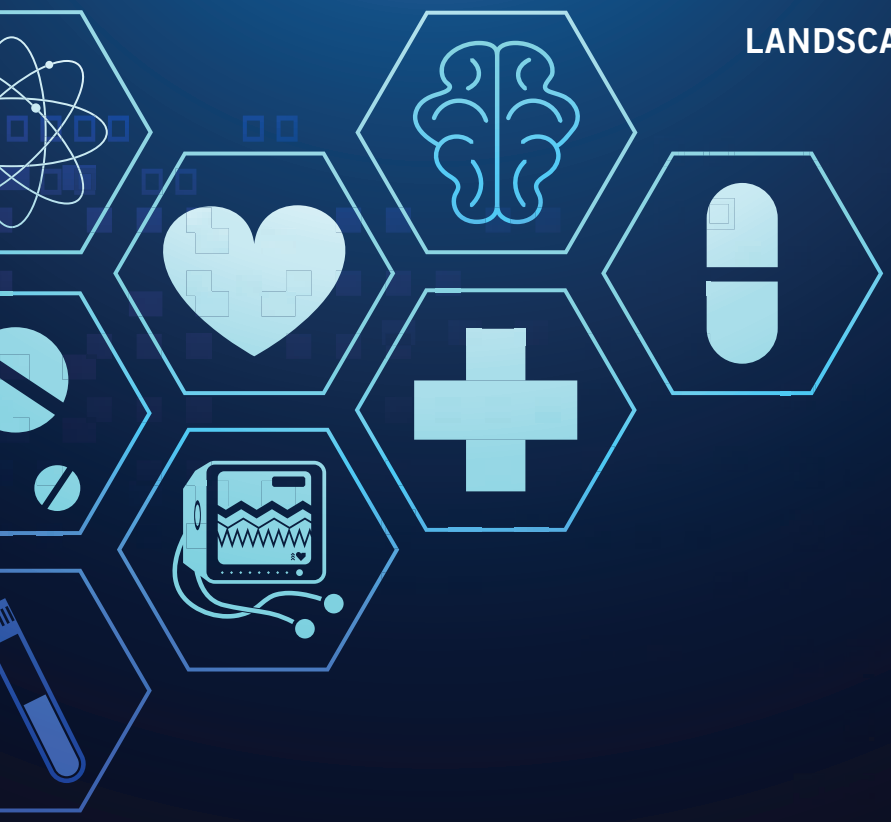
FROM INNOVATION TO SOLUTIONS

BUILDING STRATEGIC PARTNERSHIPS IN AN EVOLVING DIGITAL HEALTH LANDSCAPE



ROPES & GRAY

ROPES & GRAY

Contents

Introduction

The health care industry stands at a technology crossroads. Digital health companies hope to sell new tech solutions to providers, payors and life sciences companies, but those customers harbor some doubts about both the effectiveness of those solutions and whether they return value and preserve brand loyalty. Life sciences companies have embraced artificial intelligence as a way to streamline drug development, but this new process involves complex patient consent, privacy, and security issues, among other legal restrictions. Gray areas abound, and when something goes awry, reputations are at stake. Partnerships already have triggered lawsuits, settlements and negative press for digital health companies and their customers. Where the surveillance economy and health care intersect, can the two coexist?

Against this background of uncertainty, the law firm Ropes & Gray LLP partnered with Crain's Custom Studio to explore industry views about digital health. Through a survey, interviews with experts and this white paper analysis, we focused on partnership formation with digital health vendors. These transactions require extensive vetting because of legal issues involved, including patient privacy, data use and intellectual property issues.

Such deals also are becoming more commonplace. Digital health companies increasingly are forming alliances with providers, payors and other life sciences companies in an effort to push the boundaries of medicine. There were two examples in September alone. The Mayo Clinic announced a new partnership with Google to expand the health system's use of AI by storing its clinical data in Google's cloud. As part of the deal, Mayo will explore research opportunities to share de-identified patient data with Google or other entities. As well, Microsoft and AstraZeneca announced their joint launch of the AI Factory for Health, a European accelerator for digital health startups focused on AI. The co-innovation lab is meant to link startups, researchers and industry players, another sign of more inter-sector cooperation. As investors keep funding new entrants into digital health and AI, the pace of partnerships likely will accelerate.

Methodology and Demographics

In July and August 2019, Ropes & Gray and Crain's Content Studio, a division of *Crain's New York Business*, emailed a comprehensive survey to select Ropes & Gray clients and *Crain's New York Business* and *Modern Healthcare* readers from the health care, life sciences, digital health and health care investment sectors. The goal was to examine partnerships with digital health and AI companies to learn more about challenges, best practices and strategies for navigating complex strategic partnerships. This white paper presents an analysis of our findings.

Responses were received from 284 people who represented a wide range of companies and clinical settings, from startups to large companies or providers. Most (46%) were customers of digital health companies; 14% said they worked at a digital health tech vendor; 12% supported or provided services to digital health companies; and 6% were investors in digital health. Most of the survey respondents worked in health care provider settings. We supplemented the quantitative survey with qualitative information gained through telephone interviews. With the exception of Ropes & Gray attorneys, all interview responses are anonymized.

Respondent profile

CONCENTRATION BY SECTOR, TOP FIVE

27% Hospital, academic medical center or medical school

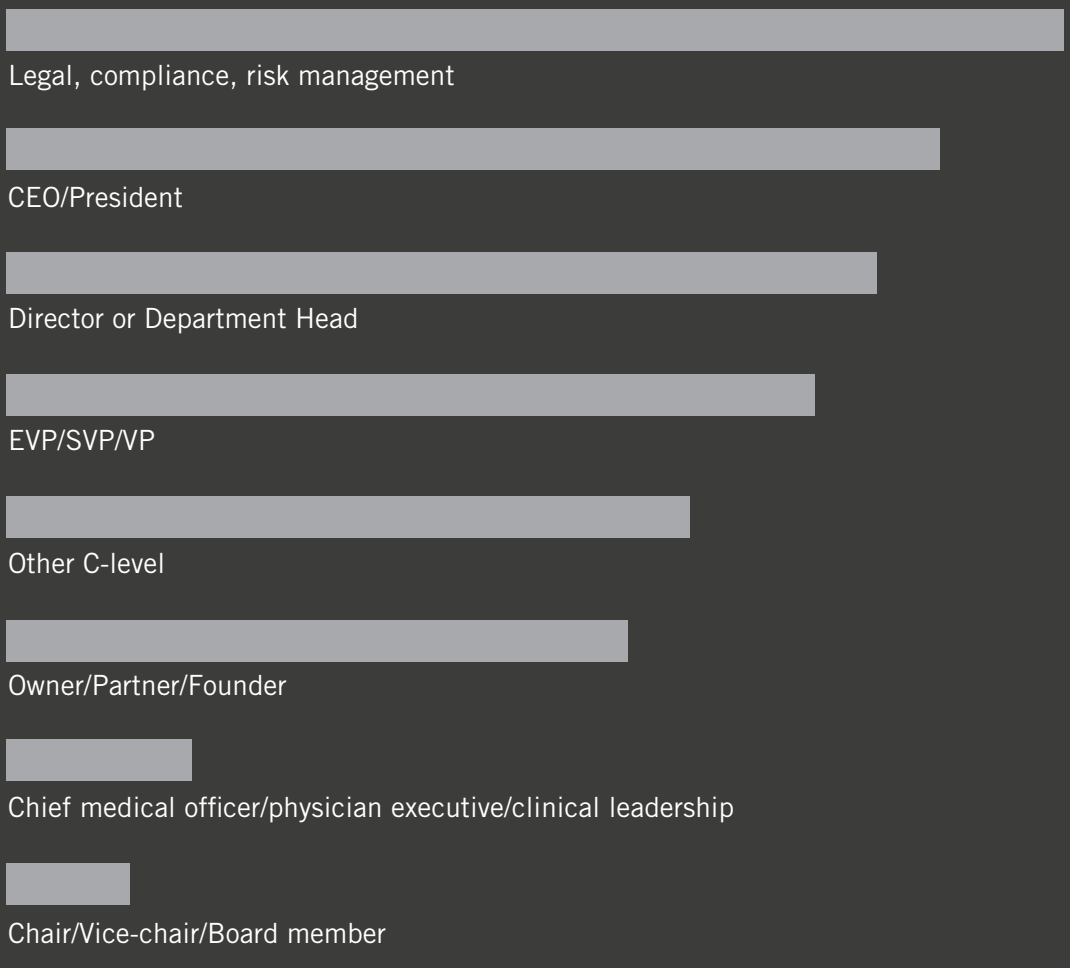
14% Pharmaceutical, life sciences or biotech companies

8% Health tech company

8% Consulting/ professional services

7% Nonprofit or foundation

MORE THAN HALF WERE SENIOR MANAGEMENT, WITH MORE THAN A QUARTER FROM THE C-SUITE



17% Legal, compliance, risk management

15% CEO/President

14% Director or Department Head

13% EVP/SVP/VP

11% Other C-level

10% Owner/Partner/Founder

3% Chief medical officer/physician executive/clinical leadership

2% Chair/Vice-chair/Board member

Key Survey Findings

"We've created a cult following around digital health. It's really cool, but is it what we really need? Should we be paying for it? Adopting it? Or are there less technical ways of solving our challenges?"

— Health care investment executive

Roadblocks to digital health

Digital health vendors offer products that don't meet market needs, and there's limited reimbursement.

60%

Health care's strongly entrenched business and reimbursement models make it difficult to bring digital health products to market

47%

Most health tech companies do not fully understand the health care market

Obstacles to pursuing digital health solutions

18%

Lack of reimbursement by insurers and payors

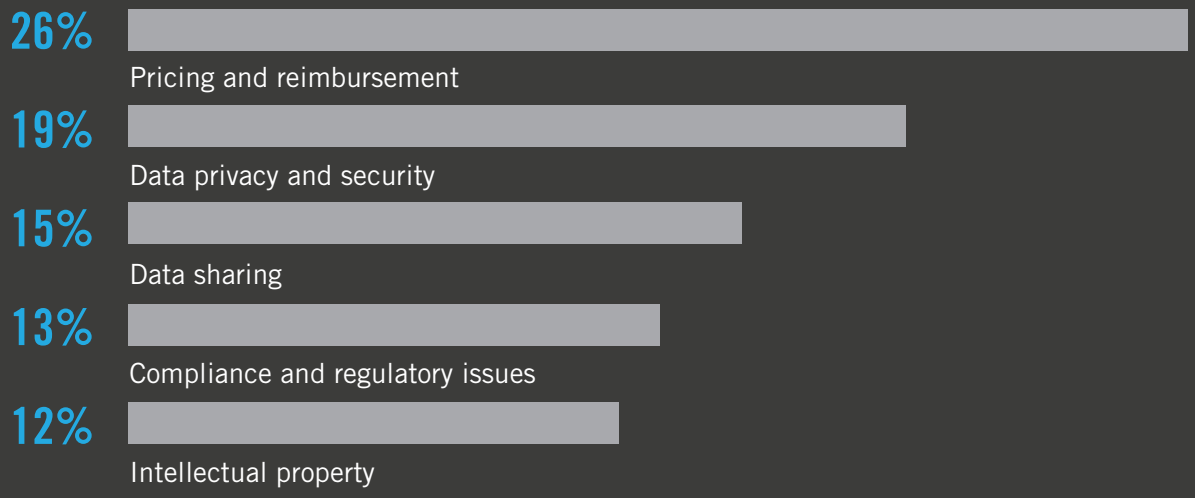
15%

Lack of expertise in digital health tech

15%

Patient privacy is mishandled in digital tech partnerships

Digital health partnerships face unique obstacles



Partnerships: Yes, no and maybe

35% Were likely or somewhat likely to have affiliation talks within the next year

29% Have either entered into a partnership or acquired a digital health company over the past year

18% Were not considering an affiliation because digital health companies do not demonstrate a value proposition

13% Were not considering an affiliation because health insurers and other payors are unlikely to pay for the product

13% Were not considering an affiliation because digital health companies have too much exposure to data privacy and cybersecurity problems

Factors influencing partnership formation

70% Said a digital health partner would fail to secure or encrypt data prior to it being shared

45% Were somewhat concerned their digital health partner would have accidental data breaches

34% Worried their digital health partner would have accidental data breaches

30% Said external attacks from cybercriminals were their organization's top cybersecurity risk

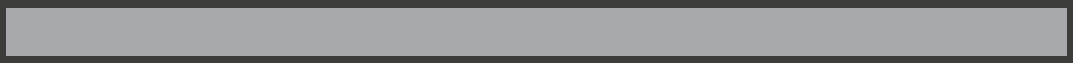
24% Cited accidental or malicious internal data breaches as their organization's top cybersecurity risk

Key Survey Findings

Health care is embracing artificial intelligence but is worried about data usage and consent

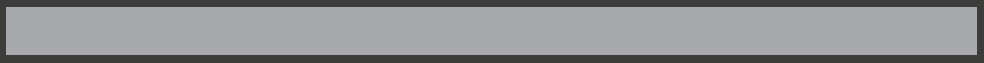
Health care sector is embracing artificial intelligence...

42%



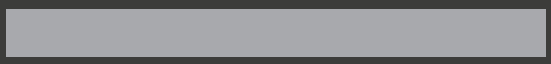
Said it was likely or somewhat likely they would partner or contract with an AI company over the next year

37%



Said it was unlikely they would partner or contract with an AI company over the next year

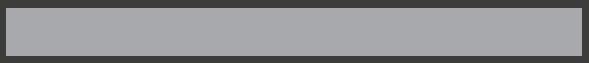
22%



Were unsure if they would partner or contract with an AI company over the next year

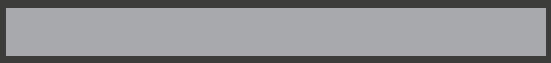
But is worried about data usage and consent

27%



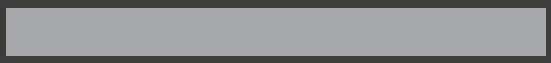
Said the problem with an AI deal is the potential lack of clear patient consent for the use of data

21%



Were concerned that a provider would share patient data without proper de-identification

21%



Said an AI company would retain patient data to create large datasets for machine learning applications

SECTION 1

Digital health's pursuit of providers and pharma

KEY TAKEAWAY: The health care sector should tackle fragmentation by cooperating with digital health companies through carefully crafted partnerships.

> "It's a very small window to collect and analyze data, refine your technology, generate shared savings, and prove outcomes before you go belly up."
>
> *—Brett Friedman, Ropes & Gray*

DIGITAL TECH ROADBLOCKS

Health care is slow to adopt new digital technologies. Providers shun technologies that interrupt their work flow without strong clinical evidence. The move to value-based models makes digital health technologies more attractive, but efficacy has not always been proven and many products are not reimbursable. That payment impasse will remain until digital health products make the shift from nice to necessary.

Providers will not purchase a product and payors will not cover it until it is proven effective, so "it's kind of a chicken-and-egg situation, and you don't have a lot of runway to demonstrate that your product works before you run out of money," said Brett Friedman, a partner in Ropes & Gray's Health Care practice and co-chair of the firm's Digital Health practice. "It's a very small window to collect and analyze data, refine your technology, generate shared savings, and prove outcomes before you go belly up. That's an enormous task when historically the health care sector moves very slowly."

And yet money continues to pour into digital health. Globally, total venture-backed digital health funding was $3.5 billion in the second quarter of 2019, up 23% over Q1'19, according to CB Insights. That cash infusion only accelerates the number of digital health vendors pursuing partnerships.

MOST IMPORTANT QUALITIES IN A DIGITAL HEALTH PRODUCT OR SERVICE

23%
Evidence of efficacy

21%
Meeting all regulatory and compliance requirements

20%
Compliance with data security and privacy standards

Survey respondents identified several obstacles to actually implementing digital health solutions: 18% blamed lack of reimbursement by insurers and other payors. Another 15% cited a lack of expertise in digital health tech, and an equal percentage was concerned that patient privacy could be mishandled in digital tech partnerships. Survey takers wrote additional comments on these obstacles:

- Lack of understanding on the part of providers
- Lack of industry familiarity with what health tech can do
- Entrenched practices and lack of vision
- Slow decision-making speed by hospitals and health plans
- Long sales cycles from health care customers
- Lack of true interconnectivity
- Complex regulatory and compliance requirements

Collectively, these results suggest that "when digital companies are going to health systems or to their potential partners, they haven't refined their thesis well enough as to why the partnership is worth it to the health system," added Friedman.

In a survey weighted toward providers, there was clear hesitancy about digital tech. "We've created a cult following around digital health," said a health care investment executive. "It's really cool, but is it what we really need? Should we be paying for it? Adopting it? Or are there less technical ways of solving our challenges?"

This diversity of opinion about digital health's utility highlights a disconnect between providers and vendors. "One of the first questions I ask digital health companies isn't even a legal one, but a practical one: What in the health care sector are you trying to fix?" said Friedman. "The second question is, 'is this something that the patient or member or consumer will appreciate?' The digital health products that work best try to solve real problems. That's even more basic than reimbursement or legal issues."

IS DIGITAL HEALTH WORTH IT?

47%
Agree

24%
Disagree

Most digital health tech companies do not fully understand the market in which they are designed to operate

55%
Disagree

27%
Agree

Most digital health tech products aren't useful to patients, physicians and caregivers because they do not address actual problems that need solving, or don't demonstrate cost savings and quality improvements

> "If they think the whole game of digital health is just to bang out apps, and evidence and validation be damned, they are missing the point of the sector they are trying to impact."
>
> *—Pharma executive*

We identified several hurdles that digital tech vendors face in selling to the health care sector. As one health care investment executive explained, "tech companies do not have a single point of entry for breaking into a large academic medical center. They may end up selling to a single service line or clinical department, and that leads to fragmentation."

"The health system doesn't have a clear enterprise-wide digital health strategy, and that creates a real strain," he added. "There are different digital health solutions selected for different providers. So you can have a variety of medication adherence solutions, for example, one for cardiac patients, and another for GI patients."

One executive from a provider network shared an anecdote that illustrates clinicians' skepticism about digital health. A vendor with an AI solution went to a health institution to propose a partnership. Its business model was not based on solving a problem for providers. Instead, the vendor planned to make money by "packaging the data to sell to pharma. It was just a data play."

WHAT DIGITAL HEALTH CUSTOMERS VALUE MOST

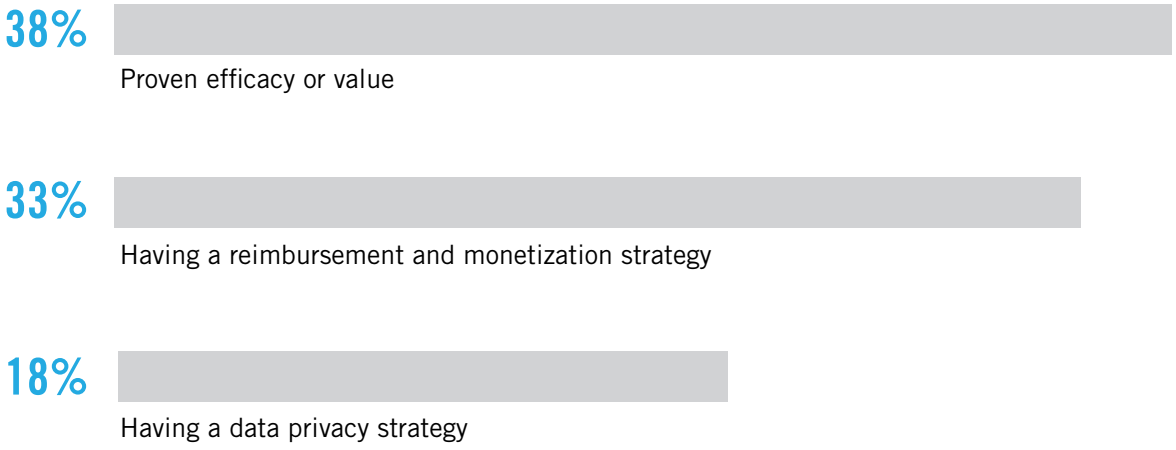
The most important qualities they look for in a digital health product or service

While just under 40% of digital health vendors said efficacy or value is very important, many struggle to validate efficacy. In the name of innovation, the health care sector might consider tackling the efficacy gap by increasing cooperation with digital health vendors through carefully crafted partnerships. In the words of the CEO of a digital health company:

"I wish leaders in non-digital health care would recognize the part of the equation they must provide. There's a ton of brainpower and energy and money thrown into digital health, but it needs cooperation. It would speed up production tremendously if there were a formal 'innovation sandbox' where digital health provides innovation, and providers bring access to patients, end-users and data. I'd love a very substantial effort to have some sort of sandbox, because even with piloting, every pilot is separate from another. I'm calling for cooperation."

WHAT DIGITAL HEALTH COMPANIES THINK THEIR CUSTOMERS WANT

The most important factors in developing a product to bring to market



BRINGING DIGITAL HEALTH PRODUCTS TO MARKET IS VERY CHALLENGING BECAUSE OF HEALTH CARE'S STRONGLY ENTRENCHED BUSINESS AND REIMBURSEMENT MODELS

DIGITAL TECH AND PHARMA

> "The FDA wasn't speaking the same language as a tech culture that is used to putting products out there, seeing how they work, and adjusting afterwards."
>
> *—Al Cacozza, Ropes & Gray*

Tech and life science companies are encroaching on one another's territory. Life science companies are involved in AI and machine learning. Technology companies have embraced digital therapeutics. Both sectors face obstacles.

Tech companies have "a huge learning curve in getting up to speed on the science and learning the ropes regarding HIPAA, human subjects research, clinical trials, the FDA, insurance and other subjects relevant to health care providers," said Megan Baca, a partner in Ropes & Gray's Intellectual Property Transactions practice and co-chair of the firm's Digital Health practice.

Four out of 10 survey respondents think that the FDA's new pre-certification program for software will slow down the time frame for bringing novel products to market. More than half think companies must invest a lot of time and money to satisfy FDA requirements. Nearly 25% think that the FDA's biggest challenge is the struggle to regulate innovative digital health applications, products and services.

Those survey findings highlight one of the fundamental differences between tech and pharma cultures. One pharma executive describes an illuminating thread that started on Twitter:

"Several digital health entrepreneurs wrote they don't need clinical trials to generate evidence for their tools or apps; of course they worked. In fact, they felt it wouldn't be fair to do a clinical trial because that would be denying the control group access to their digital solutions. It is a mindset that belies the fact that we rely on evidence, which this FDA framework gives. Ultimately, digital health companies need this FDA validation to survive."

"If they think the whole game of digital health is just to bang out apps, and evidence and validation be damned, they are missing the point of the sector they are trying to impact," he added.

The tech/pharma culture divide is nothing new. As Al Cacozza, a Ropes & Gray partner in the Life Sciences Regulatory and Compliance practice and co-chair of its Digital Health practice notes, "Years ago I'd talk to developers who come from a tech culture that is hostile to regulation, while the FDA comes from public health and benefit risk approach. The FDA wasn't speaking the same language as a tech culture that is used to putting products out there, seeing how they work, and adjusting afterwards."

Cacozza expressed surprise that 40% of survey takers thought the FDA pre-certification program stifled innovation. "It effectively pre-qualifies manufacturers and was intended to expedite and streamline rather than hinder. Yes, it's more onerous than classic Silicon Valley 'let's do various versions and keep improving them,' but from the FDA's point of view, this is progress."

A chief executive of an AI health company, who spent years in Silicon Valley, acknowledged the "anti-regulatory sentiment that runs through all these tech companies. The fact is the regulations are there and you have to abide by them. You have additional obligations within health care. To be honest, those FDA regulations are written very well and are very flexible."

SECTION 2

A deeper dive into digital health partnerships

KEY TAKEAWAY: These complex partnerships require extensive vetting and careful language because of patient privacy, data ownership and intellectual property issues.

> "Data is a slippery form of intellectual property—in some ways it resembles a copyright or a trade secret, but it is not protected by one specific form of intellectual property rights."
>
> *—Megan Baca, Ropes & Gray*

While interest in partnerships is growing, 71% of our survey respondents said that within the past year they had not entered into a formal joint venture or partnership with, or acquired, a digital health company. The remaining 29% had done deals, the majority of them (58%) with a digital health vendor.

People who were not considering partnerships offered several reasons for inaction: Digital health companies did not demonstrate a value proposition (18%); too much exposure to data privacy or cybersecurity problems (13%); insurers were unlikely to provide reimbursement for the product (13%). For this group, cost is an issue, and they are unsure whether digital health is worth it.

WHAT SPECIFIC ISSUES IMPEDE PARTNERSHIP NEGOTIATIONS?

14% Measures to protect intellectual property rights within the partnership

14% Issues related to data privacy and direct liability of business associates under HIPAA

14% Negotiating downstream data use limitations

12% Performance or delivery milestones

12% Developing governance programs to protect data assets and IP

PARTNERSHIPS: WHAT CAN GO WRONG

> "I'm always surprised when we're doing transactions or due diligence on companies at the lack of clarity about how data is to be used and disclosed."
>
> *—Deborah Gersh, Ropes & Gray*

Intellectual property is a particularly thorny issue in a collaboration. "Data is a slippery form of intellectual property—in some ways it resembles a copyright or a trade secret, but it is not protected by one specific form of intellectual property rights," said Ropes & Gray's Megan Baca.

Data sharing agreements can be a partnership's downfall, she added. "Fundamentally, intellectual property and data are really at the heart of any health tech partnership. Reaching an agreement on intellectual property and data rights is critical to moving ahead with any partnership."

We hoped to get a more complete picture of the pitfalls that can befall partnerships. Among the issues cited were pricing and reimbursement (26%), followed by data privacy and security (19%) and data sharing (15%).

"I'm always surprised when we're doing transactions or due diligence on companies at the lack of clarity about how data is to be used and disclosed," said Deborah Gersh, co-chair of Ropes & Gray's Health Care practice and co-leader of its Health Care and Life Sciences Industry Group. "We often see boilerplate language in HIPAA business associate agreements that leaves it unclear how that data can be used, and in what form."

Gersh said that business associates may be given the right to de-identify and aggregate data, "but the agreement does not address the possible uses of this data on a granular level. It is almost as if there is a fear of addressing the issue." In contrast, she noted, payors often have very restrictive language. "They'll specify you can't use their data in any way, shape or form."

That attitude reflects the importance of data to a partnership's success. "Data are valuable but also unpredictable," warns Baca. "Companies don't always know how to think about data as an asset in transactions, or about their options for how to monetize big data in their business plan."

Another potential trouble spot, she added, is "the unpredictability of what actually comes out of a collaboration. There might be data that no one thought would be interesting or valuable, and so no one planned for it in advance. You can end up in a situation where both parties think they deserve the right to exploit that data."

TOP CHALLENGE TO PROTECTING INTELLECTUAL PROPERTY IN STRATEGIC PARTNERSHIPS OR VENDOR RELATIONSHIPS

37%

Failure to create data sharing agreements that spelled out who owns the data and how data is shared

25%

Failure to create a plan that spells out what intellectual property is included or excluded

Intellectual property was also cited as one of the most difficult issues to resolve during partnership negotiations. In the words of the CEO of an AI health company, "Usage is the key question. What can you do with this data, compared to what are you forbidden from doing? For the most part, these are relatively straightforward questions. But they can be contentious, as there's a lot of value associated with the data."

SECTION 3

Partnerships: Data security, privacy and patient consent

KEY TAKEAWAY: Patient data privacy and proper consent are among the most challenging aspects of digital health.

> "People have difficulty understanding many privacy notices or authorizations. The paradigm needs to shift."
>
> —*Edward McNicholas, Ropes & Gray*

DATA SECURITY

Nearly 70% of respondents were concerned that a digital health partner would fail to secure or encrypt data prior to it being shared. Nearly 80% worried their partner will have accidental data breaches.

An executive with a disease–research foundation, for example, said the nonprofit "has processes in place to make sure we are following best practices. We consult with privacy counsel or chief legal officers to ensure that things are done in an appropriate manner. We engage penetration testers who come in and try to break firewalls. We require a sign-off on a security assessment."

Still, this executive worries about breaches, describing the experience of working with a leading customer relationship management software company that had limited experience with health care platforms. It took much hand-holding "to work with them to abide by HIPAA technical guidelines to encrypt our data, and to work with a consulting company to build out the encryption aspect of the software. As a foundation, we are experts in the digital arena and we're experts at HIPAA. It was nerve-wracking in the sense if there was a breach, what would that do to our reputation?"

Breaches are persistently a strict liability event from a public relations perspective. If there is a successful breach, few think that their preparations will be an adequate protection.

TOP CYBERSECURITY RISKS

30%

External attacks from cybercriminals

24%

Accidental or malicious internal data breaches

21%

Compliance with such regulations as HIPAA, General Data Protection Regulation (GDPR) and the Telephone Consumer Protection Act

Partners should be comfortable with how data will be stored and processed, so there isn't exposure to unnecessary risk. But 72% of survey respondents are concerned their digital health partner would use their data beyond its business associate or legal/contractual obligations. While 37% of organizations permitted their digital health partners to aggregate and analyze their data, 18% did not, and 46% were unsure. Just under 70% said they always, or to a large extent, restricted downstream use of data.

Data protection concerns are one reason why life science companies hesitate about partnering with digital health entrepreneurs. There is a very high bar for tech companies to overcome, because pharma must protect its reputation, said one pharma executive. "For digital solutions, or even simple things like mobile apps and websites, in the past, differentiation was based on personalization or other interesting flavors. Going forward, privacy and security will be the real differentiators for companies in the market."

DATA PRIVACY AND PATIENT CONSENT

With patient data privacy and proper consent, when things go wrong, they make headlines, damage reputations and trigger lawsuits. In June 2019, for example, a lawsuit about patient privacy was filed against Google and a large academic medical center. It accused the health system of giving Google records for hundreds of thousands of patients that had identifiable date stamps or doctor's notes.

"People want to believe in de-identified data, but in the era of big data, especially with health data, it's a fallacy. We can't rely on de-identification, period. Aggregated, de-identified data can be used in a thousand ways, so you have to assume that all data can be re-identified," said the pharma executive. "And if you believe that all data can be re-identified, then what proper permissions and controls should be in place? I, for one, think de-identification is a myth."

Edward McNicholas, co-chair of Ropes & Gray's Data, Privacy, and Cybersecurity practice, acknowledged a potential fear over "never being quite sure that something is completely anonymized. It is important not to restrict the science, but to address re-identification. HIPAA has a notion of a limited data set, which can be helpful, but we need to address de-identification directly."

In general, digital health companies must contend with "people's limited understanding of informed consent, which for years was the bedrock of any privacy regime," added McNicholas. "It is very difficult for people to understand some privacy notices or authorizations. That paradigm needs to shift at some point. A replacement would be very interesting. It might be something like regulation that restricts the use of data outright."

What happens when patients want to pull consent? The right to be forgotten, said Ropes & Gray's Deborah Gersh, "is very difficult to do if the data has been integrated. People think their information sits in a silo and they can just delete it. There's a lot of discussion about what that means."

The issue of patient data privacy currently is pitting federal regulators who are working on medical information-sharing rules against groups that include the American Medical Association. At issue are proposed federal rules to let patients use third-party consumer apps to retrieve their medical records. Providers would be required to send medical information to apps after a patient authorizes the data exchange. HIPAA protections no longer apply when a patient transfers that data. Condemning the new rules, provider groups argue that consumer apps could then share or sell sensitive medical data such as prescription history.

"Because HIPAA only regulates identifiable data, things are happening where I'm sure patients have no clue about how their data is being used," said the executive with a disease-research foundation. The nonprofit's consent form, for example, explains to patients what will happen to their data. Restrictions also are clear in contracts with researchers, said the executive:

"When you are a foundation, you fund things, so who owns what is key. In order to get our data, we have patient consent, but we also sign contracts with different institutions that are providing data, including from an electronic health record. We make it explicit we are allowed to own the data. We also have rules in place so that we don't release any identified data, and that when

data is released researchers can't use it for marketing purposes, to identify prescribing patterns, or to sell. It's very clear what other researchers can and can't do with this data. When the partnership ends, they have to destroy all our data."

Transparency about how data will be used is crucial for the spread of digital health initiatives. Consumer trust is key, and at some point we may need to reassess our assumptions about permissions and authorization to use data, believes the pharma executive. He offers the example of real-world evidence that is part of regulatory submissions:

"In many cases, patients have no idea their data is being used in this way. It is legal and permissible. And yet something feels wrong when the largest companies in the world are using their patient data in this way, and patients have no idea it's even happening. Do we engage patients and make them aware of how their data is actually being used?"

Digital health companies acknowledge this delicate balance. "The issue of data ownership and consent is very tricky and thorny," said the CEO of an AI health company. "There isn't a single, clear-cut, pithy answer to how those things should be handled. Patients need some level of privacy and control over their own health care, but we also need to advance health care technology to make it better and more effective for everyone. The balance between the two is complicated."

THE ETHICS OF DATA

That dilemma leads us to the ethical considerations that swirl around privacy and consent. Increasingly, nonprofit health systems are partnering with for-profit ventures in data deals. Some hospitals hesitate to sell patient data to be used in for-profit ventures, but do so to advance science and their mission.

Digital health partnerships are complex deals that involve data use, privacy, security and intellectual property concerns. We are all consumers and patients, and our health care data triggers ethical questions. Is our data for the public good and for the advancement of medicine? Or is our data ours alone?

"There are patients who say 'nothing about me without me,' and that this data is a digitalized me, essentially their digital self," said the pharma executive. "Can we do whatever we want with their digital self just because it exists in somebody's database?"

Should patient data be for the public good, or for profit? In September, medical records giant Epic announced it would tap the 20 million patients in its system to compile a database to help improve treatment decisions. Its health system clients will contribute high-quality, standardized, de-identified data to the initiative, called Cosmos. Epic said it would develop a machine learning platform to help speed medical research based on the records. While Epic said its clients will pay a "nominal" fee to access the data, the announcement was met with questions about who else could have access, and at what price.

The overarching challenge, said Ropes & Gray's Deborah Gersh, is "balancing the privacy of the individual with the greater good. There's a fair amount of tension because that data can be used in many different ways, and we must be very thoughtful about balancing those interests."

There have been missteps by some providers "that really fail to recognize their own institutional conflicts of interests," asserts the disease-research foundation executive. "Our ethics committee is headed by a bioethicist. We recognize that we put ourselves into either real or potential conflicts of interests when we get money from industry. We feel we are partnering to advance science and our mission. But feelings are one thing, and reality is another, and so if our ethics committee says 'you can't do it that way,' they usually will come up with an alternative that emphasizes transparency and helps us manage conflicts."

PARTNERSHIPS AND ARTIFICIAL INTELLIGENCE

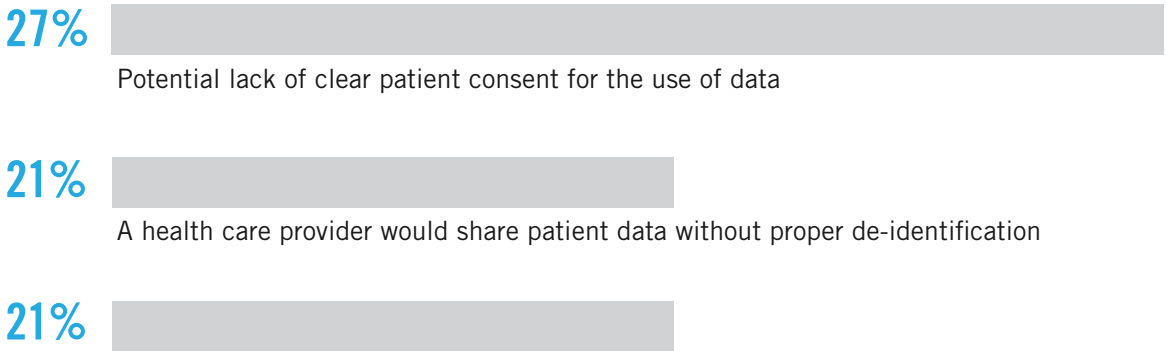
Many entities misunderstand AI, in the view of one AI health company CEO:

"AI is the use of a certain set of computational techniques in machine learning that can be adapted to many different applications. AI and machine learning already are embedded in technologies in clinical situations, but most people don't see them as AI, such as natural language processing for dictation. But the data privacy concerns are things people always point to, and they are real. AI companies all depend on data to some degree."

"When you're giving a company so much data, there's a direct risk of a breach and potential misuse of data," said Ropes & Gray's Brett Friedman. "One issue I often confront is where the recipient of the data can aggregate and monetize it. That's permissible under HIPAA because aggregated data is not identifiable data, but as a matter of corporate policy, the covered entity doesn't want these AI companies to monetize their patients' data. That's more of an ethical and moral concern than it is a legal concern under HIPAA. They are concerned they will not aggregate appropriately, and that's a real risk."

WILL YOU PARTNER OR CONTRACT WITH AN AI COMPANY OVER THE NEXT YEAR?

WHY ARE YOU CONCERNED ABOUT A PARTNERSHIP WITH AN AI COMPANY?



Conclusion

Digital health has become a catalyst for collaboration among all sectors of the health care industry—tech companies, payors, providers and life sciences. The convergence of these industries is important to the advancement of health care and population health. But not long ago, these sectors did not speak the same language and therefore rarely talked to one another about how to improve health outcomes.

All sides now recognize the enormous potential at the intersection of these sectors. Digital tech is beginning to understand the importance to providers and pharma of proving efficacy in a clinical setting, while providers are more willing to embrace digital tech. But there are still cultural differences that need to be bridged, and significant roadblocks that must be overcome.

For example, the tech industry is used to developing new products, introducing them into the marketplace and then iterating them based on experience, with an emphasis on speed of innovation and speed to market. In contrast, the life sciences sector is dependent on demonstrating safety and efficacy, through substantial clinical evidence as judged by the FDA, with its public health approach that weighs benefits against risks. The tech industry must accept that the FDA will regulate many of its digital health products. The life sciences sector and the FDA must be open to a nimbler product development path.

Regulators, of course, play a significant role in influencing convergence and digital health adoption, particularly reimbursement. Providers and tech entrepreneurs need financial incentives to encourage the adoption and use of digital health in a clinical setting. Federal regulators have been willing to move in that direction, issuing plans to reimburse providers for certain digital health tools such as remote patient monitoring and telehealth. There is more work to be done, however, and in a margin-pressured sector like health care, providers need assurance that digital health solutions will be reimbursed.

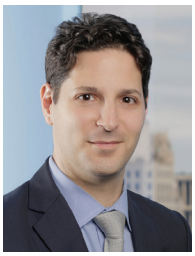
As noted in the survey results, the health care industry is grappling with this issue of how to monetize digital health innovations. Fundamentally, are they addressing real health problems by adding value? And if so, how do payors reimburse for that value? There also are complex issues around data use and intellectual property rights and lingering concern, generally from the health sector side, about data privacy and cybersecurity risks, given how much of this data may be sensitive personal health information.

We are poised to enter a new era of convergence and cooperation, where key stakeholders strive to better understand each other, the market, and these complex issues as they embrace innovation. We believe the result will be real-world benefits to patients and consumers.

Ropes & Gray Contacts

Megan Baca
megan.baca@ropesgray.com
+1 650 617 4057

Albert Cacozza
albert.cacozza@ropesgray.com
+1 202 508 4611



Brett Friedman
brett.friedman@ropesgray.com
+1 212 596 9486

Deborah Gersh
deborah.gersh@ropesgray.com
+1 312 845 1307

Edward McNicholas
edward.mcnicholas@ropesgray.com
+1 202 508 4779

About Ropes & Gray

Ropes & Gray is a preeminent global law firm with approximately 1,400 lawyers and legal professionals serving clients in major centers of business, finance, technology and government. The firm has offices in New York, Boston, Washington, D.C., Chicago, San Francisco, Silicon Valley, London, Hong Kong, Shanghai, Tokyo and Seoul, and has consistently been recognized for its leading practices in many areas, including private equity, M&A, finance, asset management, real estate, tax, antitrust, life sciences, health care, intellectual property, litigation & enforcement, privacy & cybersecurity, and business restructuring.

ropesgray.com

ROPES & GRAY