Q1 2020

WILSON SONSINI

DIGITAL HEALTH REPORT

During this unprecedented time, digital health is disrupting our healthcare delivery system for the better. Digital health companies are working hard to provide innovative telehealth, digital screening, and testing services. They are leveraging AI to assess symptoms, model outcomes, and identify possible treatments for COVID-19. Digital health companies are providing physicians and other frontline responders with new tools to fight this pandemic.

The Wilson Sonsini digital health team is here to support you during this time. Providing a cross-functional team approach for our digital health clients, we can help you:

- understand the latest regulatory changes;
- draft and enter into contracts;
- protect your ground-breaking intellectual property (IP); and
- obtain financing for your next round of innovation.

Please feel free to reach out to your Wilson Sonsini team member or a member of the digital health practice group for assistance.

In This Issue

Machine Learning Legal Issues for Digital Health Companies in Commercial Transactions..... Pages 1-4

How to Incorporate FDA into Your R&D..... Pages 5-7

Preparing for Your First Sale: How Digital Health Companies Can Plan for Healthcare Business ..... Pages 8-9

How HITRUST Can Help Get You to a Series A..... Pages 9-12

Machine Learning Legal Issues for Digital Health Companies in Commercial Transactions

By Rob Parr and Scott McKinney

With its potential to revolutionize industries and products of all types, "machine learning" (**ML**) is a hot topic. ML, a sub-category of artificial intelligence, refers to software algorithms that are programmed to analyze data, learn from that analysis, and improve themselves. ML has gained significant traction in the digital health space, with numerous digital health companies developing ML products designed to help predict, detect, and treat illness, increase the efficiency of delivering healthcare, and find solutions to other complex challenges facing health providers, payers, and patients.

Artificial intelligence technologies like ML present some unique legal challenges for digital health companies, and traditional contract approaches may not properly address intellectual property, risk allocation, data use, and other important issues that are unique to ML or artificial intelligence more generally. This article is intended to highlight for digital health companies that wish to commercialize ML-enabled technologies (**ML Providers**) five key areas in commercial contracts where we routinely help clients identify and address certain issues unique to artificial intelligence and ML.

1) **Input Data**. Input data refers to data that ML technologies process to generate a given output. ML Providers benefit from obtaining vast amounts of input data,

Continued on page 2...

Machine Learning Legal Issues . . . *(Continued from page 1)*

because the more input data ML technologies process the "smarter" those technologies become. This is especially true for ML Providers whose products focus on preventing, diagnosing, or treating medical conditions given the importance of generating accurate results. We often find that agreements do not adequately and clearly address the data provider's and data recipient's rights to input data, so ML Providers should be careful to obtain proper input data licenses or usage rights to avoid claims of intellectual property misappropriation or infringement.

(a) Negotiated Terms. ML Providers may obtain input data pursuant to negotiated contract terms, such as from their customers or other commercial data providers. In these negotiated transactions, ML Providers should consider seeking rights to modify, restructure, and reorganize input data, and to use input data, including when aggregated with other data, to enable ML Providers to train and improve their ML technologies and to create output data (further described in Section 3 below). ML Providers should also consider trying to get perpetual rights to store and use the input data because it can be difficult to track data sources and to separate individual data elements from larger data sets. ML Providers should also carefully review any confidentiality terms in their contracts with data providers to ensure those provisions do not prevent the ML Providers from storing, processing, and using the input data in the manner that they plan to. ML Providers should also consider obligating data licensors to provide input data on an aggregated and de-identified basis because that aggregated and de-identified data is more likely to be exempt from laws that govern the collection, use, disclosure, and protection of sensitive data such as personal information. This is especially important for ML Providers whose ML technologies are designed to process patient data that would be subject to the Health Insurance Portability Accountability Act of 1996 (HIPAA) unless that data is de-identified in accordance with HIPAA's specific requirements. Finally, ML Providers who obtain input data under negotiated terms should also consider trying to obtain specific representations, warranties, and covenants regarding the input data as further described in Section 4(c) below.

(b) Non-Negotiated Terms. ML Providers may also obtain input data from many different online sources under standardized, non-negotiated contractual terms. These kinds of terms typically apply to health-related, open sourced scientific or research data made available in online repositories and to data obtained from third party websites. ML Providers should exercise caution when obtaining input data in this manner. Non-negotiated data terms often allocate to the data user all risks associated with using the data and may also include specific data use terms governing what a data user can and cannot do with the data. For ML Providers whose ML products are designed to function as diagnostic or treatment tools for certain medical illnesses, assuming all risks associated with the use of source data could mean that the ML Provider is taking on significant risk. Before downloading or using data that is available under non-negotiated terms, ML Providers should carefully evaluate the corresponding data use terms to ensure that the ML Provider's intended use of the data complies with all applicable data use rights and restrictions. It is also in many ML Providers' interests to track the source(s) for input data obtained under standardized terms to evaluate potential risks associated with using the data and better enable ongoing compliance with applicable license terms.

2) **ML Technology Improvements.** Absent clear contractual terms describing each parties' rights to improvements to, changes to, and derivatives of the underlying ML technology that arise from an engagement between an ML Provider and an ML technology licensee (**Improvements**), there is legal uncertainty around who would be deemed to own those Improvements, especially when the

licensee may exert some control over the operation of the ML technology.[1] Accordingly, ML license agreements should state clearly who owns all Improvements as a contractual matter between the parties and properly effect transfer of ownership from one party to the other with appropriate contractual assignment language.

The ML Provider could start with the position that it will exclusively own Improvements. This is often the most practical approach from the ML-Provider's standpoint because Improvements may arise from an aggregation of inputs and actions that cannot be attributed solely to one party or licensee and may not be readily separable from or useful independent of the baseline ML technology. If a licensee of ML technology pushes for ownership to Improvements during a negotiation, then the ML Provider should evaluate whether to accommodate that request on a case-by-case basis, taking the relevant circumstances into account. Ultimately, the ML Provider's goal is to only cede ownership over a narrowly defined category of Improvements that in fact can be readily separated from the baseline ML technology, and to try and obtain a broad and unrestricted license back to use those Improvements in the future.

3) **Output Data**. ML technologies process input data to produce a given output. Although this output data may be protectable as intellectual property, primarily under trade secret law[2], in some cases the protection offered to ML output data by intellectual property laws and other legal doctrines is ambiguous or altogether non-existent. As a result, similar to the approach we described in Section 2 above for Improvements, ML license agreements should clearly and expressly identify who owns the output data as a contractual matter between the parties and include appropriate assignment language to effect the desired allocation of ownership rights. ML license agreements should also address any rights the non-owner obtains to use the output data. If output data is sensitive or valuable to an ML Provider, then an ML Provider who owns that output data pursuant to its ML agreement could try to grant the licensee of that output data a license to use the output data that is narrowly tailored to the licensee's needed use cases and that includes clear restrictions on use and obligations sufficient to maintain the secrecy of the output data. An ML Provider who cedes ownership of the output data also could try to obtain a broad license to use that data on a go-forward basis as described in Section 1 above.

4) **Risk Allocation**. ML Providers should also consider trying to negotiate risk allocation provisions in their license agreements to obtain certain protections for the transaction. The ultimate terms of that protection will depend on the ML technology being licensed, its intended application and the applicable deal dynamics, including the parties' respective bargaining power. That said, at a minimum, these general guidelines may be helpful for ML Providers to consider when contracting with customers/licensees:

(a) Representations and Warranties – ML Provider representations and warranties about the accuracy, quality, or performance of the ML technology and output data present some unique challenges in transactions involving the licensing of ML technology. These things can be difficult to gauge when the ML technology learns during an engagement, particularly given the opacity that surrounds exactly how ML technology makes decisions and produces output data.

(b) Indemnification – ML Provider indemnification commitments could be drafted such that the ML Provider does not have an obligation to indemnify the licensee for issues that are more directly traceable to the licensee's activities or that are more readily within the licensee's control. For example, this may include third-party claims alleging violations

[1] U.S. copyright law covers original works of authorship fixed in a tangible medium of expression, and U.S. patent law generally covers novel, useful, and non-obvious inventions. U.S. copyright and patent laws are currently interpreted to cover only works of authorship and inventions created by humans. For example, in Naruto v. Slater, 888 F.3d 418 (9th Cir. 2018), the Ninth Circuit Court of Appeals held that only humans have standing to sue for copyright infringement and the U.S. Copyright Office has taken the position that copyrights in works of authorship can only vest in humans. See Compendium of the U.S. Copyright Office Practices, Third Edition, Section 306. Similarly, the U.S. Patent Act protects inventions created by "individuals" and includes other requirements that may not be readily satisfied by a machine inventor. See 35 U.S.C. § 100(f). Given the current state of U.S. copyright and patent laws, it will in many cases be unclear who would be deemed to own or have rights to improvements to ML technologies arising from processing a data provider's input data absent clear contractual terms that address this issue.

[2] U.S. trade secret laws apply to valuable, non-public information that is subject to reasonable efforts to maintain its secrecy.

Continued on page 4...

Machine Learning Legal Issues . . . *(Continued from page 3)*

of intellectual property or other rights directed to Improvements arising from processing *the licensee's* input data or *the licensee's* operation of the ML technology.

(c) All Necessary Rights – Consider seeking representations, warranties and covenants from the licensee that it: i) has and will continue to have all rights and consents necessary to provide the input data to the ML Provider for use as permitted by the applicable agreement; and ii) will use the output data in compliance with all current and future laws, and consider seeking an indemnity for third-party claims alleging a breach of these commitments.

(d) Limitation of Liability – Consider trying to include a limitation on liability provision that covers claims asserted under all theories, including tort and statutory claims, to help protect the ML Provider from potential products liability lawsuits related to ML technology failures or defects. These provisions typically i) limit recoverable damages in disputes between the parties to direct damages only (i.e., damages that immediately and naturally result from the breach, as opposed to indirect damages, such as lost profits) and ii) incorporate an overall ceiling or "cap" on liability. Limitations on liability typically exclude certain types of claims from their coverage (e.g., indemnification claims). ML Providers should carefully consider any proposed exclusions and whether to negotiate that those exclusions should be subject to other rules on liability (e.g., higher caps on liability).

5) **Compliance with Laws**. New regulation in the artificial intelligence field may be on the horizon.[3] ML Providers should prepare accordingly and consider trying to negotiate terms in their contracts with their licensees that would allow them to adjust their product offerings or terminate their agreements altogether if new laws or regulations take effect that would outlaw or substantially constrain them from licensing, operating, or training their artificial intelligence products as originally contemplated in their agreements with licensees.

ML Providers should also closely scrutinize the extent to which they may be subject to certain laws given the nature of the input data they ingest, the output data they may create and their relationships with their licensees. For example, ML Providers who process "protected health information" on behalf of a "covered entity" are subject to HIPAA as a "business associate." And, ML Providers that ingest personal data may be subject to a growing body of data privacy laws that include onerous compliance obligations and significant penalties for non-compliance, such as the EU's General Data Protection Regulation 2016/679 and the California Consumer Protection Act, and certain state laws regulating how companies can use biometric data that are working their way through state legislatures. ML Providers must diligently assess whether data privacy laws like these laws apply, and, if so, take the necessary steps to ensure continued compliance.

Conclusion

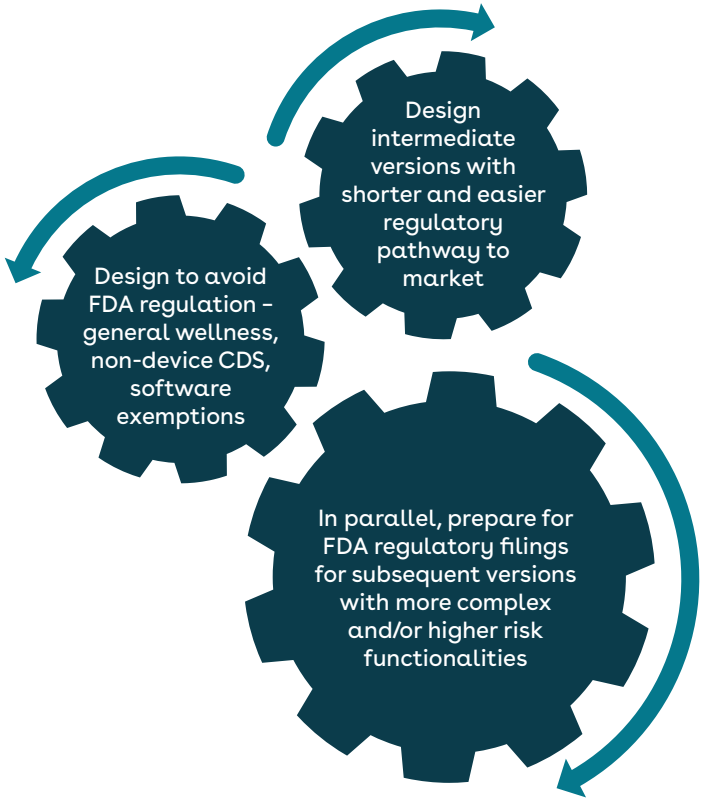
This article highlights five key areas where we often help ML Providers identify and address certain important issues in commercial transactions involving ML technologies. ML Providers should keep in mind that using ML technology can present other risks that are beyond the scope of this article, so it is important to engage counsel to help ensure those risks are adequately evaluated and addressed.

[3] For example, on January 7, 2020, the White House Office of Science and Technology released a memorandum proposing new rules to guide future federal regulation of artificial intelligence technologies. See Guidance for Regulation of Artificial Intelligence Applications, January 7, 2020. This is one of several recent developments signaling possible future regulation in the artificial intelligence space in the U.S.

How to Incorporate FDA into Your R&D

By Eva F. Yin and Paul S. Gadiock

Whether a software or a hardware product is subject to U.S. Food and Drug Administration (FDA) regulation is impacted significantly by the intended use(s) and the claims associated with the product. Understanding the impact of these and other factors on how a product may be regulated by the FDA early in the R&D provides a valuable opportunity for a company to strategically design its product around functionalities that trigger FDA regulation and premarket authorization so that it can go to market sooner. Releasing an earlier version of the product that falls outside of the FDA's jurisdiction can provide the ability to collect important data, including user feedback for and market data, for supporting a regulatory authorization of subsequent versions of the device that incorporate FDA-regulated functionalities. Pursuing these different versions of the product simultaneously (or in parallel) with both short-term and long-term goals in mind can also allow a company to adapt more easily to the changing regulatory landscape, market trends and consumer demands, and evolving technology in the digital health space.



Of course, companies would need to carefully assess whether it is commercially viable to release an earlier non-FDA regulated product, with due consideration of the intellectual property strategy and the risk of reverse engineering by competitors. In some cases, the potential benefits of launching a non-FDA regulated product may be outweighed by the costs associated with doing multiple commercial launches of incremental versions of the product. Furthermore, the ability to market and claim that the product has been FDA cleared or approved can provide significant competitive advantage by increasing consumers' and investors' confidence in the product.

In particular, companies with a first-in-class technology that will require premarket authorization through either the De Novo (available only for Class I and II medical devices) or the PMA (for Class III medical devices) pathway, both of which typically require significantly more time, data, and resources than the 510(k) pathway, should clarify and incorporate its FDA regulatory strategy in its R&D as early in the process as possible. For example, to obtain clinical data on an FDA-regulated product before clearance or approval for product development or to support an FDA filing, companies should take into account that an Investigation Device Exemption (IDE)[1] may be needed before one can test their investigational product in humans.

Another strategy to generate clinical data is for the digital health product to collect data from users that can be used to validate future regulated functionalities that are not presently manifested in the product. Under this stepwise approach to product use and not prematurely treading into FDA-regulated territory, manufacturers may be able to amass data for future FDA-regulated functionalities while bypassing the need for an IDE.

Not allocating sufficient time and resources to consider how the FDA may regulate the company's product or delaying such consideration until

[1] FDA, IDE Application, *available at* https://www.fda.gov/medical-devices/investigational-device-exemption-ide/ide-application.

Continued on page 6...

How to Incorporate FDA into Your R&D. . . *(Continued from page 5)*

much later in the R&D or just before commercial launch can end up costing more time and resources than strategizing with an FDA regulatory counsel earlier in the R&D process, when companies have an opportunity to tailor their product design according to its regulatory and market strategies.

Designing Around FDA Jurisdiction as a Non-Medical Device

In general, products that are intended for use in the diagnosis, cure, mitigation, treatment, or prevention of a disease or other condition, or intended to affect the structure or any function of the body are considered medical devices subject to FDA regulation.[2] One approach is to design a product that does not implicate these functions so that it is not considered a regulated medical device. In the digital health space, common categories of products that the FDA does not regulate include low-risk, general wellness products and non-device clinical decision support (CDS) products, each of which is summarized below.

1) Low risk, general wellness products

General wellness products are those that present a low risk to the safety of users and other persons and have an intended use that either 1) relates to maintaining or encouraging a general state of health or a healthy activity, or 2) relates the role of a healthy lifestyle with helping to reduce the risk or impact of certain chronic diseases or conditions and where it is well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or condition.[3] To be considered low risk, the general wellness product should not be invasive, implanted, or involve any intervention or technology that may pose a risk to the safety of users and other persons if specific regulatory controls are not applied, such as risks from lasers or radiation exposure.

Further, the design of the general wellness product as well as all promotional materials and claims associated with the product, including the instructions for use and the company's website, must comply with one of the following principles: 1) claims about sustaining or offering general improvement to functions associated with a general state of health do not make any reference to diseases or conditions; or 2) if making reference to diseases or conditions, then the intended uses must be narrowly tailored to promote, track, and/or encourage choice(s), which, as part of a healthy lifestyle, i) may help to reduce the risk of or ii) may help living well with certain chronic diseases or conditions. Claims that exceed these limitations may subject the product to FDA regulation.

Examples of general wellness claims or intended uses that fall outside of FDA regulation include:[4]

- Software that coaches breathing techniques and relaxation skills, which, as part of a healthy lifestyle, may help living well with migraine headaches.
- Software that tracks and records your sleep, work, and exercise routine which, as part of a healthy lifestyle, may help living well with anxiety.
- Product that promotes making healthy lifestyle choices such as getting enough sleep, eating a balanced diet, and maintaining a healthy weight, which may help living well with type 2 diabetes.
- Product that promotes physical activity, which, as part of a healthy lifestyle, may help reduce the risk of high blood pressure.
- Software that tracks your caloric intake and helps you manage a healthy eating plan to maintain a healthy weight and balanced diet. Healthy weight and balanced diet may help living well with high blood pressure and type 2 diabetes.

2) Non-device clinical decision support (CDS) products

Another common category of products that falls outside of FDA jurisdiction is non-device CDS products that meet the following four criteria:[5]

1) not intended to acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system;

2) intended for the purpose of displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

3) intended for the purpose of supporting or providing recommendations to a healthcare professional about prevention, diagnosis, or treatment of a disease or condition; and

4) intended for the purpose of enabling such healthcare professional to independently review the basis for such

[2] 21 U.S.C. § 321(h).
[3] FDA, General Wellness: Policy for Low Risk Devices (September 27, 2019), *available at* https://www.fda.gov/media/90652/download.
[4] FDA, General Wellness: Policy for Low Risk Devices, at 5.
[5] FDA, Clinical Decision Support Software (September 27, 2019), *available at* https://www.fda.gov/media/109618/download.

recommendations that such software presents so that it is not the intent that such healthcare professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.

For additional information on FDA exemptions, please refer to the Fall 2019 issue of the *Digital Health Report*.[6]

Planning Ahead for Premarket Authorization

Products that include functionalities of an FDA-regulated medical device, such as those that are intended to treat, diagnose, prevent, or mitigate a disease or health condition, will likely require premarket authorization by the FDA before the product can be legally distributed or marketed in the U.S. However, even within the realm of FDA-regulated medical devices, some medical devices are exempt from premarket notification or approval. For medical device products that are subject to FDA regulation and are not exempt from premarket notification, they generally require FDA premarket clearance through the 510(k) pathway, which requires demonstrating substantial equivalence to a previously cleared medical device, or a PMA approval for high risk Class III medical devices. The FDA aims to review 510(k) submissions within 90 days, subject to delays due to requests for additional information or questions raised by the FDA during the review process.[7]

For medical devices that are not considered high risk Class III medical device and where there is no substantially equivalent predicate (e.g., due to a new technology or a new intended use that raises new questions of safety or effectiveness), the company will need to submit a De Novo request to the FDA, including clinical testing, validation, and special controls for providing reasonable assurance of safety and effectiveness for the intended uses(s). The FDA aims to review De Novo requests within 150 calendar days, but the process can take longer if the FDA requests additional information or raises any issues during the review.[8]

Once the De Novo request has been granted, the FDA will establish a new classification regulation for a new device type, which allows competitors to use the product as a predicate device for their 510(k) submission. In some cases, the FDA may change the regulation and later exempt such device type from premarket notification. As such, companies with first-in-class products subject to FDA approval through the De Novo pathway will likely incur more cost than competitors who enter the market later through the shorter and less costly 510(k) regulatory process by using the earlier product as a predicate. That said, companies can also exploit this strategy by exploring available predicates for releasing intermediate versions of the product with functionalities that can be cleared by the FDA through the shorter 510(k) pathway, while pursuing in parallel a fully loaded version of the product for approval under the De Novo or PMA pathway.

Conclusion

Incorporating FDA regulatory strategy early in the R&D can provide significant competitive advantage and help companies avoid regulatory pitfalls, adapt more easily and quickly to changing market trends and consumer demands, and overcome hurdles in obtaining the appropriate FDA premarket authorization for the company's product(s). Early in the R&D, companies can more easily design its product or diversify its pipeline to avoid FDA regulation entirely, or plan for intermediate versions of the product that present faster FDA regulatory pathways to market, while simultaneously develop and purse the appropriate FDA premarket authorization for more regulated functionalities of the product. Such diversified strategy can help start-up companies obtain critical data, revenues, and additional financing needed for further R&D and for supporting FDA filings for subsequent versions of the product.

[6] WSGR Digital Health Report: Fall 2019, "A Window into the FDA's Risk-Based Regulatory Approach for Clinical Decision Support Software" and "Qualifying for FDA's Medical Software Exemptions" *available at* https://www.wsgr.com/en/insights/digital-health-report-fall-2019.html; FDA, Clinical Decision Support Software (September 27, 2019), *available at* https://www.fda.gov/media/109618/download.
[7] FDA, 510(k) Submission Process, *available at* https://www.fda.gov/about-fda/510k-submission-process#substantive.
[8] FDA, De Novo Classification Request, *available at* https://www.fda.gov/medical-devices/premarket-submissions/de-novo-classification-request#FDA_Review_and_Review_Timeline; De Novo Classification Process (Evaluation of Automatic Class III Designation) (October 30, 2017), *available at* https://www.fda.gov/media/72674/download.

Preparing for Your First Sale: How Digital Health Companies Can Plan for Healthcare Business

By Melissa Hudzik

It is no surprise that technological advances have changed the practice of medicine. Technology companies are creating digital health products that are modernizing and advancing the healthcare industry far beyond what any of us would have believed possible just a few years ago. Digital health products consist of a wide range of items, from devices sold direct-to-consumers to software that is added to operating room equipment in hospitals. Bringing digital health products to the healthcare industry requires companies to consider who is going to buy and pay for their products and how they are going to get paid. These factors are vital pieces of the business plan and it is never too early to start planning for that first sale.

The healthcare industry is one of the most regulated industries in America. The federal and state governments are major payors for healthcare items and services. Accordingly, laws are in place to help protect governmental purses. From fraud and abuse and compliance laws, to laws requiring licensure of durable medical equipment suppliers, the healthcare industry is a field filled with landmines for those unprepared for what may be encountered. However, with due diligence and planning, entry into the industry will be smooth and successful.

In this article we will discuss two types of buyers: 1) patients and 2) healthcare providers and three types of payors: 1) patients (often called "self-pay"), 2) healthcare providers, and 3) third-party payors. Third-party payors include: Medicare, Medicaid, other federal and state healthcare programs, and private healthcare insurance companies. Knowing who will buy your product is a key element in knowing who will pay for your product.

Knowing Your Buyers and the Payors

If you plan to sell direct-to-consumers, that is your product does not require a physician's order, your research and analysis are easy. Consumers are your target market and they will buy from you (or a third-party seller) and pay out of their own pockets for your product. For purposes of this article, we will remove the direct-to-consumer option from the calculus.

If you plan to sell to consumers, but your product will require a physician's order, those consumers are now patients and will be the ultimate buyer of your product; however, all three types of payors are in play. Likewise, if your product will be sold to healthcare providers, all three types of payors could pay for your product. Healthcare providers include:

- Physicians
- Hospitals
- Ambulatory Surgery Centers
- Durable medical equipment and device providers
- Durable medical equipment and device manufacturers
- Other health technology companies.

Once you know who will buy your product, you can evaluate how you will get paid for your product.

Knowing Who Will Pay for Your Product

Unlike the direct-to-consumers option above, which has a single payor, selling to healthcare providers or patients presents all three types of payors. At the earliest stages of your business planning, you should consider whether a third-party payor will cover your product. The variables and options are numerous. Start thinking about the following questions:

- Are there similar products on the market that are covered?
- How are they covered?
  - Are the products separately reimbursed so that the third-party payor pays for the products specifically?
  - Is payment for the product bundled into the payment for another product or procedure so that there is no separate payment?
- Do similar products have their own unique Healthcare Common Procedure Coding System (HCPCS) code? Or is there a broad code that captures like-products?
  - If similar products have unique codes, you may need to plan time in your business plan to apply for a new HCPCS code.
- Is anticipated third-party payor reimbursement enough to cover costs and expenses?
  - Has reimbursement trended upwards or downwards?

If you anticipate that a third-party payor will cover your product, you will need to decide whether you will sell your product to another manufacturer or health technology company who will in turn bill third-party payors or whether you will become a healthcare provider and bill the third-party payors yourself. Becoming a healthcare provider takes considerable time and resources but is an option that is available.

If you anticipate that your product will not be covered or if you do not intend to seek coverage, your payors will be your buyers: patients and healthcare providers. Below are a few examples of possible buyers and payors.

- If your product is something physicians will use in their offices, you may choose to sell directly to the physicians who will pay you directly.
- If your product is intended for patient-use and requires a physician's order, you may sell your product to a durable medical equipment supplier who will sell to the patient. Your payor is the durable medical equipment supplier and their payor is the patient.
- If your product is intended for patient-use and requires a physician's order, you may become a healthcare provider and sell directly to patients. Your payor here is the patient.

Why It Matters

The healthcare industry, compared to general commerce, puts distinct duties and responsibilities on digital health companies. When a federal or state healthcare program will reimburse for your product, your company must comply with all applicable laws and regulations that govern healthcare providers. This includes federal laws such as the Anti-Kickback Statute and the False Claims Act and state laws that govern healthcare providers. Accepting federal or state healthcare program payments will put scrutiny on your business that you would not face otherwise. Absent accepting federal and state healthcare program payment, some states have broad "all payor" laws that are applicable even if a private insurer or the patient themselves pay for your product.

While not accepting third-party reimbursement could ease some compliance burdens, a digital health company's interactions with patients and health care providers have their own potential obligations. For example, relationships with physicians may trigger reporting obligations to the federal and state governments, such as under the federal Sunshine Act, and maintaining protected health information could trigger Health Insurance Portability and Accountability Act (HIPAA) compliance requirements. Fortunately, regulatory and compliance obligations can be researched and planned for well in advance.

Conclusion

The healthcare industry is heavily regulated and presents regulatory and compliance challenges that are not present in other industries. Digital health companies can prepare well in advance of their first sale by knowing their buyers and payors. Digital health companies can work with counsel at any stage to research and plan for business.

How HITRUST Can Help Get You to a Series A

By Catherine Warren

Venture capital fundraising continues to be a prominent vehicle to fuel new companies. Although 2019 likely won't top 2018 in total capital raised, overall deal value is set to meet or surpass that of 2018.[1] Before moving any further, it's important to note that venture financing isn't the only avenue for a growing company. If you are unsure of whether it is the best route for your start-up, consider reading the two-part article in the previous issues of this report to help you evaluate the four partner options available for digital health start-ups.[2]

Assuming you have decided to continue down the venture capital road, it is important to start with a basic understanding of how to approach venture financing and what can make this journey easier. Any start-up hoping to receive funding from investors must consider how they organize and present their business making it appealing to investors. Researching potential investors is the best starting point. Does the investor target early- or late-stage companies? Does the investor have experience investing in your market? Are there companies in the fund's portfolio that could be seen as competitors? What risk factors do they look for? These are all questions you should be able to answer before beginning to deal directly with potential investors. Know who the big players are and what they are looking for and you can prioritize and emphasize

[1] Venture Monitor, Pitchbook and National Venture Capital Association (NVCA), https://nvca.org/wp-content/uploads/2019/10/3Q_2019_PitchBook_NVCA_Venture_Monitor-1.pdf.

[2] Digital Health Report, WSGR (Spring/Summer 2018), https://www.wsgr.com/images/content/1/3/v2/13538/DHReport-Spring-Summer2018.pdf; Digital Health Report, WSGR (Fall 2018), https://www.wsgr.com/images/content/1/3/v2/13537/DHReport-Fall2018.pdf.

Continued on page 10...

How HITRUST Can Help Get You to a Series A. . . *(Continued from page 9)*

on these areas. Not only will this help you get the financing you need, but often the elements of a start-up company that venture capitalists (VCs) prioritize are also good for your long-term business model. In the digital health market, data protection and privacy policy falls into this bucket.

This article will outline the basic trends in venture financing over the past few years, including those specific to digital health, and identify one particular factor that is continuing to gain interest to venture funds in the digital health space: The Health Information Trust Alliance (HITRUST).

2019 Venture Financing Trends

Looking at the venture field in general over the past year, the average deal size has remained high with more than 50 percent of deals raising more than $1 million. Early-stage deals have continued to draw millions in capital with an average of $14.5 million per deal and closing of more than 44 mega-deals, although it's important to note that a number of these deals include an element of debt.[3] Focusing largely on seed and early-stage deals, Pitchbook reported that the continued increase in deal size at the seed stage could be due to investors' willingness to invest despite the start-up only having a minimum viable product prior to the seed round. The result is that the company can go to market much earlier than before, giving the investor earlier return on investment.[4] An interesting dichotomy in timing has also developed. Larger investors who used to wait until later rounds of financing are more willing to jump in at the early stage while start-ups are waiting longer before looking for seed investing (an average of three years). The result here is investors are given a better picture of the company overall prior to investing. Although there are some concerns about Committee on Foreign Investment in the United States (CFIUS), immigration, and political candidate policy proposals impacting the market, 2019 did not show major signs of slowing investment.

Venture in Digital Health and Moving Forward

Turning to digital health venture trends, fundraising for healthcare and life sciences start-ups set a record in 2018 with more than $2 billion raised over two years by U.S. venture funds alone.[5] In 2019, nearly $50 billion was invested in the healthcare sector where digital health companies represented 31 percent of those investments.[6] StartUp Health reported that in 2019 there was a total of $13.7 billion in funding across 727 deals, becoming the second most funded year to date.[7] Interest in digital health continued to increase in Q3 of 2019, especially for companies showing improved patient outcomes and paths to lower healthcare costs.[8] However, there are also some concerns within the digital health market that continued expansion of CFIUS regulation could impact investment in healthcare companies resulting in a decline in investment from Asia and potentially leading to investors favoring companies that are considered "higher quality."[9]

Privacy policies and/or Health Insurance Portability and Accountability Act (HIPAA) compliance are something that many, if not all, "high quality" digital health companies have in place. We have seen the unfortunate impact on companies who do not protect the private health information that consumers have given them. Last year, the *Wall Street Journal* reported that a number of smartphone apps provided their user information to Facebook.[10] This is just one of the many stories that, combined with the numerous accounts of private patient information exposure, contributes to a negative image for digital health. By no surprise, Rock Health's 2018 National Consumer Health Survey found that only 11 percent of respondents were willing to share their personal data with tech companies.[11] The impact that a data breach can have on a start-up is detrimental and something investors are keen to ameliorate to increase a digital health start-up's chance of success.

For years venture capital firms, especially those focused on investing in digital health start-ups, have shown a preference for investing in companies that are HITRUST certified and venture capitalists are aware that if a digital health company doesn't have an iron-clad privacy and security policy in place, they are at risk of being the next company to endure a data breach. One group of venture firms, led by Frist Cressey Ventures, recently made it very clear to digital health start-ups the importance of prioritizing privacy and data protection.

[3] Venture Monitor, Pitchbook.
[4] Venture Monitor, Pitchbook.
[5] Venture Monitor, Pitchbook.
[6] HITRUST® and Frist Cressey Ventures Launch Venture Council and Program to Build Security and Privacy into the "DNA" of Tech Startups, https://hitrustalliance.net/hitrust-and-frist-cressey-ventures-launch-venture-council-and-program-to-build-security-and-privacy-into-the-dna-of-tech-startups/.
[7] StartUp Health Insights, StartUp Health, file:///C:/Users/cwa1/Downloads/2019%20Q4%20End%20of%20Year%20Full%20Report.pdf.
[8] Venture Monitor, Pitchbook.
[9] StartUp Health Insights, StartUp Health.
[10] You Give Apps Sensitive Personal Information. Then They Tell Facebook, Wall Street Journal, https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.
[11] Beyond Wellness For the Healthy: Digital Health Consumer Adoption 2018, Rock Health, https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/.

Frist Cressey Ventures in collaboration with HITRUST formed the Venture Capital Advisory Council (VC Council) and Venture Program. Currently, the VC Council includes a number of prominent venture capital firms, including Ascension Ventures, Bain Capital Ventures, Echo Health Ventures, Frist Cressey Ventures, Heritage Group, Maverick Ventures, New Enterprise Associates, 7Wire Ventures, and is continuing to gain more. The VC Council members have assets of more than $30 billion with over 1,000 companies in their portfolios combined. Two of these investors—Echo Health Ventures and Maverick Ventures—were among the top 10 most-active investors in the innovative health field in 2019, according to StartUp Health.[12]

The purpose of the Venture Program is to provide start-ups with tools and services to expedite the process of implementing adequate risk management and compliance controls. Specifically, the program provides training courses and an annual conference, a personalized assessment platform allowing start-ups to compare its HITRUST assessment scores to other companies, and additional guidance and resources to successfully establish and implement a privacy policy.[13] Note that to be eligible, the start-up must have been incorporated or founded within the last five years, have under 100 full-time employees, and have an annual revenue under $20 million.

If digital health start-ups aren't already prioritizing data protection, the move by Frist Cressey Ventures to partner with HITRUST should be their wake-up call. Let's return quickly to a concept first mentioned in this article. It is good practice to understand the aspects that an investor looks for in a start-up, and since venture firms are showing an increased interest in privacy and data protection, and specifically in HITRUST, you as the start-up eager for venture financing should be prioritizing this as well. With that in mind, the next section of this article will take a look at HITRUST and what it has to offer.

HITRUST and Whether It's Worth It

HITRUST is an organization founded in 2007 and governed by a representative body in the healthcare industry that developed a comprehensive information risk management and compliance program, the Common Security Framework (CSF). The HITRUST CSF is approved by the U.S. Department of Health and Human Resources as an acceptable risk management framework for HIPAA. Additionally, the framework provides a common set of controls for a larger group of compliance standards including GDPR, PCI, ISO, NIST, and COBIT.[14] The program is designed to be flexible and adapt to changes in policy and provide compliance throughout the life cycle of any healthcare company.

To begin the compliance process, a start-up will input its risk factors based on a provided list into the software, that then generates a report with control specification based on 19 categories of control requirements. Following this report, the company can choose to complete three stages of assessment to determine how the company is doing based on the specified controls.[15] The first step is the self-assessment, where the company can use the CSF Assessment Report and MyCSF Software to run through a checklist internally and determine any gaps in their security control system. This can take up to around two months to complete depending on the needs of the company. Furthermore, because this is done internally, there is only a basic level of assurance that HITRUST can offer at this point.

If the company would like more compliance security, it can then seek CSF Validation, a second and more stringent assessment. This involves a CSF or third-party assessor reviewing the company's self-assessment, conducting an in-depth look at security controls, and evaluating compliance with each control requirement through an on-site visit to the company. The assessor will determine any major issues missed during the self-assessment and return a Validated Report. It is important to note that this stage will not ensure that the company could pass a HIPAA audit—only the CSF Certification will ensure this.

Finally, if the company chooses to, it can apply for CSF Certification, which will ensure that the company is compliant with all regulating bodies. The assessor will score the company's compliance on each security measure. This is determined by how the company's security policy is put in place and the procedures for that policy. HITRUST will then review the assessment, which can take a few months, and then they will issue a CSF certification. The certification will be valid for two years at which point, the company will need to undergo assessment again.

Clearly, the HITRUST certification process is very taxing. Many months of assessment and use of company time, money, and resources can burden a start-up. However, due to the way the assessment is completed, integrating

[12] StartUp Health Insights, StartUp Health.
[13] Which Assessment is Right for Me?, HITRUST, https://hitrustalliance.net/assessment-right/.
[14] HITRUST CSF, HITRUST, https://hitrustalliance.net/hitrust-csf/.
[15] What is the HITRUST Certification Process?, RSI Security, https://blog.rsisecurity.com/what-is-the-hitrust-certification-process/#1963.

Continued on page 12...

How HITRUST Can Help Get You to a Series A. . . *(Continued from page 11)*

the HITRUST framework early on in the life of a company can reduce this burden. Moreover, venture capital firms are eager to invest in digital health start-up companies that are HITRUST compliant and assessing your HITRUST compliance may allow you, as a start-up, to negotiate for better terms in your next equity financing. Also consider that investors are concerned with reducing cybersecurity threats and want to ensure that these threats are minimized as much as possible before investing. This is an understandable concern since consumers are skeptical about sharing health data with tech companies, which can stunt development in start-up company work, therefore limiting the returns that a venture firm will see on its investment. More importantly, for long-term success, it's imperative that a company assures its customers that their health information is secure and will remain secure.[16] Ensuring customers that their health information remains protected by a HITRUST-certified company may be the comfort that the customer needs.

Conclusion

Digital health start-ups are starting to find their place more and more in the venture world, leading venture firms to give them more attention. As one venture capital put it, investors care about how a digital health company will "move the needle on cost, quality, and access to care."[17] Adequate data protection and privacy policies are a necessary preliminary matter before any start-up can consider how they will move the needle. Venture firms understand the costs that come with establishing and maintaining a privacy policy. The Venture Program aims to encourage start-ups to seek HITRUST CSF certification while reducing the burden that comes along with that process. If you plan to seek HITRUST certification, consider participating in the Venture Program as it may give your start-up an opportunity to connect with venture firms on the Venture Council to help kickstart your next venture financing while also providing your company with a strong privacy foundation necessary for long-term success.

[16] Why Your Health Startup Should Prioritize Privacy And Data Security, Forbes, https://www.forbes.com/sites/forbesbostoncouncil/2019/08/26/why-your-health-startup-should-prioritize-privacy-and-data-security/#3fa0aa465c90.
[17] Where Top VCs are Investing in Digital Health, Tech Crunch, https://techcrunch.com/2019/12/16/where-top-vcs-are-investing-in-digital-health/.

The Digital Health Report is developed and reviewed by a team of attorneys from the firm's corporate, intellectual property, litigation, and regulatory departments, including the individuals listed below.

Ali R. Alemozafar
Partner
Intellectual Property
415-947-2054
aalemozafar@wsgr.com

Farah Gerdes
Partner
Technology Transactions
617-598-7821
fgerdes@wsgr.com

David Hoffmeister
Partner
Corporate
650-354-4246
dhoffmeister@wsgr.com

Michael Hostetler
Partner
Patents and Innovations
858-350-2306
mhostetler@wsgr.com

James Huie
Partner
Corporate
650-565-3981
jhuie@wsgr.com

Manja Sachet
Partner
Technology Transactions
206-883-2521
msachet@wsgr.com

Kathleen Snyder
Of Counsel
Technology Transactions
617-598-7857
ksnyder@wsgr.com

WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Beijing Boston Brussels Hong Kong London Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC Wilmington, DE