Six Things to Know About the MedTech Landscape in 2019
On March 5, 2019, BakerHostetler presented a CLE seminar in Princeton, N.J., focusing on key issues in the medical technology industry, including venture capital investment, patent portfolios and post-grant proceedings, the volatile political landscape, data privacy and blockchain technology. Here are some important takeaways from this timely presentation.

**Trends in Venture MedTech Investing**

*Presenter: Tom Gordon, Managing Director for Silicon Valley Bank*

Venture fundraising for the healthcare industry is on a four-year upward trend, reaching a record $9.6 billion in 2018. Quick biopharma exits, and high IPO mark-ups drove accelerated healthcare fundraising. A swell in biopharma deals and round sizes over the past two years highlights the continued appetite for venture funding in the sector.

A healthy pipeline of exciting private companies, excellent biopharma and device exit numbers, and high-performing IPOs in the diagnostics/tools sector indicates continued robust venture fundraising through 2019. However, the totals will be more in line with the 2016-17 numbers, around $8 billion.

Silicon Valley Bank anticipates total U.S. venture fundraising for life science companies to continue at a healthy pace, with established funds likely to be joined by new spinout funds anchored by established investors. In addition, tech firms may raise life science-only sister funds.

The Top 15 crossover investment in venture-backed companies could soften by 25 percent or more, leading to biopharma investments decreasing to more closely match 2017 numbers.

The biotech IPO pipeline is strong, but market uncertainty could drag IPOs down to 30 to 35 deals and moderately reduce pre-money valuations and dollars raised. As a result, Silicon Valley Bank expects an increase in private biopharma M&As.

The device investment sector is expected to be stable with additional growth in Series A. A strong performing group of later-stage, venture-backed companies shows promise for up to eight device IPO opportunities in 2019. Little change is expected in device M&A activity from 2018.

**Valuation Based on Patent Portfolio**

*Presenter: Hussein Akhavannik, Partner, BakerHostetler*

Using 10 years of data, Akhavannik compared the valuation at time of exit for U.S. medical device and pharma companies with the number of patent families for each sector. He noted that in the early stages of investment, the number of patent families averages between six and nine for medical device companies and between four and five for pharma companies. Consistently, med device companies tend to patent more aspects of their inventions than the pharma companies do.
In middle stages of funding, there is a noticeable jump. By the time funding reaches the $100 million mark, the patent family numbers are in the mid-30s for medical device companies and about 22 for pharma. The numbers flatten out a bit as investors pull back to assess but move higher at the $500 million to $1 billion level.

Akhavannik then compared patent portfolio size based on transaction type, moving from seed round funding through M&A or LBO, noting that in 2018 there were 68 exits, as compared to 45 in 2017.

Ferguson’s observations include:

- The medtech industry has largely succeeded in avoiding the significant scrutiny from Congress and federal agencies that has been leveled at drug companies. However, that may be changing as Democrats assume control of the House. Over the years, Republicans had focused on improving the transparency of FDA processes, and fees were increased in exchange for better communication and a faster review process.

- Rep. Elijah Cummings (D-Md.) is now chairman of the House Committee on Oversight and Reform, and it appears that the Democrat agenda will expand to include medtech in addition to its already active investigation into drug pricing. In the wake of the 2016 election, the drug and medtech industry lost two of its biggest champions – Sen. Orrin Hatch, who retired, and Rep. Erik Paulsen (R-Minn.), who was not re-elected.

As regulatory risks, Ferguson listed:

- Potential scrutiny of the 510(k) approval process for medtech and whether relations between the agencies and companies seeking approval are too cozy. A recent coordinated effort by investigative journalists has made this easy fodder for a possible congressional investigation.

- Pre-market approval (PMA) reform and the threat of preemptive legislation.

- Post-market data collection.

However, significant FDA legislation is not expected in the next year as the 2020 election nears and Congress remains divided.

In the area of reimbursement payments, Ferguson said Medicare frequently is not nimble enough to keep pace with advances in medical technology and its reimbursement system is inadequately equipped to cover the cost of many new drugs and therapies. Addressing these disparities is a focus of the industry in addition to the medical device tax.

The top priority of the medtech industry is the medical device excise tax, which was packaged in the Affordable Care Act (ACA) to help cover its cost. The tax is currently suspended but is scheduled to return at the end of 2019. Industry advocates continue to press for its permanent repeal, and there are a number of legislative vehicles that could include such a repeal. However, it is also feared that repealing the tax could undermine the ACA, as it generates about $20 billion in tax revenue.
Post-Grant Proceedings: A Factor to Consider in Product/Patent Acquisitions

Presenters: David Farsiou, Partner, BakerHostetler, and John Murphy, Partner, BakerHostetler

When considering an investment involving patents, investors should value the asset, assess the strength of the intellectual property covering the asset and consider how, when and where the patents can be attacked.

The America Invents Act (AIA) introduced post-grant challenge proceedings in 2012. These place less burden on the challenger to prove unpatentability, requiring only a preponderance of evidence, and the number of such challenges has skyrocketed, as has the number of claims being invalidated. In 2013, Chief Judge Randall R. Rader of the U.S. Court of Appeals for the Federal Circuit, compared the judges on the Patent Trial and Appeal Board (PTAB) to “death squads killing property rights.” The phrase stuck and patent holders have been on the lookout for change in the process.

However, in 2018, Andrei Iancu, director of the U.S. Patent and Trademark Office (PTO), announced, “It is a new day at the PTAB” and this has been followed by procedural changes and new case law that have led to greater balance and more protections for patent owners.

Seven reasons the PTAB pendulum is swinging back:
- SAS Institute v. Iancu.
- Amendment rules.
- End of broadest reasonable interpretation (BRI).
- Patent owner response rights.
- Denial of successive petitions.
- Standing requirements.
- Estoppel enforcement.

Data Privacy for MedTech/Healthcare: Recent Happenings at the FTC, FDA and Office for Civil Rights

Presenter: Laura Jehl, Partner, BakerHostetler

There is a patchwork of privacy regulation that can or may affect the medtech industry, with responsibility splintered among several federal agencies, as well as state breach notification laws and international data protection regulations.

Health Insurance Portability and Accountability Act (HIPAA).

The main features of this well-known federal law:
- Applies to: Vendors of personal health records (PHRs), PHR-related entities, or third-party service providers for vendors of PHRs or PHR-related entities.
- Covers: Electronic health information on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.
- Definition of breach: The unauthorized acquisition of PHR-identifiable health information that is unsecured (unencrypted) and in a personal health record.
- Who must be notified: Any business that is a vendor of PHRs or a PHR-related entity must notify every affected U.S. citizen or resident, the FTC. and the media, if more than 500 residents of a single state are affected.
- Notification timeframe: Without unreasonable delay and in no case later than 60 calendar days after the breach is discovered.
- Preemption: The FTC’s Rule preempts contradictory state breach notification laws, but not those that impose additional – but non-contradictory – breach notification requirements.

A data breach is defined in the Final Rule as “acquisition, access, use or disclosure of unsecured protected health information in a manner not permitted under the HIPAA Privacy Rule. … unless the Covered Entity or Business Associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.”
Breach risk assessments must be documented and must be evaluated at least the following four factors:

- The nature and extent of the personal health information (PHI).
- The unauthorized person involved.
- Whether the PHI was actually acquired or viewed.
- Extent to which any risk has been mitigated.

Ransomware is estimated to have cost organizations around the world $5 billion in 2017, up 400 percent from 2016, and ransomware attacks occur daily. Healthcare organizations are particular targets.

- Hackers gain access to your computer’s file system by installing a program via a phishing link/attachment or by poorly configured Remote Desktop Protocol service.
- Ransomware prevents a user from accessing the operating system or encrypts all the data stored on the computer.
- The user asks the ransom to pay a fixed amount of money, as opposed to decrypting files or allowing access again to the operating system.

Best practices to avoid a ransomware attack include maintaining a robust, off-site data backup and properly configured Remote Desktop Protocol services.

Interplay between HIPAA and the Federal Trade Commission means a company may qualify under both laws if the vendor or business acts as a business associate under HIPAA but also offers personal health record services to the public at large.

**Federal Trade Commission**

Section 5(a) of the Federal Trade Commission Act provides:

- **Authority:** Section 5(a) authorizes the FTC to protect consumers by “prevent[ing] persons, partnerships, or corporations . . . from using unfair . . . acts or practices in or affecting commerce.”
- **Unfair practices:** An unfair practice is one that is grounded in well-established legal policy that causes or is likely to cause an unavoidable “substantial” injury to the consumer that is not outweighed by any countervailing benefits to consumers or competition.
- **Privacy context:** The FTC considers it “deceptive” when companies do not follow their privacy practices when handling consumer information, sell or disclose information without notice to consumers, and/or misrepresent participation in compliance programs.
- **Security context:** The FTC has also alleged deceptive practices when companies have failed to safeguard data that is considered private in nature or would cause monetary or other harm to consumers if exposed.

**FDA privacy enforcement activity**

- **Labeling:** Recent draft guidance recommends device manufacturers inform end-users of data security risks as a way to comply with the labeling requirements.
- **Memoranda of Understanding/Agreement:** The FDA entered into two new Memoranda of Understanding with multiple stakeholder groups to create information sharing analysis organizations (ISAOs) – MedISAO and Sensato-ISAO – to share emerging threats with the FDA. The FDA also entered into an Memorandum of Agreement with the Department of Homeland Security to share device threats and vulnerabilities.
Mobile apps as devices: The FDA published 2015 guidance that informs manufacturers, distributors and other entities about how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms. Certain mobile apps are now regulated as devices if the software provides patient-specific analysis or if they attach to a mobile platform and must meet the requirements of device classification.

Office of Inspector General (OIG)

In September 2018, the OIG released a report advising the FDA to use pre-submission meetings with manufacturers to address cybersecurity issues, include cybersecurity documentation as a criterion in the Refuse-to-Accept checklist, and add cybersecurity questions to the FDA Smart template.

When an incident happens, what do regulators expect from you?

- Transparency; no coverups.
- A prompt and thorough investigation.
- Good attitude and cooperation (commitment to compliance and safeguarding PHI).
- Appropriate and prompt notification.
- Corrective action (know the root cause and address it; staff training; awareness programs; technical safeguards; new policies/procedures/physical safeguards).
- Remediation and mitigation.

Blockchain for the Pharma and Life Sciences Industry

Presenters: Laura Jehl, Partner, and Robert Musiala, Counsel, BakerHostetler

A blockchain is a cryptographically secured transaction network and ledger that is shared among and verified by all computer nodes participating in a distributed system. Its characteristics include:

- Distributed network: Multiple independent computer nodes support the network and verify updates.
- Cryptography: The integrity of information stored on a blockchain is secured by public-private key cryptography.
- Immutability: Every transaction is linked to the previous transaction, making it (practically) impossible to alter network data.
- Disintermediation: The first three characteristics enable trusted peer-to-peer transactions without using a central authority (like a bank) as intermediary.

Bitcoin was the first widespread use of blockchain technology: however, “cryptocurrencies” need not have anything to do with currency, and blockchain technology can be engineered and implemented independently of the bitcoin blockchain.

Blockchain for enterprise

When multiple parties use the same dataset, blockchain may reduce costs, enhance security, and increase data accuracy and auditability. Blockchain may drive efficiencies in situations where multiple business entities:

- Rely on and update the same dataset.
- Mutually benefit from increased speed of updates.
- Desire independent verification of data updates.
- Want to save money by cutting out the data intermediary.
- Share an interest in automating certain transactions.

AWS, Microsoft Azure, Oracle and SAP all have launched solutions to support enterprise blockchains on their cloud service platforms.

As blockchain technology is deployed in business applications, there are two primary areas of cybersecurity concern:

- Wallet attacks: Hackers break into blockchain user wallets, allowing diversion of digital assets.
- 51% attack: By taking control of 51 percent or more of the network processing power, the attacker can manipulate the blockchain.
In addition, it is uncertain how immutable blockchain technology can be compliant with new privacy regulations in Europe, California and elsewhere. Antitrust concerns regarding blockchain also have arisen.

Notwithstanding these concerns, blockchain solutions for the pharmaceutical supply chain will likely be the first to gain market exposure, followed by applications to improve clinical trial data management. Applications for healthcare insurance and patient records will take much longer to develop.

The Drug Supply Chain Security Act (DSCSA) became law in 2013 and will be phased in over 10 years, beginning in 2019. It calls for an electronic system to track and trace certain prescription drugs in the U.S. as they move from manufacturers to distributors, healthcare providers, retailers and patients. Its key provisions include:

- **Product identification**: Manufacturers and repackagers must put a unique product identifier on certain prescription drug packages, for example, using a bar code that can be easily read electronically.
- **Product tracing**: Manufacturers, wholesaler drug distributors, repackagers and many dispensers (primarily pharmacies) in the drug supply chain provide information about a drug and who handled it each time it is sold in the U.S. market.
- **Product verification**: Manufacturers, wholesaler drug distributors, repackagers and many dispensers (primarily pharmacies) must establish systems and processes to be able to verify the product identifier on certain prescription drug packages.
- **Detection and response**: Manufacturers, wholesaler drug distributors, repackagers and many dispensers (primarily pharmacies) must quarantine and promptly investigate a drug that has been identified as suspect, meaning that it may be counterfeit, unapproved or potentially dangerous.
- **Notification**: Manufacturers, wholesaler drug distributors, repackagers and many dispensers (primarily pharmacies) must establish systems and processes to notify FDA and other stakeholders if an illegitimate drug is found.
- **Wholesaler licensing**: Wholesale drug distributors must report their licensing status and contact information to the FDA. This information will then be made available in a public database.
- **Third-party logistics provider licensing**: Third-party logistics providers, those who provide storage and logistical operations related to drug distribution, must obtain a state or federal license.

On Feb. 7, 2019, the FDA published a news release and an accompanying notice in the Federal Register announcing a DSCSA pilot project program and soliciting applications from industry to explore and evaluate methods to enhance the security of the pharmaceutical distribution supply chain.

On Oct. 2, 2018, the SAP Blockchain Consortium Program announced the formation of a blockchain industry consortium for the pharma and life sciences supply chain. In addition, nonprofit MediLedger is working to build a private permissioned blockchain for the pharma supply chain, created specifically to comply with the DSCSA.

In the clinical trial arena, several projects are underway to securely share health data, research, critical supplier information and more. The Center for Biomedical Blockchain Research, established to lead efforts within the Icahn School of Medicine at Mount Sinai, is currently affiliated with 153 active projects involving healthcare, biomedicine and open science.

It is important to consider the practical legal considerations of blockchain projects, including:

- Costs of hosting a private/permissioned blockchain.
- Establishing membership tiers and rights/responsibilities.
- Aligning interests in data standards and integrity.
- Regulatory risk.
- Implementing smart contracts applications.
- Renegotiating traditional contractual relationships.
- Managing new tech platforms in a consortium environment.
For more information about any of these topics, contact the BakerHostetler presenters.

Contacts

Hussein Akhavannik
hakhavannik@bakerlaw.com
+1.202.861.1642

David Farsiou
dfarsiou@bakerlaw.com
+1.215.564.8984

Michael Ferguson
mferguson@bakerlaw.com
+1.202.861.1663

Laura Jehl
ljehl@bakerlaw.com
+1.202.861.1588

John Murphy
johnmurphy@bakerlaw.com
+1.215.564.1603

Robert Musiala
rmusiala@bakerlaw.com
+1.312.416.8192


The Blockchain Monitor
https://www.theblockchainmonitor.com

Data Privacy Monitor
https://www.dataprivacymonitor.com/

IP Intelligence
https://www.ipintelligencereport.com/

Ohio Clock
https://www.ohioclock.com/

bakerlaw.com
Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation and Tax – the firm has more than 970 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.

Baker & Hostetler LLP publications inform our clients and friends of the firm about recent legal developments. This publication is for informational purposes only and does not constitute an opinion of Baker & Hostetler LLP. Do not rely on this publication without seeking legal counsel.

© 2019 BakerHostetler