Protecting Trade Secrets in the Life Sciences and Pharma Industry

8 Steps to Prevent Corporate Espionage and Theft

Protecting trade secrets in any business is critical, but the stakes are higher in life sciences and pharma. Given the high focus on innovation in the industry, corporate espionage can result in devastating financial and reputational damage – whether through external hacking or internal theft. It's your job to take steps to minimize threats that could come from disgruntled workers, departing employees, unscrupulous competitors, or even state-sponsored actors. By taking some proactive measures, you can safeguard proprietary information and prevent unauthorized access. Here are eight steps your business should implement to protect your trade secrets from espionage and theft.

Identify and Classify Trade Secrets

The first step in protecting trade secrets is both obvious and overlooked: knowing what your trade secrets are and labeling them accordingly. Not every piece of proprietary information will qualify. Generally in the life sciences industry, trade secrets include:

- Formulations, compounds, and process know-how
- Preclinical and clinical trial data
- Algorithms and diagnostic models
- Research protocols, IND strategies, and commercialization roadmaps
- Strategic business information like customer lists, marketing strategies, acquisition targets, and other confidential data that provides a competitive edge.

Once identified, classify your trade secrets based on their sensitivity and potential impact if exposed. Ensure they are explicitly marked as trade secrets.

Implement Strong Access Controls

Not everyone in your organization needs access to all of your information. Limiting access to trade secrets is essential in minimizing exposure risks. In fact, the most exploitable risks arise from internal oversharing. Your business should:

- Adopt a need-to-know policy, granting access only to employees and contractors who require it to perform their job functions – even within your research teams.
- Use secure file storage systems with encryption and multi-factor authentication (MFA).
- Restrict physical access to sensitive documents by using locked filing cabinets and controlled office areas.

Use Confidentiality and Non-Disclosure Agreements (NDAs)

NDAs are essential, but generic templates won't cut it in this industry. All of your employees, vendors, and business partners with access to confidential information should sign NDAs and confidentiality agreements. These legally binding contracts establish clear obligations to protect trade secrets and outline consequences for unauthorized disclosure. But make sure you tailor them to the industry and your organization, so they:

- Cover joint R&D, licensing negotiations, and cross-border data sharing
- Include non-reverse-engineering clauses
- Specify obligations that survive M&A activity, spinouts, or product divestitures

Establish Robust Employee Training Programs

Your research and medical teams are no doubt brilliant researchers, but that doesn't mean they understand data security. Make trade secret protection part of your culture. Regular training should emphasize:

- Recognizing phishing scams and social engineering tactics used to extract confidential information – and gear them towards your industry, using phishing drills where simulated emails pose as journal reviewers or grant agencies
- Best practices for handling sensitive data, including password management and secure communication
- The importance of reporting suspicious activity, whether internal or external
- Guidance on sharing research findings pre-publication or at conferences

Monitor and Restrict Data Transfers – Especially Offsite

Whether it's a lab laptop going home for weekend data crunching or files uploaded to a third-party AI model for analysis, data leakage is a real risk. To prevent unauthorized data leaks, you should:

- Ban the use of personal email accounts and cloud storage for business-related documents
- Use data loss prevention (DLP) software for key research and trial datasets to track and prevent unauthorized file transfers.
- Implement logging and monitoring tools to detect unusual access patterns or suspicious downloads – especially before major departures or partnership transitions.

Conduct Regular Security Audits

Periodic security audits help identify vulnerabilities before they can be exploited. But don't rely on general IT audits – you need reviews that understand your industry's nuances. Your business should:

- Review access logs to detect unauthorized attempts to access confidential files
- Test cybersecurity defenses against potential threats, including penetration testing
- Update security protocols based on evolving threats and regulatory requirements

Implement Strong Exit Procedures for Departing Employees

Employees leaving a company—whether voluntarily or involuntarily—pose a significant trade secret risk. The departure of a research lead, formulation chemist, or BD exec can trigger major risk. Life sciences companies must act fast when departures occur. To mitigate this danger:

- Conduct exit interviews to remind employees of their confidentiality obligations
- Immediately revoke access to company systems, including email, databases, and cloud storage – especially to lab management systems and ELNs
- Retrieve all company-issued devices and ensure your departing employee retains no proprietary information

Take Legal Action When Necessary

If a trade secret is misappropriated, you should act swiftly to mitigate damage. Whether it's a former employee uploading files to a competitor's server or a biotech partner violating a collaboration agreement, delay can mean irreparable loss. Your next moves may involve:

- Sending cease-and-desist letters
- Seeking an injunction to prevent further disclosure or use of the stolen information
- Pursuing legal claims under the Defend Trade Secrets Act (DTSA) or applicable state laws
- Coordinating with law enforcement if you suspect corporate espionage

If your life sciences or pharma company needs legal guidance on trade secret protection or enforcement, or if you have any questions, please contact us today.

James C. Fessenden
Partner
San Diego/Irvine
858.597.9600/949.851.2424
jfessenden@fisherphillips.com

Brandon Kahoush
Partner
San Francisco
415.490.9034
bkahoush@fisherphillips.com