and because they are often on the front line for patients who have questions about the use of their data, HHSs must navigate multi-dimensional compliance issues and other legal factors. Outlined below are key considerations for HHSs as they contemplate potential data-focused collaborations and other relationships.

McDermott
Will & Emery

RESEARCH PATHWAYS

In the healthcare industry, there can be a misconception that use of data to develop software or other technologies does not constitute a "research" use of data. Where the data in question is protected health information (PHI) under HIPAA, or is otherwise personally identifiable information (PII) subject to other applicable federal, state or multinational privacy laws, this misconception has the potential to create material compliance risk. Whether the HHS is contributing data for such purposes or is itself using data to develop or refine digital health solutions, it should analyze each project to determine whether the activity constitutes research that is subject to any of these laws, and confirm that a pathway appropriate for research is implemented for the use or disclosure of any PHI or PII.

PUBLIC RELATIONS

Beyond the purely legal dimensions of a proposed data strategy or arrangement, an HHS should evaluate how the activity could be perceived to anticipate and manage any potential reputational risks or challenges. There are many examples of organizations facing significant public scrutiny for using or disclosing personal data despite having a legally compliant pathway for the activity.

In data collaboration arrangements, consider negotiating contractual language that:

- Gives the HHS significant control over publicity
- Includes proscriptive provisions regarding the use of the HHS's marks
- Allows the HHS to suspend data access or transmission in certain circumstances
- Provides flexibility with respect to termination

However, even the most HHS-favorable agreement may not insulate the HHS from meaningful reputational harm that could result from a venture or collaboration that is perceived to lack a solid foundation for protecting the privacy and security of the data used, or to be motivated primarily by commercial interests.

PRIVACY AND FRAUD AND ABUSE LAWS

The HHS should ensure that any data arrangement complies with HIPAA's requirements related to permitted uses and disclosures of PHI (and any applicable state law corollaries for PII). Arrangements must be carefully structured so as not to fall within the restrictions under HIPAA, state privacy laws or other applicable laws regarding the sale of PHI or PII. Note that "remuneration" for purposes of the HIPAA Privacy Rule's sale of PHI provisions includes nonfinancial as well as financial benefits. This may create complexities where an arrangement involves the provision of services by the entity receiving PHI from the HHS. The value that each party receives under the arrangement should be thoroughly assessed to mitigate any risk that the arrangement could be determined to involve a sale of PHI that would require authorization under HIPAA or consent under state or other applicable law.

While traditional HIPAA use and disclosure considerations are familiar to HHSs, relationships with start-up digital health companies in the current healthcare industry may also require familiarity with privacy and security laws that are beyond those that the HHS typically navigates. For example, health or wellness solutions marketed directly to consumers rather than to healthcare providers or health plans are primarily under the jurisdiction of the Federal Trade Commission and state consumer protection offices, attorneys general and other regulators with respect to the collection, use and disclosure of PII. Arrangements therefore should be nimble enough to adapt and best position the HHS for future compliance as information privacy and cybersecurity laws continue to evolve at the state and federal levels.

Where the HHS is a potential referral source for the collaborator, the parties should assess whether the arrangement creates any risks under anti-kickback, patient inducement, or other fraud and abuse laws that should be mitigated through a valuation or other steps.

EXCLUSIVITY RIGHTS

Carefully consider the scope of any data exclusivity that the HHS is willing to grant in a collaboration or joint venture, and any exceptions to a grant of exclusivity that the HHS may need to preserve. Precision and clarity in drafting these contractual provisions is critical to limiting or avoiding the risk of being precluded from using the data in ways that dovetail with key dimensions of the HHS's clinical or research programs—for example, participation in industry-sponsored research or collaborations with nonprofit organizations that could result in intellectual property that can be commercialized. As collaboration arrangements are formulated, early and ongoing consultation with all potential HHS stakeholders is an important safeguard.

The HHS should also consider whether to grant exclusivity in the context of a collaboration or joint venture in assessing alignment of the proposed arrangement with HHS mission-based or organizational principles. At a more fundamental level, the HHS should determine whether it is amenable to exclusivity with respect to a particular data set or repository of biospecimens (from which genomic data may be obtained). This determination may involve weighing the potential benefits that may arise from the arrangement, such as enhanced likelihood of discovering important biomedical insights or developing breakthrough solutions or products, against the potential disadvantage of precluding all other uses of the data during the exclusivity period. The HHS may also wish to consider whether exclusivity would align with any ethical or other commitments it has made regarding open access to data for research, and how its patient population or community may perceive such exclusivity.

ALIGNMENT OF COLLABORATOR INTERESTS

The HHS should be aware in a collaboration or joint venture arrangement that its mission and regulatory obligations might differ significantly from those of its partner, especially if that collaborator views the opportunity as purely commercial. Awareness of and sensitivity to these considerations can vary widely based on the partner's experience, size and business maturity. The HHS should seek partners that are willing to acknowledge, invest in and support the HHS's compliance obligations, even if the partner itself is not directly subject to regulation.

DUE DILIGENCE

The HHS should assess the appropriate level of due diligence to conduct on digital health partners. The scope of diligence will be influenced by the applicable privacy, cybersecurity and other regulatory schemes. Due diligence considerations may include, but are not limited to, the following:

- Ensuring (where applicable) that the partner has implemented a robust HIPAA compliance program that includes written policies and procedures, workforce training, allocation of responsibility for privacy and cybersecurity functions, etc.
- Devoting sufficient resources to maintaining a robust internal data governance program, including regular and tailored training, clear disciplinary measures for violations, and robust processes for overseeing vendors that process data on the company's behalf
- Deploying security measures that are reasonable and proportionate to the amount and sensitivity of the data being collected, as well as the size and nature of the company, including regular security risk assessments and role-based access controls
- Ensuring that the HHS has a clear understanding of how the data will be received, processed, stored and disclosed by the company (*e.g.*, a data map)
- Limiting access rights for users to the minimum permissions they need to perform their work (*i.e.*, the principle of least privileged)
- For consumer-facing technologies, having a readily accessible, clear and concise privacy policy regarding how the company maintains, uses and discloses user data, and regularly reviewing the policy and communicating updates to users
- For consumer facing technologies, to the extent necessary or appropriate, obtaining consent for the use and disclosure of user information in a manner that requires clear, affirmative action by the user
- For consumer facing technologies, to the extent necessary or appropriate, providing easily accessible mechanisms for users to exercise their rights with respect to their data, such as any opt-out or opt-in preferences or the right to access or delete their data

CONCLUSION

HHSs are at the forefront of the digital health frontier, leveraging data to create technologies that improve care, empower patients and advance important research. An HHS's ability to successfully take advantage of this opportunity largely depends on how it anticipates and manages the various legal, regulatory and business considerations involved in digital health collaborations. Adopting a holistic approach that addresses these items during the project planning and development cycle can head off unwanted surprises and set the project up for long-term success.

McDermott Will & Emery