

# Digital Health Tools—Run Forward or Step Back? The Role of Due Diligence in Assessing M&A and Investment Opportunities in Digital Health

Jodi G. Daniel\*

Todd D. Rosenberg

Crowell & Moring LLP

Washington, DC

**D**igital health tools have the potential to improve health care delivery and its associated cost, change individual behaviors related to health and fitness and disease management, and enable doctors and hospitals to manage their increased accountability for patient outcomes. As a result, digital health technology, such as wearable sensors, remote monitoring devices, mobile health tools, and data analytics services, is of increasing interest to investors and health care organizations that seek to invest their funds.

If the digital health market had its own remote monitoring device to track progress and improvements based on mergers and acquisitions (M&A) activity, venture capital funding, Initial Public Offering (IPO) success, and other metrics, a person reviewing the data stream would be pleased with the healthy market results.

The venture capital firm Rock Health reported that 2015 saw \$4.5 billion of venture capital funding of digital health companies, an increase in the number of later stage rounds for digital health companies, and 187 digital health M&A transactions that represented an aggregate disclosed value of \$6 billion.<sup>1</sup> IPOs by FitBit, MindBody, Evolent Health, Teladoc, and Invitae created \$9 billion in market capitalization.<sup>2</sup> The trend seems to be continuing this year, as evidenced by IBM Watson Health's announcement that it is acquiring Truven Health Analytics for \$2.6 billion.<sup>3</sup>

Improvements in communications and information technology, the introduction of more sophisticated wearable sensors, at-home diagnostics and improved genomics capabilities, and the promise of additional sources of data and new abilities to interpret and understand large data sets should help the growth trend to continue.

At the same time, however, digital health companies may not be immune from the current bear market conditions. Indeed, a number of digital health companies have suffered from post-IPO degenerative conditions evidenced by declining value and underperformance when measured against benchmarks such as the S&P 500. For example, venture-backed IPOs such as Vocera, Imprivata, Everyday Health, and Accretive Health all underperformed against the S&P 500 following their IPOs.<sup>4</sup>

Moreover, many digital health product developers lack a clear understanding of the health care market and the regulatory issues that impact success. Complex regulations and guidance govern digital products generally, at the same time that a different complex regulatory landscape governs health care-related products. Digital health businesses will fall under both sets of regulatory requirements. Accordingly, business and marketing strategies will be more or less successful depending upon the legal requirements that affect the product or the company that makes or markets the product and depending upon how well the company factors those requirements into its technology and business plans.

The conflicting financial trends, coupled with the complex regulatory environment, underscore the need for investors to take care when considering M&A and venture capital financing opportunities in the digital health space. In conducting due diligence for digital health companies, it is important to look not only at the company, but to consider the company, the product, and its business strategy in light of the regulatory environment and the health care market.

The need for caution calls for a prescription of sound business and legal due diligence—with the two often overlapping in the world of digital health. While there is no one-size-fits-all approach to due diligence, here are ten topics specific to digital health companies that should be part of a thorough legal due diligence review of any M&A or investment opportunity in this arena.

## 1. Payment Opportunities

Investors in digital health will want to understand the target company's plan to monetize its products. Accordingly, any investor will want to thoroughly understand how consumers and other product users pay for the product, whether by purchase or license of the technology. Moreover, the success or failure of a digital health company often depends on whether use of the company's products will be reimbursed by governmental and/or private payers. While many digital health tools are marketed to consumers for fitness and wellness, a growing number of digital health tools are capable of supporting clinical and treatment discussions and deci-

### Volunteer for the Governance AG

The Governance AG always is seeking volunteers to write for our publications, particularly email alerts, Executive Summaries, and Member Briefings. This is a great opportunity for you and your firm/organization to share knowledge and enhance your national profile. If you are interested in authoring a publication, please contact Governance AG co-chairs John Garver at [jgarver@robinsonbradshaw.com](mailto:jgarver@robinsonbradshaw.com) or Matthew Roberts at [mroberts@nexenpruet.com](mailto:mroberts@nexenpruet.com).

sions. Federal health care programs and commercial payers are developing new ways to pay for care, including growing requirements for consumer engagement and provider quality standards. Future regulations may pose opportunities to market products to health care providers to help them meet requirements for reimbursement for patient monitoring or related activities. Other laws may impact a company's marketing approach by limiting its ability to provide a product in exchange for referrals.<sup>5</sup> An investor should understand whether the target's products meet the relevant requirements for payment and whether its business model is consistent with federal health care laws and regulations.

## 2. Impact of Product Design and Functionality on Regulatory Requirements

It is not always clear which regulator(s) and regulation(s) govern particular digital health tools. Digital health tools may be consumer products within the jurisdiction of the Consumer Product Safety Commission (CPSC) or they may be medical devices subject to U.S. Food and Drug Administration (FDA) oversight. Advertising that includes claims of medical benefits can move the product from the jurisdiction of the CPSC into the FDA's purview in overseeing the safety of medical devices. The FDA has issued guidance regarding which mobile medical applications and health information technology are considered medical devices and, if they are, whether they will require oversight and prior approval or whether the FDA will exercise enforcement discretion.<sup>6</sup> Moreover, a product launched today may have very different functionality down the road as new software and functionalities are added—so preapproval may be required before new functionalities are added to existing technology. Both compliance and non-compliance come with real costs. It is, therefore, important to determine the appropriate regulatory framework and to assess the target's compliance prior to finalizing a transaction.

### Share Your Knowledge and Enhance Your Personal Brand!

The BLG PG seeks attorneys to share their knowledge with the PG by writing email alerts and/or recording podcasts on hot business law and governance topics. Email alerts are short summaries of newsworthy developments in the area of health care business law and governance. Podcasts are brief, audio-only recordings (usually no more than 10 minutes long) that the BLG PG makes available on its webpage. Podcasts are intended to be a learning tool on a discrete substantive topic, often at an introductory level. These opportunities provide you with a great chance to showcase and share your expertise. Please contact Vice Chair of Research and Website Jeff Kapp at [jlkapp@jonesday.com](mailto:jlkapp@jonesday.com) or (216) 586-7230 if you are interested.

## 3. Design for Safety

A thorough due diligence review should consider whether the target has designed its digital health tools with an eye towards consumer safety. Like other consumer goods, digital health tools must be safe for consumer use and comply with product safety laws and regulation or FDA requirements for safety and effectiveness.<sup>7</sup> Companies marketing digital health tools to children should be especially mindful of rules specifically applicable to children's products (such as CPSC requirements regarding testing and certification of compliance with lead levels and the need for tracking labels).<sup>8</sup> Safety design should take into account how the interconnectivity of devices could make digital health tools more susceptible to compromise by third parties, such as someone hacking into a medical device to change the settings on a pacemaker or altering data that is used for decision support.

## 4. Interoperability with Other Data

Much of the value of the data available through digital health tools comes from the ability to connect the data with other data sources, including lifestyle data and clinical data, and to analyze that data. There are federally adopted standards and interoperability guidance for clinical data and financial and administrative data, which may be required or optional.<sup>9</sup> For interoperable medical devices, these include FDA-issued guidance regarding design, security, and risk management considerations as well as verification, validation, and labeling.<sup>10</sup> Depending on the product, assessing the target's use of standards to support health care providers, understanding the target's strategy for interoperating with other products and services, and evaluating compliance with federal guidance may be key components of an evaluation of a digital health company and the viability of its products.

## 5. Design for Privacy and Security

Information captured by digital health tools may be covered by various federal and state (and potentially even foreign) privacy laws that specifically relate to health care and other

### Looking to Build a Name for Yourself or Share Your Expertise?

The BLG PG seeks speakers to present on one of our monthly educational calls to our members on a health care business law, transactional, or governance topic. The months of September, October, November, and December 2016 are open and available for presentations. Is there a topic on which you would like to present, but just need the right forum? We can provide that forum. Contact Vice Chair of Educational Programs Carolyn Metnick at [carolyn.metnick@akerman.com](mailto:carolyn.metnick@akerman.com) or (312) 634-5719 for more information.

personal information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) limits the use and disclosure of information and includes requirements for policies and procedures to protect the confidentiality, integrity, and availability of information.<sup>11</sup> Technology targeted toward, or that may collect information about, children, may fall under the Children's Online Privacy Protection Act of 1998, which governs the collection of data from children and includes requirements for privacy policy content, for parental consent, and for the protection of children's online privacy and safety, including marketing restrictions.<sup>12</sup> The Federal Trade Commission (FTC) also protects consumer privacy and has encouraged a "privacy by design" approach to build privacy protections into products at the outset, including minimizing the collection and storage of data where practicable and training employees on the importance of security.<sup>13</sup> The FDA and FTC also have made recommendations to companies seeking to release internet-connected medical devices and other products.<sup>14</sup> It will be important to assess how the company interacts with the health care system and whether the company is operating on behalf of health care providers, health plans, or consumers in order to understand how HIPAA's (and other similar) limitations and requirements apply to the target and its digital health tools. It also is important to review how data is used and disclosed, as this impacts the application of HIPAA and other requirements. State laws in California, Florida, and several other states require companies to take reasonable measures to protect and secure health care data,<sup>15</sup> and almost every state now has some form of breach notification law targeting personal information.<sup>16</sup> In addition, if the target has global aspirations, it is important to consider whether the target has designed its product to comply with international privacy, data security, and data transfer requirements in the European Union and elsewhere, which may be even more stringent than those applicable exclusively within the United States.

## 6. Security and Breach Mitigation

As no product can be hack-proof and security breaches can have significant economic and reputational consequences for a target, it is important to assess whether the target has developed an appropriate HIPAA Security Rule<sup>17</sup> risk assessment process and has implemented reasonable measures to protect the data that it collects, stores, and transmits, including by using a belt-and-suspenders approach that provides layers of security. An investor also should review the target's preparedness to respond to a security incident, including by examining the tools and processes that the target has developed to identify, investigate, mitigate, remediate, and (if necessary) notify individuals and third parties regarding a security incident. In addition to understanding the physical, technical, and policy approaches the target has deployed to reduce the impact of any security breach, the investor will want to understand whether appropriate contractual measures are in place to deal with a security inci-

dent. Insurance is another key piece of the risk management strategy, and it is important to assess whether the target has adequate cyber liability and other coverage.

## 7. FCC Equipment Authorization

In addition to considering the applicability of FDA requirements, digital health tools must meet Federal Communications Commission (FCC) regulations. The FCC has three different authorization schemes for wireless devices to prevent interference—verification, declaration of conformity, and certification.<sup>18</sup> An investor should consider whether the target has familiarized itself and complied with these requirements.

## 8. Accurate and Truthful Advertisements

Under both federal and state law, fair advertising principles apply to the labels affixed to products, the claims made on a website, the advertisements and brochures, and the claims sales representatives make.<sup>19</sup> A due diligence investigation should include a review of the target's advertising claims, particularly in the area of health and wellness, where the FTC has been very vigilant in protecting consumers from fraud.<sup>20</sup>

## 9. Intellectual Property Rights

When developing new products, companies must protect their inventions from disclosure to preserve their products' novelty and eligibility for patent protection. Numerous cases for patent infringement have been filed after the launch of wearable technology inventions such as smart shirts, location-aware fitness training, and systems for medical monitoring and treatment.<sup>21</sup> Accordingly, it is important to assess how well the target has taken care not to violate third-party intellectual property rights and to protect its own valuable intellectual property.

## 10. Consider License and Service Agreements

Investors should carefully review the target's contracts to consider how well it has used licensing and service agreements to ensure compliance with government expectations, to limit the likelihood of disputes over intellectual property rights, and to allocate risks related to safety or security issues that may arise after a product's launch.

Each target and its digital health tools have unique issues and business relationships that should be assessed, and due diligence regarding digital health issues should be integrated into

### Come Tweet With Us!

The BLG PG seeks volunteers to provide content for the PG's Twitter feed. You'll rotate tweeting with other volunteers without overburdening your busy schedule. No prior Twitter experience is required. Contact Social Media Coordinator Reema Sultan at [reema.sultan@rivkin.com](mailto:reema.sultan@rivkin.com) or (516) 357-3295 to sign up.



an overall comprehensive due diligence review appropriate for the transaction, but this checklist provides a good start. Due diligence and proper management of these issues will help ensure that investment decisions are made with transparency and increased comfort regarding the opportunities and risks that the target and its digital health products present.

*\*The authors are partners in the Washington, DC office of Crowell & Moring LLP. They extend their appreciation for assistance with this article to their Crowell & Moring LLP colleagues Cheryl A. Falvey (Co-Chair, Advertising & Product Risk Management Group), Catherine A. Barach, and Danielle Rowan.*

- 1 Wang, King, Perman, Tecco, Rock Health Digital Health Funding: 2015 Year in Review, <http://rockhealth.com/reports/digital-health-funding-2015-year-in-review/>.
- 2 *Id.* (2015 performance data collected from NASDAQ and Google Finance as of market close on December 8, 2015; 2016 IPO outlook based on Rock Health survey of Rock Weekly readers).
- 3 News Release, IBM, IBM Watson Health Announces Plans to Acquire Truven Health Analytics for \$2.6B, Extending Its Leadership in Value-Based Care Solutions (Feb. 18, 2016), available at [www-03.ibm.com/press/us/en/pressrelease/49132.wss](http://www-03.ibm.com/press/us/en/pressrelease/49132.wss).
- 4 Zina Moukheiber, *Digital Health IPOs Continue to Disappoint*, Forbes Pharma & Healthcare (Nov. 25, 2014), available at <http://www.forbes.com/sites/zinamoukheiber/2014/11/25/digital-health-ipos-continue-to-disappoint/#2e34f383793e>.
- 5 *See, e.g.*, 42 U.S.C. § 1320a-7b.
- 6 *See* U.S. Food and Drug Administration, Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff (Feb. 9, 2015), available at [www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf](http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf).
- 7 *See Id.*; FDA, Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices (Feb. 9, 2015).
- 8 *See* 16 C.F.R. 200; *See also* Consumer Product Safety Improvement Act of 2008, Section 101, 15 U.S.C. § 1278a (Pub.L.110-34, 112 Stat. 3017-3022, enacted Aug. 14, 2008).
- 9 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, 80 Fed. Reg. 200 (Oct. 16, 2015); Office of the National Coordinator for Health IT, 2016 Interoperability Standards Advisory.

- 10 U.S. Food and Drug Administration, Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff (Jan. 26, 2016), available at [www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf).
- 11 *See* 45 C.F.R. 160, et. seq. (HIPAA).
- 12 Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506 (Pub.L. 105-277, 112 Stat. 2681-728, enacted Oct. 21, 1998).
- 13 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (Mar. 2012).
- 14 *See* U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff (Jan. 22, 2016), available at [www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf); FTC Staff Report, Internet of Things: Privacy & Security in a Connected World (Jan. 2015).
- 15 *See, e.g.*, Cal. Civil Code § 1798.81.5; Florida Information Protection Act of 2014 (Fla. Stat. § 501.171).
- 16 *See, e.g.*, Mo. Rev. Stat. § 407.1500 (2009); N.H. Rev. Stat. Ann. §§ 359-C:19-C:21, 358-A:4 (2006).
- 17 45 C.F.R. 160.302, et. seq.
- 18 *See* Federal Communications Commission, Equipment Authorization, available at [www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization](http://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization).
- 19 16 C.F.R. 500-503 (Fair Packaging and Labeling Act of 1967).
- 20 *See, e.g.* FTC cases challenging supplements and food advertising. Over the last decade, the FTC has filed 120 cases challenging health claims made for supplements. Meanwhile, in recent years there has been a trend in food advertising toward making unproven claims that eating certain foods can improve health and even reduce the risk of serious illnesses such as prostate cancer and heart disease.
- 21 *E.g.*, U.S. Patent Nos. 6,381,482 and 6,970,731 for wearable technology at issue in *Sarvint Technologies Inc. v. Textronics Inc. et al.*, No. 15-cv-00073 (N.D. Ga.).

## Questions About BLG PG Membership or Benefits?

Want to know how you can receive all of the great benefits of BLG PG membership? Who does what at the BLG PG? How to get involved? That's easy. Please contact Vice Chair of Membership Glenn Prives at [gprives@mdmc-law.com](mailto:gprives@mdmc-law.com) or (973) 425-4179.