DIGITAL HEALTH REPORT
FALL 2018
WSGR Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

Evaluating Prospective Partners When Scaling Your Digital Health Company (Part 2)

By Jake D. Gatof

In Part 1 of this article from our last Digital Health Report, we looked at the opportunities and some of the potential limitations of engaging with a venture or strategic technology (FAANG+) partner alone. As a digital health company continuing to look around the "digital health room" so-to-speak, you're still not sure whom to engage with next and what it would look like. You contemplate how to obtain deployment in a major healthcare system, and you start to wonder about the challenges of penetrating large healthcare systems and potentially disrupting or complementing the current ways of providers and caregivers; navigating the payment and reimbursement landscape; and the changes to the business model that addressing each of those challenges will necessitate.

IN THIS ISSUE

Payers

Opportunities and Limitations

Necessity: You recognize that while your technology could in fact transform patient care by improving health outcomes and lowering costs, it can only do so if key stakeholders, most notably payers and providers, take the leap with you and are willing to reward you appropriately for cost-savings, efficiencies, and improvement. From a pure business viability perspective, the primary focus becomes payers first.

Impetus to Innovate: Fortunately, as much as you seem to need payers, they seem to need you. As more and more healthcare information and plan options become available to consumers, payers are quickly recognizing the need to focus on improving customer satisfaction. According to a new HealthEdge survey, a majority of payer survey participants highlighted the need to modernize technology to achieve the goal of improving customer satisfaction.[1] For insurers, secure communication platforms, wearables, health monitoring apps, and other means of patient engagement are spearheading preventative medicine, and could help lower costs associated with chronic illnesses. Payers are no longer challenging the place for digital health solutions in their systems.

Compatibility: You are also confident that the most important digital health objectives for payers could be achieved through the adoption and implementation of your technology. In its paper, "Healthcare Payers: In Pursuit of Four Digital Objectives," INFOSYS outlined the following four digital health focus-points for

[1] https://www.healthedge.com/confirmation-survey-report-download-voice-health-plan-market-modern-technology-key-enabler-reduce-costs

(Continued on page 2)

Evaluating Prospective Partners . . . *(continued from page 1)*

payers: 1. Robust consumer experience strategy, 2. Effective "mobile application channel" for customer reach, 3. Optimized operations through digitization, 4. Collaboration for connected health. These points have a common thread: a focus on patient utility and engagement, revealing, in turn, that collaboration with a payer may be a vital gateway to patient adoption.[2]

Risks of Exclusivity: Of course, partnering with or collaborating with a single payer may limit your future ability to engage with other payers or provider networks. With increased competition to provide value-based care among payers, and with an increased focus on bundled-payment options, competition for exclusive engagements with novel digital health innovation is fierce. Another frequent pain point is that payers may already want you to have hard evidence and proof points.

Transactional Issues and Processes

Native Complexity and Increased Diligence Requirements: As Dr. Karen Lee of Humana has noted about payers, "[T]hese are large, political, complex organizations with current programs being deployed. Even if [they] notice a new technology or pilot is going really well, [they] have to start planning out the longer term of how [they're] going to shift current programs to a new program."[3] In anticipation of this increased administrative complexity, the difficulty of overcoming existing momentum regarding legacy deployments, enhanced diligence (including a focus on preparedness for regulatory hurdles), and the complexities of engaging with covered entities, digital health startups should strive to add legitimacy to their adoptability early on (e.g., gathering frequent hard and "soft" evidence from users and stakeholders or engaging with the Food and Drug Administration (FDA) rather than structuring the business to avoid required approvals).

Digital health innovators should also engage with their advisors to track initiatives of relevant governmental bodies, such as The Centers for Medicare & Medicaid Services' identification of telemedicine as a priority for improving rural healthcare, as indications of payer preferences and priorities, and as a way to provide clearer expectations for future commercial partners. Early on, digital health start-ups should also consider requesting ongoing commercial covenants to support engagement with stakeholders in other partner categories.

Special Rights Regarding Mergers & Acquisitions: Payers, which have driven a significant portion of M&A activity in the digital health space, will also likely be concerned about falling behind their competition, and may make more long-lasting proposals to solidify their opportunity to engage with you and modernize their offering. Given this, payers, like strategic technology investors, may ask for certain restrictions and covenants related to sales and acquisitions, including rights of first negotiation/offer/refusal and exceptions from drag-along restrictions.

Providers

Opportunities and Limitations

Irreplaceability: While the other partner categories look toward a patient-centric and consumer-focused digital health future, you and your colleagues agree that it would be foolish to ignore the norm of physician-driven healthcare data and the critical role that individual providers and provider networks play when it comes to adoption, feedback, and improvements of digital health innovations. Beyond the fact that physician adoption is as an excellent bellwether for your technologies' ability to meet the use case, you understand that the only real ability for such technology to reach its potential is dependent on whether it can be tailored or refined to properly consider physician workflow and the practical challenges facing the coordination of patient care (not to mention the regulatory restrictions on use of patient data outside of a care scenario).

Investment and Engagement: You and your team also recognize the clear commitment such providers and provider networks have made to adopting digital health solutions. For example, the American Medical Association strengthened its commitment to driving provider adoption and usage of digital health solutions — committing $27 million to its partner incubator Health2047, according to MobiHealthNews, and academic institutions, like Beth Israel Deaconess Medical Center's launching of the Health Technology Exploration Center, an incubator aimed at developing scalable digital health technologies—that are, as stated by the Digital Health Briefing by *Business Insider*, "further indications that providers now consider fostering new digital health technologies crucial to the future of healthcare….With their existing patient data and physician expertise, hospital-led initiatives may be uniquely positioned to direct digital health improvements that streamline delivery of care."

Transactional Issues and Processes

Structural Complexities: Like payers, providers—whether they are nationally consolidated provider networks, regional health systems, or those affiliated with academic medical centers—frequently come with certain inherent transactional inefficiencies and limitations as a covered entity. As provider networks have consolidated, multi-layered approval processes and increased diversity in perspectives among internal stakeholders can cause challenges in collaboration and implementation. Most notably, providers, already under significant cost pressures, are largely subject to the preferences of payers, governmental bodies, and other external stakeholders as to the real value of adopting or deploying a digital health solution. The need to navigate a sophisticated web of both internal and external stakeholders makes such engagements more complicated.

Takeaways and One More Important Group—Patients

In an ideal world, there would be engagements with each of these abovementioned partner categories. In the less-than-ideal world of being a start-

[2] https://www.infosys.digital/assets/pdfs/healthcare-payers-digital-objectives.pdf
[3] https://www.youtube.com/watch?v=C1xA893xPAg

up, however, near-term capital needs may lead you down one path, while early relationships with familiar organizations may instead, first, take you down another. What remains critical, no matter who you engage with first, is continuing the conversation as to the strengths and limitations of each partner category and the varied nature of the transaction issues and processes related to a respective engagement. No single partner type alone can drive success in the digital health space.

Therefore, it is helpful to engage with partners that have a proven track record of engaging with the different partner categories. The market has already seen examples of such engagement. For instance, Cerner has partnered with Salesforce to offer cloud solutions for population health, Epic has integrated its electronic health record offering with artificial intelligence company Nuance's virtual assistant, and Comcast has recently announced a partnership with Independence Health Group to develop a new healthcare platform. Just as important, however, is approaching, preparing for, and executing on transactions, early on in a company's growth, that are forward-looking in manner and that are structured and negotiated with the inevitability of other partnerships in mind, rather than in a manner that challenges the need for other stakeholder involvement.

Finally, and irrespective of the value of any of the four potential partners covered in this series, it is imperative not to forget the most essential group of all: ***patients***. Whether you work with venture, established technology players, payers, or providers first, your ability to impact the delivery of healthcare must focus on the improvement of the patient health experience, especially considering many of the most successful consumer-facing products and technologies today have been able to improve how consumers interface with our most "usual" tasks and resources and how preeminent a position health holds in all of our hierarchies of needs.

Designing and managing digital health solutions—along with the development of related internal policies—to address the needs, challenges, and frustrations of patients is essential to creating health technologies that cultivate and encourage patient ownership of health. Even more important may be the need to design and manage such digital health solutions with an awareness as to varying technology usage patterns, transfer needs, and diversity in access, especially as regulatory frameworks regarding privacy, payment and reimbursement, and required adoption continue to evolve. Having a patient-first mission that expects and is prepared to be flexible and adaptable to serve that goal will likely help mitigate the impact of any outside forces or uncertainty, including changes to applicable laws and regulatory regimes.

Get Your Facts Right: *Berkheimer's* Impact on the Second *Alice/Mayo* Step of the Patent Eligibility Analysis

By Peter S. Kang

A previous WSGR Health Report generally described how the United States Patent and Trademark Office (USPTO) applies the two-step *Alice/Mayo* framework to determine whether a digital health software patent application satisfies the requirements under 35 U.S.C. § 101, the statute governing patent-eligible subject matter.[1] The instant article provides additional detail around the second *Alice/Mayo* step, the Federal Circuit decision *Berkheimer v. HP*, 881 F.3d 1360 (Fed. Cir. Feb. 2, 2018), *Berkheimer*'s impact on the fact-finding component of the second *Alice/Mayo* step analysis, and takeaways from *Berkheimer* as applied to the prosecution of digital health software applications.

The Two-Step *Alice/Mayo* Framework

The two-step *Alice/Mayo* framework provides guidance on how to distinguish between patentable subject matter and non-patentable subject matter.[2] The first *Alice/Mayo* step examines whether the claims are directed to a patent-ineligible concept such as an abstract idea.[3] If the claims are found to be directed to an abstract idea under the first *Alice/Mayo* step, the second *Alice/Mayo* step comes into play. The second *Alice/Mayo* step – sometimes referred to as the "search for an inventive concept" or the "significantly more" analysis – "consider[s] the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim into a patent

[1] *See generally* Jackie Stroneck, *Patent-Eligible Subject Matter in Digital Health*, Wilson Sonsini Goodrich & Rosati Digital Health Report, Winter 2018, *available at* https://www.wsgr.com/publications/PDFSearch/digital-health-report/Winter18/digital-health-report.htm#2

[2] *See generally id.*

[3] *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014). While not the subject of the instant article, claims that are directed to improvements in computer functionality or other technology have generally been held to not be directed to an abstract idea. *See, e.g.*, *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016) (claims to a self-referential table for a computer database were directed to an improvement in computer capabilities and not an abstract idea); *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1315 (Fed. Cir. 2016) (claims to automatic lip synchronization and facial expression animation were directed to an improvement in computer-related technology and not an abstract idea); *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1259-60 (Fed. Cir. 2017) (claims to an enhanced computer memory system were directed to an improvement in computer capabilities and not an abstract idea); *see also* MPEP § 2106.04(a).

Continued on page 4...

Get Your Facts Right . . . *(continued from page 3)*

eligible application.'"[4] The second step is satisfied when the claim limitations "involve more than performance of 'well-understood, routine, [and] conventional activities previously known to the industry.'"[5] In the past, claims have been shown to show "significantly more" under the second *Alice/Mayo* step when there is/are:

- improvements to the functioning of a computer;
- improvements to any other technology or technical field;
- applying the judicial exception with, or by use of, a particular machine;
- effecting a transformation of reduction of a particular article to a different state or thing; or
- adding a specific limitation other than what is well-understood, routine, conventional activity in the field, or adding unconventional steps that confine the claim to a particular useful application.[6]

Summary of *Berkheimer*

In *Berkheimer*, the patent at issue related to "digitally processing and archiving files in a digital asset management system."[7] The representative claim recited:

> A method of archiving an item in a computer processing system comprising:
>
> - presenting the item to a parser;
> - parsing the item into a plurality of multi-part object structures wherein portions of the structures have searchable information tags associated therewith;
> - evaluating the object structures in accordance with object structures previously stored in an archive;
> - presenting an evaluated object structure for manual reconciliation at least where there is a predetermined variance between the object and at least one of a predetermined standard and a user defined rule.[8]

The lower court held as a matter of law that the asserted claims were directed to an abstract idea and did not contain an inventive concept.[9]

On appeal, the Federal Circuit found the claims were directed to an abstract idea under the first *Alice/Mayo* step.[10] But when analyzing the second *Alice/Mayo* step, the Federal Circuit noted that the "question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact."[11] Here, the Federal Circuit highlighted that some of the asserted claims contained limitations "directed to the arguably unconventional inventive concept described in the specification."[12] Consequentially, the Federal Circuit concluded that a genuine issue of material fact as to these claims' inventive concept existed in light of the specification and that it was improper to find these claims patent-ineligible as a matter of law.[13]

***Berkheimer*'s Impact on the Fact-Finding Component of the Second *Alice/Mayo* Step**

Since *Berkheimer*, the USPTO has issued materials providing guidance on *Berkheimer*'s impact on the second *Alice/Mayo* step analysis.[14] Of note, these USPTO materials emphasize that the "question of whether additional elements represent well-understood, routine, conventional activity is distinct from patentability over the prior art under 35 U.S.C. §§ 102 and 103" because "a showing that additional elements are obvious under 35 U.S.C. § 103, or even that they lack novelty under 35 U.S.C. § 102, is not by itself sufficient to establish that the additional elements are well-understood, routine, conventional activities or elements to those in the relevant field." Moreover, these USPTO materials state how "an examiner should conclude that an element (or combination

---

[4] *Alice*, 134 S. Ct. at 2355 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 78-79 (2012)).
[5] *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1347-48 (quoting *Alice*, 134 S. Ct. at 2359).
[6] *See generally* MPEP § 2106.05(a)-(e).
[7] *Berkheimer*, 881 F.3d at 1362.
[8] *Id.* at 1366.
[9] *Id.* at 1366, 1368.
[10] *Id.* at 1366-67 ("The claims are similar to claims we held directed to an abstract idea in prior cases. . . . Because the claims are directed to an abstract idea, we proceed to the second step of the *Alice* inquiry.").
[11] *Id.* at 1368 (emphasis added).
[12] *Id.* at 1370 ("Claim 4 recites "storing a reconciled object structure in the archive without substantial redundancy." The specification states that storing object structures in the archive without substantial redundancy improves system operating efficiency and reduces storage costs. It also states that known assert management systems did not archive documents in this manner.").
[13] *Id.*
[14] The USPTO has indicated that it is requesting comments on some of its *Berkheimer* materials. *See generally* Request for Comment on Determining Whether a Claim Element Is Well-Understood, Routine, Conventional for Purposes of Subject Matter Eligibility, *available at* https://www.gpo.gov/fdsys/pkg/FR-2018-04-20/pdf/2018-08428.pdf. To date, the USPTO have received numerous comments from the public. *See* Comments on Request for Comments on Determining Whether a Claim Element Is Well-Understood, Routine, Conventional for Purposes of Subject Matter Eligibility, *available at* https://www.uspto.gov/patent/laws-and-regulations/comments-public/comments-request-comments-determining-whether-claim. Time should tell whether these comments will have any substantive impact on the USPTO materials.

of elements) represents well-understood, routine, conventional activity *only* when the examiner can readily conclude that the element(s) is widely prevalent or in common use in the relevant industry."[15] In particular, the USPTO materials highlight that an additional element (or combination of elements) is *not* well-understood, routine, or conventional *unless* the examiner finds, and expressly supports a rejection in writing with, one or more of the following:

1. a citation to an express statement in the specification or to a statement made by an applicant during prosecution that demonstrates the well-understood, routine, conventional nature of additional element(s);
2. a citation to one or more of the court decisions discussed in MPEP § 2106.05(d)(II) as noting the well-understood, routine, conventional nature of the additional element(s);
3. a citation to a publication that demonstrates the well-understood, routine, conventional nature of the additional element(s);
4. a statement that the examiner is taking official notice.[16]

With respect to No. 1, a "specification demonstrates the well-understood, routine, conventional nature of the additional elements when it describes the additional elements as well-understood or routine or conventional (or an equivalent term), as a commercially available product, or in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. 112(a)."[17]

With respect to No. 3, "an appropriate publication could include a book, manual, review article, or other source that describes the state of the art and discusses what is well-known and in common use in the relevant industry."[18] Importantly, the "nature of the publication and the description of the additional elements in the publication would need to demonstrate that the additional elements are widely prevalent or in common use in the relevant field, comparable to the types of activity or elements that are so well-known that they do not need to be described in detail in a patent application to satisfy 35 U.S.C. § 112(a)."[19] Hence, "merely finding the additional element in a single patent or published application would not be sufficient to demonstrate that the additional element is well-understood, routine, conventional, unless the patent or published application demonstrates that the additional element are widely prevalent or in common use in the relevant field."[20]

With respect to No. 4, the USPTO materials make clear that this option should be used "only when the examiner is certain, based upon his or her personal knowledge, that the additional element(s) represents well-understood, routine, conventional activity engaged in by those in the relevant art."[21] An applicant may challenge an examiner's Official Notice by specifically stating that such element(s) is not well-understood, routine, conventional activity, which in turn would turn the burden on the examiner to provide one of item Nos. 1– 3, or an affidavit or declaration under 37 CFR 1.104(d)(2) setting forth specific factual statements and explanation to support his or her position.[22]

Takeaways for Prosecution of Digital Health Software Patent Applications

Being mindful of the *Berkheimer* case as well as the aforementioned USPTO *Berkheimer* materials can be helpful before filing a digital health software patent application or responding to USPTO Office Actions after such an application has begun prosecution.

- Applicants should carefully consider what components, if any, of the claimed subject matter are "well-understood, routine, and conventional" and be mindful of these considerations as they draft the specification.
- When applicable, applicants should carefully consider drafting the specification to include adequate disclosure that describes how the claimed features offers technical improvements or a technical advantage over the prior art.
- If an examiner issues a second *Alice/Mayo* step rejection because the digital health software claims are "well-understood, routine, and conventional" in light of court decisions in MPEP § 2106.05(d)(II) described in Item No. 2 above, applicants should carefully consider whether the additional elements in the digital health software claims are identical to the element addressed in the cited court cases. The USPTO *Berkheimer* materials indicate that the "additional element in the claim must be the same as the element addressed in the court case" for No. 2 described above to apply.[23]
- If an examiner issues a second *Alice/Mayo* step rejection because the digital health software claims are "well-understood, routine, and conventional"

[15] Robert W. Bahr, Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*) (Apr. 19, 2018) at 3 (emphasis in original), *available at* https://www.uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF (hereinafter "April 19, 2018 USPTO Memo"); Training: Well-Understood, Routine, Conventional Activity (posted May 7, 2018) at 3 (emphasis in original), *available at* https://www.uspto.gov/sites/default/files/documents/berkheimer-training-20180427.pptx (hereinafter "May 7, 2018 USPTO Berkheimer Training").
[16] April 19, 2018 USPTO Memo at 3-4; May 7, 2018 USPTO Berkheimer Training at 9-14.
[17] April 19, 2018 USPTO Memo at 3-4.
[18] *Id.* at 4.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] May 7, 2018 USPTO Berkheimer Training at 11 (emphasis added).

Continued on page 6...

Get Your Facts Right . . . *(continued from page 5)*

in light of a publication described in No. 3, applicants should carefully consider whether the publication shows that the elements are "widely prevent or in common use." The USPTO *Berkheimer* materials emphasize that "[m]erely finding the additional element in a single patent or published application would not be sufficient to demonstrate that the additional element is well-understood, routine, conventional, unless the patent or published application demonstrates that the additional element is widely prevalent or in common use in the relevant field."[24]

- If an examiner issues a second *Alice/Mayo* step rejection because the digital health software claims are "well-understood, routine, and conventional" under any circumstance, applicants should carefully consider whether the examiner properly evaluated the additional elements individually and in combination to determine whether the claim includes significantly more than a judicial exception. The USPTO *Berkheimer* materials emphasize that to "support a rejection of a claim where the examiner takes the position that additional elements A and B are routine, the combination of A and B must be shown to represent well-understood, routine, conventional activity in the pertinent art."[25]

[24] *Id.* at 12 (emphasis in original).
[25] *Id.* at 16 (emphasis in original).

HIPAA for Digital Health Entrepreneurs: First Installment

If you picked up a copy of the WSGR Digital Health Newsletter, chances are you may have already spent time (perhaps quite a bit of it) thinking about HIPAA – the U.S. federal law governing certain types of health information, also known as the Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191. As a digital health entrepreneur, at some point HIPAA may have become more than a form you sign at the doctor's office, or the line behind which you stand while waiting to pick up your prescription. Rather, HIPAA is an integral part of your company's development and ultimate success: How your product operates, who you market it to, what you can do with the data you collect, and other fundamental questions are inextricably tied to these regulations, for better or, (as it may seem sometimes) for worse.

For many of our clients at the cutting edge of digital health technology, HIPAA is often seen as an obstacle to innovation versus the oil to an otherwise well-tuned idea. Beginning with this article, and in future installments, however, we aim to turn on its head the notion that HIPAA is simply a burden to be shouldered, but rather with a bit of knowledge and planning, HIPAA compliance can be your competitive advantage and a framework to safeguard your company's most valuable asset—data. While it is never too late to start thinking about HIPAA, identifying and planning for HIPAA earlier on will support a more seamless and successful product trajectory.

We begin this series with some basics, and over time will expand to cover more nuanced and highly relevant topics emerging at the intersection of HIPAA and digital health. This article will tackle some foundational questions, particularly what is HIPAA and who are the key players.

A Brief, Selected History of HIPAA

HIPAA is a federal law that establishes certain standards for the use and disclosure of protected health information or "PHI," among other things. Since it was enacted by Congress in 1996, HIPAA has been amended over time to contain four distinct rules: the Privacy, Security, Breach Notification, and Enforcement Rules. In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the recession recovery effort to promote the adoption and meaningful use of health information technology. The HIPAA Omnibus Rule was finalized four years later in 2013, which incorporated a number of provisions under HITECH to strengthen privacy and security protections, as well as finalize the Breach Notification Rule.

This brief timeline brings us up to present-day HIPAA, but it is useful context to take a few steps back and consider why Congress passed HIPAA in the first place. It may be somewhat surprising that HIPAA became law with the express purpose to "improve portability and continuity of health insurance coverage" for employees moving between jobs. While continuity of health insurance may seem fairly attenuated from the challenges confronting digital health companies today, consider for a moment HIPAA's impact on the mass transition from paper records (recall those floor-to-ceiling filing systems that opened with the turn of a crank?), to information being stored and transmitted digitally. By directing the U.S. Department

of Health and Human Services (HHS) to adopt national, simplified standards for electronic healthcare transactions through HIPAA, Congress aimed to push the health industry to computerize patients' medical records, thereby facilitating the "portability" of health information. As the largest payer in the country, the federal government was able to exercise enormous influence on how transmission of information would evolve in certain ubiquitous healthcare transactions, such as billing for a claim or determining enrollment eligibility. For those readers with a medical background, the national provider identifier or "NPI" was also an innovation of HIPAA, which vastly improved efficiency and effectiveness of electronic healthcare transactions. Years later, the U.S. government through HITECH poured billions of dollars ($35 billion to be exact) into the widespread adoption of EHR systems.

With a bit of history as context, one can begin to see that HIPAA has played a central role in ushering in the digital era of healthcare.

However, for all the emphasis on "portability," Congress also recognized early on that advances in electronic technology could undermine the privacy and security of health information, particularly as this information moved more freely between different entities. To address this, HIPAA mandates the adoption of safeguards for individually identifiable health information by entities that are subject to its rules (as discussed in more detail below).

The "A" in HIPAA standing for "accountability" imposes on the healthcare industry a certain *quid pro quo* to the ease, efficiency, and new opportunities afforded by the rapid transmission of health information. Things that impact the health, safety and welfare of individuals are understandably ripe targets for regulation; therefore, we should not be surprised that fundamental to HIPAA is protecting the security and integrity of our health information.

Who Are the Key Players?

With that brief history of HIPAA, the next question is, to whom does it apply?

HIPAA primarily regulates "covered entities," defined as a health plan, a healthcare clearinghouse (e.g., a billing service) and a healthcare provider who transmits any health information in electronic form in connection with certain specified healthcare transactions (e.g., billing).

Rather than HIPAA obligations beginning and ending with these covered entities, HIPAA recognizes that covered entities often outsource a number of internal processes to third parties, who will provide certain services that involve PHI. To avoid PHI becoming vulnerable after leaving the covered entity, but acknowledging the practical need to obtain services, HIPAA also regulates the so-called "business associates" who perform these services to covered entities.

Business associates are persons or businesses which: 1. create, receive, maintain, or transmit PHI for a function or activity that is regulated by HIPAA (e.g., activities related to practice management), or 2. who provide certain other broadly defined services (e.g., management or administrative services), if those services involve the disclosure of PHI. The definition of a business associate is subject to certain limited exceptions, including, for example, that a member of the covered entity's workforce would not be considered a business associate. Note that a covered entity can be a business associate of another covered entity if it otherwise meets the definition by providing the services in (1) or (2).

Particularly relevant to our clients in digital health, the HHS Office for Civil Rights (OCR), the agency responsible for enforcing HIPAA, has issued guidance designating cloud service providers (CSPs) as business associates if the CSP receives, transmits, creates, or maintains PHI in the normal course of providing the service. This is true even if the PHI is only held for a brief time, and regardless of whether the CSP can even access the PHI (e.g., it does not matter if the PHI is encrypted and the CSP lacks the key). Given the importance of this particular topic to our clients, we will delve more deeply into CSPs as business associates in a subsequent installment.

The third key player under HIPAA is the "subcontractor." To use some helpful imagery, if a covered entity is the first link in the chain, then the business associate is the second, and a subcontractor is any subsequent entity with whom the *business associate* delegates a function it would have performed on behalf of its covered entity customer or client.

Subcontractors are bound to the same obligations under HIPAA as a business associate, but the unique term is appropriate because the contractual relationship is distinct as between a business associate and its subcontractor: Whereas covered entities are responsible for entering into a particular agreement with any business associate with whom it discloses PHI, it is the *business associate's* responsibility to execute a separate agreement with a subcontractor. By shifting the burden to the business associate (who is in the best position to vet a potential subcontractor), it encourages them to choose wisely, as it will be the business associate's responsibility (not the covered entity's) for a breach or other misuse of PHI by a subcontractor it has engaged with.

An Introduction to Business Associate Agreements

As a digital health entrepreneur, you may have encountered the contractual glue that holds these various entities together–the business associate agreement (BAA). HIPAA requires that prior to a covered entity disclosing PHI to a business associate, the parties must execute a BAA (sometimes called a "business associate addendum" because it is attached to a master services agreement). The BAA contains a number of standard provisions required by HIPAA: It must include parameters around the permitted use and disclosure of PHI, representations that the business associate will employ reasonable safeguards to protect the PHI pursuant to the Security Rule, and obligations to report breaches and other security incidents, among other provisions. (As noted, if you are a business associate engaging a subcontractor, you must separately execute an agreement containing the same core terms, although it need not be an identical agreement to the one the business associate itself signed).

Continued on page 8...

HIPAA for Digital Health Entrepreneurs . . . *(continued from page 7)*

One of the most frequent questions we receive about HIPAA revolves around BAAs, as this is often the first point of contact with HIPAA for many of our digital health clients. A typical scenario begins with the sales team encountering a customer who wants the company to enter into a business associate agreement, and the question is, to sign or not sign? The first question (particularly if this is a new territory for the company), is to pause and ask, "Why is this customer requesting a BAA?" Specifically, is the customer a covered entity under HIPAA. (It's not uncommon for the party on the other side to make assumptions about this that may or may not be correct.) If the answer appears to be yes, then the second question is whether the company endeavoring to provide services will place it squarely within the definition of a "business associate." This is often a nuanced question given the multi-dimensional nature of our client's product offerings, and it is a good time to reach out to your WSGR attorney or other counsel to come to some clarity on the matter.

You may ask, as many have, what exactly would be the harm in just signing the BAA? It's a good and very reasonable question. What we find to be unique about BAAs is that if your company has not previously considered HIPAA, representing the degree of compliance with HIPAA required by a BAA is not something that can be "eyeballed," so to speak. While you may often hear that the HHS OCR is not necessarily looking for sterling perfection by business associates, failing to take at least the first, well-defined steps with respect to HIPAA compliance will not play well with a regulator or your customer. This first step is a process called a "risk assessment," which evaluates your company's current privacy and security policies and procedures against the (flexible) standards required under HIPAA. Given the foundational importance of this topic to many of our clients, we reserve the details for a future installment. However, documenting your compliance with this prescribed assessment, identifying the gaps, and beginning to work on a plan to fill those gaps, are of primary importance when it comes to deciding whether or not to sign a BAA.

Next Steps

Having reviewed the basics, we can look forward to covering more critical and foundational ground. On the way are real-world, cutting-edge examples and analysis of how HIPAA is impacting the digital health industry. If this newsletter has provoked questions about HIPAA, privacy, or other topics in digital health, please contact your WSGR attorney for more information.

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.

Haley Bavasi
Associate
Intellectual Property
617-598-7826
hbavasi@wsgr.com

Jake D. Gatof
Associate
Corporate
617-598-7812
jgatof@wsgr.com

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

Charles T. Graves
Partner
IP Litigation
415-947-2109
tgraves@wsgr.com

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

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

Peter Kang
Associate
Intellectual Property
858-350-2362
pkang@wsgr.com

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

WSGR
Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

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