Title: Breaking Barriers: Mastering FDA Regulations, National Security, and Tariffs to Expand Your MedTech Company to the U.S.

Full Article: *Note: members of our team will be on-site at the 2026 LSX World Congress in Lisbon, Portugal, March 24-26 and will be hosting a Medtech CEO Forum for C-suite executives and decision-makers of emerging MedTech companies in attendance. We've prepared this primer to outline some of what our team will be covering and provide a go-forward resource for these companies looking to expand their business operations into the U.S. Details on the CEO Forum can be found HERE, and our team would love to meet with you if you'll be at LSX.*

Given the United States' dominant position in the global life sciences market, expanding into the US is a strategic objective of paramount importance for many early-stage European life sciences companies. The U.S. pharmaceutical and medical devices markets were recently valued at over $600 billion and $180 billion, respectively, with projections suggesting that each of these markets could double in the next 5-8 years.

Expanding into the U.S. market offers substantial opportunities for growth and innovation. To successfully penetrate this lucrative market, startups must carefully assess their capital needs, determine the most appropriate form of funding and nature of potential investors, and establish a suitable legal framework for their expansion, whether through establishing a branch office, forming a subsidiary, or restructuring the company entirely via a "flip" or some other transaction structure.

Fundraising and Structural Concerns

Fundraising

Typically, early-stage companies finance their U.S. expansion using domestic capital sources. While raising funds from U.S.-based investors can be an effective strategy, it often involves certain implications, including potential corporate restructuring within the United States — either as a prerequisite for securing investment or to enhance their appeal to investors — given that U.S. investors generally prefer investing in U.S. entities due to familiarity with local legal and regulatory frameworks.

When considering venture capital financing, startups must evaluate the types of capital available, such as equity financing, convertible debt, or hybrid arrangements, as well as the nature of each potential investor and the strategic advantages or disadvantages that various investors bring to the table. In addition to comprehensively evaluating which approach aligns best with the company's strategic objectives and financial situation, companies must also consider which investors are amenable to the company's existing country of domestication/corporate structure, and which are going to require significant structural/governance overhaul prior to investment.

Corporate Structure

Foreign startups also have several options regarding the legal structure of their U.S. presence. The first option is establishing a branch office, which serves as an extension of the foreign entity

operating within the United States. A branch is not a separate legal entity and thus maintains a direct liability chain to the parent company. This approach is relatively simple and cost-effective, often viewed as an initial step toward full U.S. market entry. However, operating as a branch can present challenges in attracting talent, as U.S. companies are eligible for certain tax incentives that extend to employees and various forms of equity compensation. These incentives typically do not apply to employees holding foreign equity, potentially impacting the company's ability to compete for skilled personnel in the U.S. market. A branch also does not create any sort of U.S.-based investment target for potential investors, so the company's fundraising pool is limited to those investors with sufficient structural comfort and appetite to invest in foreign entities.

The second option is forming a U.S.-based subsidiary, which is a distinct legal entity under the laws of the United States that provides a layer of liability protection for the parent company. Although establishing a subsidiary involves higher costs and regulatory filings, it facilitates easier access to U.S. contracting, tax incentives, and local employment opportunities, while also helping to shield the foreign parent from liabilities specific to the U.S. business.

The third option, frequently employed by foreign entities looking to secure significant early funding from U.S. investors, involves a corporate restructuring known as a Delaware "flip." Typically driven by U.S.-based VC firms, this process entails establishing a U.S. entity to serve as the parent company and investment target and subsequently converting the original foreign entity into a subsidiary of the U.S. entity. This structure allows venture capitalists to hold equity directly in the U.S. parent company, which is governed by U.S. law — an aspect that often increases investor comfort and confidence. However, such a structure can be quite involved from a process perspective in both the U.S. and the jurisdiction of the company's original formation as it relates to existing third-party contracts, licenses and regulatory approvals, and additional structural machinations are often required in tandem with the flip transaction to help manage U.S. operational risk, including separate establishment of a U.S. operational subsidiary as noted above.

Managing IP Risk

Breaking into the U.S. market also requires a deliberate, U.S.-focused IP strategy, well before the first product is sold. The IP checklist for startups involves careful attention to both protecting innovation and avoiding third-party intellectual property risks.

IP Protection

IP protection can be critical for a startup to establish a foothold and compete in the U.S. market. Among other steps, a comprehensive strategy for protecting intellectual property includes

- carefully crafting enforceable patent claims and filing U.S. patent applications (or advancing through PCT to U.S. national phase) claiming your device's core structures, methods of use, and key manufacturing steps;
- pairing utility patent and design patent protection as appropriate; and
- locking down trade secrets such as manufacturing know-how, algorithms, and clinical data with tight confidentiality and employee controls.

Equally important are enforceable employment agreements that: 1) secure your company's ownership rights (through, e.g., assignments and work made for hire provisions) in the valuable intellectual property created by employees; and 2) require confidentiality regarding the company's valuable trade secrets and other proprietary information.

IP Enforcement

But protecting your inventions is only half the battle — selling in the U.S. brings significant IP enforcement exposure. Without freedom-to-operate clearance, you risk infringement suits, injunctions, and import exclusion orders that can abruptly halt sales and impose heavy damages or licensing costs. With respect to medical devices, regulatory filings and interactions with the FDA also create disclosure and trade-secret risks that must be coordinated with the prosecution strategy. These filings can also provide a public road map for third-party IP enforcement against your product, making it critical to work with counsel on such regulatory submissions. Moreover, U.S. patent infringement is expensive and burdensome, resulting in the requirement (through the discovery process) to exchange a substantially greater amount of confirmation and sensitive information as compared to litigation in other countries.

Regulatory Compliance & Enforcement

While expanding into the U.S. market presents significant opportunities for medical device companies, it also involves navigating a complex regulatory landscape. Understanding and complying with the Food and Drug Administration's (FDA) requirements is crucial for a successful market entry.

Regulatory Compliance

Medical device companies entering the U.S. market must determine whether their product qualifies as a medical device under U.S. law. The Food, Drug, and Cosmetic Act (FDCA) defines a medical device as any instrument, apparatus, implant, in vitro reagent, or similar article that is recognized in official pharmacopeias such as the U.S. Pharmacopeia or National Formulary, which is intended for use in diagnosing, curing, mitigating, treating, or preventing disease in humans or animals, or designed to affect the structure or function of the body of humans or animals. Importantly, the device's primary purpose must not be achieved through chemical action within or on the body, nor should it depend on being metabolized to accomplish its intended function. If a product is labeled, promoted, or used in a manner that aligns with this definition, it becomes subject to regulation by the FDA and may require premarket approval or notification before it can be marketed.

Having approvals or certifications in foreign markets does not automatically grant permission to sell products in the U.S., as the FDA's regulatory standards are specific and often more stringent. Companies must ensure their products fully comply with all applicable FDA regulations. For instance, before selling in the U.S., manufacturers are required to register their establishments and list their devices with the FDA. Additionally, they must classify their devices based on risk, which depends on the intended use and indications for use. This classification determines whether a premarket submission is necessary, with Class I devices generally being low risk and often exempt from premarket submission, Class II devices considered moderate risk requiring a

510(k) premarket notification demonstrating substantial equivalence to a legally marketed device, and Class III devices being high risk, typically necessitating a Premarket Approval (PMA) involving a rigorous review process, including clinical trials. For novel devices with no predicate, such as digital health innovations, the De Novo review process applies.

Manufacturers must also ensure their production processes comply with the FDA's Quality Management System Regulations (QMSRs), which are aligned with ISO 13485, governing the development, control, and monitoring of manufacturing to guarantee device safety and efficacy. Reporting adverse events and device malfunctions to the FDA is mandatory to support ongoing safety monitoring. Clear, compliant labeling — including instructions, warnings, and intended use—is essential to meet FDA standards. As digital health technologies evolve, cybersecurity has become a critical regulatory focus; the FDA now requires cybersecurity measures to be integrated into the design and maintenance of connected medical devices that handle sensitive data or connect to networks. Companies often need to implement robust cybersecurity protocols and may also seek insurance coverage to manage associated risks.

Logistical Considerations

Beyond regulatory compliance, entering the U.S. market involves logistical considerations such as navigating customs procedures, establishing reliable distribution channels, and designating a U.S.-based agent or representative. Companies must also develop systems for monitoring, reporting, and responding to adverse events, ensuring that contractual arrangements, particularly quality agreements with suppliers, distributors, and partners, meet FDA standards.

Enforcement & Litigation Risk

While the United States offers a lucrative market, it also presents notable regulatory risks. FDA regularly inspects and audits companies it regulates, and if the agency discovers any compliance issues, there is a risk of a warning letter and monetary penalties. Moreover, a manufacturer may have to recall their product to address a problem with a device that violates FDA law. Finally, the FDA has the power to issue injunctions to stop companies from violating the FDCA. Compared to the EU, where the regulatory process can be more streamlined, the U.S. system is often viewed as more rigorous and enforcement-oriented, necessitating diligent compliance and proactive risk management.

Liability and litigation risks are also significant considerations for medical device companies entering the U.S. market. To mitigate these risks, companies often establish well-capitalized corporate entities, implement comprehensive insurance coverage, and adopt rigorous quality and compliance protocols. Learning from industry best practices and legal counsel can help navigate the complex liability landscape.

Entering the U.S. market with a medical device requires careful planning, a thorough understanding of FDA regulations, and strategic risk management. While the regulatory environment can seem daunting, proactive compliance and operational readiness can pave the way for successful market entry and sustained growth in the United States.

The legal landscape governing U.S. national security considerations for pharmaceutical and biotechnology companies seeking market entry is complex and multifaceted. Companies must

navigate an array of statutes, regulations, and executive authorities that collectively serve to protect national interests, regulate foreign influence, and ensure compliance with U.S. policies on trade, security, and ethical conduct.

International Trade Relations & National Security Concerns

Tariffs and Trade Laws Post-IEEPA Ruling

Historically, tariffs have been a significant tool in U.S. economic and foreign policy, used to shape international trade relations and safeguard domestic industries. Under statutes such as the International Emergency Economic Powers Act (IEEPA), Presidents historically relied on broad statutory authority to impose tariffs during national emergencies, including sanctions on foreign goods or import restrictions. However, a recent Supreme Court decision clarified that IEEPA does not explicitly authorize the President to levy tariffs, thereby limiting the scope of executive power under this statute. The Court emphasized that Congress's intent, as evidenced by legislative history, was to delegate emergency powers primarily related to property control and financial transactions, not to tariff imposition. As a result, the President has promised to pursue alternative statutory authorities — such as the Trade Expansion Act or the Tariff Act — when implementing tariffs related to national security concerns. This shift introduces uncertainty into the tariff landscape, requiring companies to monitor evolving legal bases for import restrictions and potential new uses of existing statutes or future legislation to justify tariffs impacting the life sciences industry.

Committee on Foreign Investment in the United States (CFIUS)

A critical component of the U.S. national security framework is the Committee on Foreign Investment in the United States (CFIUS). CFIUS reviews certain foreign investments, acquisitions, and joint ventures to assess their potential impact on national security. For pharmaceutical and biotech companies, especially those engaged in critical or emerging technologies, CFIUS review can be a significant hurdle to entering the U.S. market. Transactions involving foreign entities that acquire control or certain access to critical technologies may be subject to mandatory filings and review processes. The scope of CFIUS has expanded over recent years to include investments in "critical technology," "critical infrastructure," and "sensitive personal data," with particular attention paid to sectors like biomedicine, pharmaceuticals, and life sciences. Companies must therefore conduct thorough due diligence, evaluate whether their transactions trigger CFIUS jurisdiction, and prepare for potential mitigation measures or rejection of investments deemed a security risk.

Foreign Corrupt Practices Act (FCPA)

Compliance with the Foreign Corrupt Practices Act (FCPA) remains a key legal obligation for companies operating internationally. The FCPA prohibits corrupt payments to foreign officials to obtain or retain business, emphasizing transparency and ethical conduct. For pharmaceutical and biotech firms, which often engage in licensing, collaborations, and distribution agreements abroad, strict adherence to FCPA provisions is essential. Violations can lead to severe penalties, including substantial fines, criminal charges, and reputational damage. Companies should implement robust internal compliance programs, conduct due diligence on foreign partners, and

establish clear policies against corrupt practices to mitigate risks associated with their international operations.

Sanctions and OFAC Regulations

The Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security objectives. Sanctions may target specific countries, regimes, individuals, or entities involved in activities deemed inconsistent with U.S. national security goals. These restrictions can prohibit or limit dealings with designated persons or jurisdictions, impacting the ability of foreign or domestic companies to operate in or access markets effectively. For biotech and pharmaceutical companies, OFAC compliance involves screening transactions, supply chains, and partnerships against the Specially Designated Nationals and Blocked Persons (SDN) list and other sanctions lists. Non-compliance can result in hefty fines, criminal charges, and loss of license to operate within the U.S. market.

Emerging Trends and Strategic Considerations

Pharmaceutical and biotech companies aiming to enter the U.S. market must adopt a comprehensive compliance strategy that considers the shifting legal terrain surrounding tariffs, foreign investment, sanctions, and ethical standards. Vigilance in monitoring legislative developments, engaging with regulatory counsel, and establishing strong internal governance are essential to navigating the intricate web of U.S. national security laws and safeguarding their operations against legal and reputational risks.

Buchanan has a team of corporate and venture capital, IP, FDA and regulatory, and international trade and national security attorneys ready to help early-stage international life sciences companies expand into the U.S. market.

Author(s)' Name(s), Title(s), and Email(s):

Adam Wicks	*412 562 8331*	adam.wicks@bipc.com
Christopher Blaszkowski	*302 552 4204*	christopher.blaszkowski@bipc.com
Jordan Yeagley	717 237 4822	jordan.yeagley@bipc.com
Marco Ramirez Torres	215 665 3827	marco.ramireztorres@bipc.com
Tina Hu-Rodgers	202 452 7308	tina.hu@bipc.com