

Seyfarth

Protecting Life Sciences Trade Secrets: From Development to the AI Era

November 5, 2026

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal or expert opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Speakers



Tricia Macaluso
Partner
Dallas



Puya Partow-Navid
Partner
Los Angeles



Francis Wilson
Associate
Washington, DC

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential



Agenda

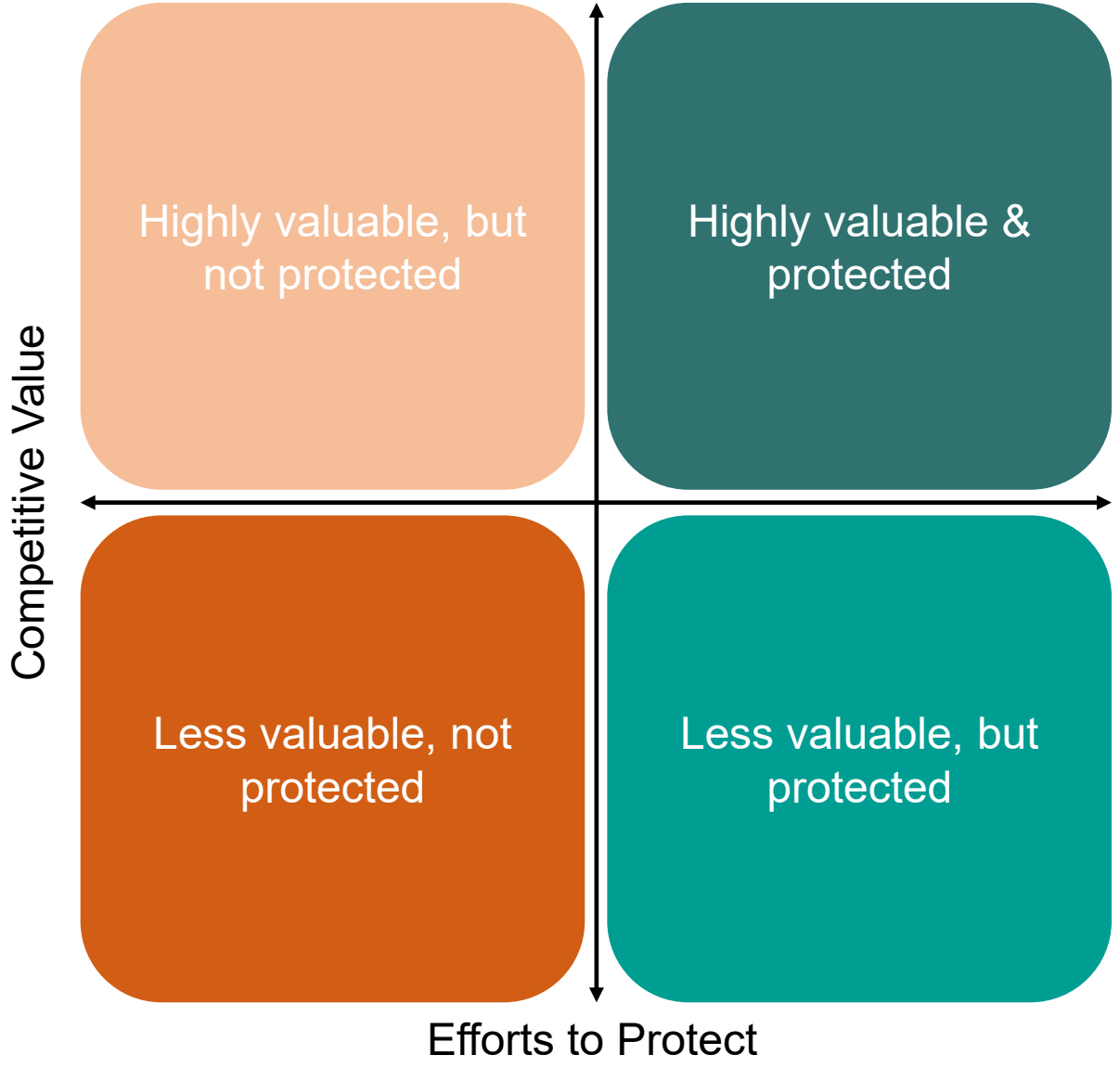
1. What is a trade secret?
2. Information that is/is not protectible as a trade secret
3. Best practices to establish *existence* of trade secrets
4. Best practices to establish *reasonable protection* of trade secrets
5. Trade secrets in the AI era
6. Responding to suspected misappropriation

What is a trade secret?

- **Applicable statutes:**
  - Defend Trade Secrets Act, 18 U.S.C. § 1839
  - State equivalents (Uniform Trade Secrets Act)
- **Requirements (DTSA):**
  - Financial, business, scientific, technical, economic, or engineering information;
    - Whether tangible or intangible
    - Whether stored/compilated physically, electronically, graphically, photographically, or in writing
  - **Owned** by the entity asserting trade secret protection;
    - Legal/equitable title
    - License
  - **Reasonable measures** to keep information **secret**; and
  - Derives **independent economic value** from not being generally known to, and not being readily ascertainable through proper means by, competitors
  - **UTSA** requirements largely the same, but no ownership requirement

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Protectability is a spectrum, not a label



©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

What types of information are protectable?

- Protectability and typical method of protection (*patent*, trade secret, unprotected/public) depends on what information is most competitively sensitive, which itself depends on the specific sub-industry

Life Sciences			
Sub-industry	**Medical Devices**	**Pharma**	**Testing/diagnostics**
Most mission-critical information	• *Product development* • Clinical trial data, efficacy, safety profiles • Customer information (identities, contact info, preferences, historical/projected sales volume) • Pricing • Marketing strategy • Product feedback • Competitive intel	• *Drug development* • Clinical trial data, efficacy, safety profiles • *Manufacturing processes* • Customer information (identities, contact info, preferences, historical/projected sales volume) • Pricing • Marketing strategy (wholesalers, insurance providers/PBMs, physicians/clinics/hospitals, patients) • Competitive intel	• *Test development* • Algorithm development • Clinical trial data, efficacy, sensitivity • Physician/clinic/hospital historical/projected patient volume • Marketing strategy • Competitive intel

- Two most common areas for trade secret disputes: **product development** and **product sales**

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Product development trade secret considerations

- Trade secret protection may only be available until patents filed, but still critical to protect during development
- Typical trade secrets:
  - Novel technologies, techniques, algorithms
  - Unique manufacturing processes
  - Product feedback, know-how, negative know-how
  - Go-to-market strategy, timelines
  - Competitive intel
- Unique considerations:
  - Broad (sometimes worldwide) market impact, unlike narrow geographic territories for salespeople
  - For clinical data, much more subject to potential waiver of putative trade secret protection because of mandatory reporting requirements
  - Critical that trade secrets are protected internally and **across the entire supply chain**
  - Primarily internally-created information

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Product sales trade secret considerations

- Typical trade secrets:
  - Customer information/feedback/preferences
  - Product feedback, know-how, negative know-how
  - Competitive intel
  - Pricing/contractual information
  - Market analyses
- Unique considerations:
  - Sales often relationship-driven, so competitive value often limited to particular territory/accounts
  - Primarily concern information gathered from external sources (feedback from customers/patients)
  - Focus on trade secret protection internally and with customers
  - Tradeoff: operational efficiency vs. documenting customer-related information learned in field
  - Often less stringent requirements regarding collection/storage
  - Misappropriation via knowledge/inevitable disclosure more viable as a legal theory
  - Salespeople are salespeople…

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

What types of information are protectable?

- Key focus: “Independent economic value” by reason of its secrecy
  - What does this mean?
    - Depends on jurisdiction
      - Some require substantial investment in time or money to develop/maintain
      - Continuum: Information in employee’s head → Information documented in emails → Information compiled into reports/CRMs/repositories
  - Other important considerations:
    - Timing: Is my trade secret “stale?”
    - How “secret” is the information truly?
    - Proof?
      - Time/cost for you to develop that trade secret
      - Value derived specifically from fact that it is secret
      - Barriers to entry for competitors
      - Competitors’ ability to expedite development of trade secret/enter market

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Patent or trade secret?

- If non-provisional patent filed, information loses trade secret status
- Ask yourself:
  - Is information patentable?
    - Product design
    - Product formulas (unless required to be publicly disclosed)
    - Proprietary manufacturing processes/techniques
  - Information likely to be publicly disclosed/beneficial to publish?
  - How long do you need protection?
    - Provisional (1 year)
    - Utility (20 years)
    - Design (15 years)
  - Ancillary protections from patenting important?
  - Where do you need protection (domestic vs international)?
  - Reverse-engineering risk?
  - Future applications of technology?
  - Can you detect infringement?



"To patent, or not to patent, that is the question."
- Prince Hamlet (probably)

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Patent or trade secret?

- When should you patent?
  - Provisional filing preserves flexibility during development
  - Benefit/necessity of public disclosure?
    - Marketing
    - Clinical trial recruitment
    - Required regulatory disclosure
  - Key disclosure/commercialization triggers?
- What should you patent?
  - Not all-or-nothing decision
  - Evaluate on a component-by-component basis
    - Same for manufacturing processes
- Other considerations
  - File non-provisional patent?
  - Risk if non-provisional patent not granted?



"To patent, or not to patent, that is the question."
- Prince Hamlet (probably)

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

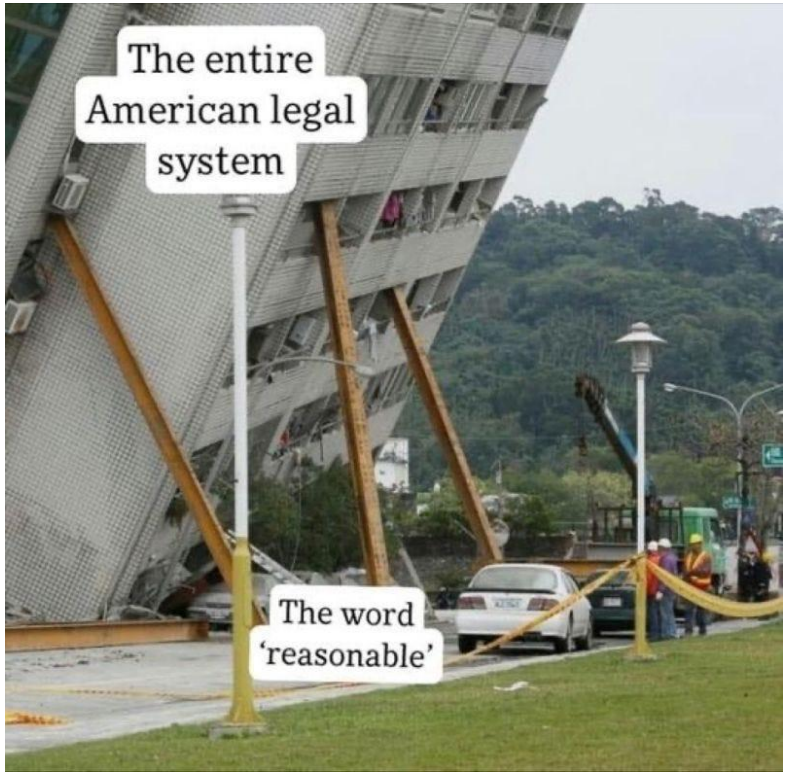
Best practices to establish existence of trade secrets

- Clear definition of what information company considers a trade secret
  - Distinguish true trade secrets from generalized market know-how
- Clear, repeated, and consistent messaging/training for all relevant stakeholders:
  - What information is considered a trade secret
  - Policies/procedures for documenting, handling, and protecting trade secrets
- The more trade secrets are documented, the stronger they become
  - Can convert disparate pieces of public information (not protectible) into protectible asset
  - Can assist with knowledge management
  - Reduction to tangible form allows company to:
    - Manage and track access,
    - Identify attempted exfiltration,
    - Prove ownership,
    - Prove exfiltration

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

“Reasonable” measures to protect secrecy

- Even if certain information is potentially protectable, you must demonstrate you undertook **reasonable measures** to protect its secrecy
- **<u>What is “reasonable?”</u>**
  - Fact-intensive determination
    - What specific trade secret?
    - How is trade secret stored?
    - Operational needs to access it?
    - What protections available? What protections utilized?
    - Consistency in utilizing protections?
    - Cost of prophylactic controls compared to operating budget?
    - Responses to data breaches/potential disclosures involving trade secret?



©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

“Reasonable” measures to protect secrecy

- Probably the single most important element to establish existence of trade secret
- Multi-faceted approach, no single item sufficient alone:
  - Prophylactic controls:
    - Physical access controls
    - Electronic access controls – **need-to-know**
    - Policies/procedures – confidentiality, document handling, offboarding
    - Employee/manager training
    - Cybersecurity
      - Encryption, audits, vulnerability assessments, incident monitoring
    - Data collection/retention
      - Web history, electronic data transfers, external device activity logs, account/device activity logs, etc.
    - Document marking (“Internal distribution only,” “Proprietary,” “Confidential,” etc.)
  - Contractual protections:
    - Employee contracts – confidentiality agreements, restrictive covenants, return/destroy, etc.
    - Customer contracts – ownership, data rights, restrictions on third-party disclosure (especially important for pricing)
    - Third-party contracts with suppliers, vendors, contractors, distributors, insurers, PBMs, etc. – confidentiality, NDA, ownership, data rights
  - Response to threatened/actual disclosure:
    - Historical efforts to go after violators (trade secret misappropriation, restrictive covenant/confidentiality breaches)
    - Timely challenges to FOIA requests
    - Proper marking of trade secret information required to be reported to government (e.g., adverse event reports to FDA)
    - Evidence preservation

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Proving reasonable measures to protect trade secrets

- It is one thing to draft a policy. It is another to implement that policy. It is yet another to prove execution of that policy.
- Ask yourself: “Could I prove reasonable measures if called to testify tomorrow?”
  - **Information governance**: administrators, how access privileges are managed, exceptions
  - **Information access**: strict need-to-know basis, MFA
  - **Data movement**: which devices/accounts permissible for what purposes, external media, personal email, access to personal cloud accounts from company devices, controls on uploading/sending sensitive information
  - **People**: acknowledgement of policies, documented periodic training, offboarding procedures
  - **Third parties**: contractual protections, InfoSec/Privacy requirements/audits, record retention

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Proving reasonable measures to protect trade secrets

- Documentation of reasonable measures:
  - Policies in effect at relevant times
  - Systems access permission rosters and audit logs
  - Monitoring for potential exfiltration
  - SOPs for high-risk incidents (e.g., mass data exports, leaving to join direct competitor in identical role)
  - Configuration of data and metadata retention requirements
  - Training records
  - Forensic evidence from devices/accounts/cloud storage spaces, such as emails, activity logs, SharePoint/OneDrive/Google Drive/Salesforce activity logs, document version histories, chat records, browser history, VPN/IP access records, call logs, etc.
  - Offboarding activities (affirmation of ongoing obligations, certification property returned/destroyed, exit interviews, etc.)
  - **Witnesses who can explain actual operations and practices**

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

AI use and loss of secrecy

- AI has plenty of operational benefits, but is laden with risks
- Allow access to public AI tools or only closed-system/enterprise AI tools?
- **Public AI tools**:
  - Higher secrecy + retention risk
  - Personal accounts often used
  - Weak administrative control
  - Limited ability to control retention/ preservation/deletion of AI chat logs
  - Disclosure of trade secret information could eliminate trade secret protection entirely
    - Potential HIPAA risk
- **Enterprise AI tools**:
  - Lower risk, with the right terms and configuration
  - Closed system = no inadvertent public disclosure of sensitive information
  - Negotiated confidentiality terms with vendors
  - More ability to control retention/ preservation/deletion of AI chat logs
  - SSO, role-based access and admin controls
  - Audit logs and export capabilities

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

AI use and discovery

- Treat AI interactions, policies, and controls as discoverable ESI in litigation
  - Prompts, outputs, logs, uploaded files, exported files, model interactions, etc.
- Relevant to “reasonable measures to protect trade secrets” analysis
- Questions to assess at the outset:
  - What tools did policies allow to be used, and for what purposes?
  - Which tools were actually used, and for what purposes?
  - What contractual/technical protections applied to those AI tools?
- Important that Legal, IT, InfoSec, Privacy, and operational employees/management well-trained and aligned on AI policies
- Key takeaways:
  - Policies and actual practice both matter
  - Do not allow employees to put something into an AI bot that you would not be comfortable explaining later to a judge in discovery

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

AI use and discovery

- If not careful, AI use can potentially destroy attorney-client or work product privilege
  - Split in authority:
    - *U.S. v. Heppner*, 820 F.Supp.3d 292 (S.D.N.Y. 2026) (defendant's communications with public Claude AI tool not protected by attorney-client privilege or work product doctrine)
    - *Warner v. Gilbarco, Inc.*, 820 F.Supp.3d 629 (E.D. Mich. 2026) (*pro se* chat prompts/outputs with ChatGPT not discoverable pursuant to work product doctrine)
    - *In re: OpenAI, Inc. Copyright Infringement Litigation*, 25-md-3143, 2026 WL 21676 (S.D.N.Y. Jan. 5, 2026) (compelling OpenAI to turn over sample of 20 million de-identified ChatGPT logs in copyright fair use dispute)

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Protective orders and AI use

- Do “reasonable measures” include ensuring that trade secrets, disclosed during discovery, are not input *by the opposing party or its attorneys*, into public AI tools?
  - Best practice: Include language in blanket protective orders setting parameters for when confidential documents produced in discovery can be uploaded to AI tools
  - *See Morgan v. V2X, Inc.*, No. 25-cv-01991, 2026 WL 864223 (D. Colo. Mar. 30, 2026) (granting motion to amend protective order to add language prohibiting uploading confidential information to AI tools if it could be used to train such tools)

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Responding to potential trade secret misappropriation

- Your response to suspected trade secret misappropriation should begin **before** any misappropriation occurs
  - SOPs for Legal, InfoSec, HR, the former employee's nuclear team
  - Training on those SOPs
  - Physical/electronic data preservation, **capturing all capturable data**
    - Image all relevant company-issued devices
    - Not just devices, but also web-based **accounts**, which often have short retention periods:
      - Web history
      - Chat logs
      - SharePoint/Google Drive/OneDrive audit logs
      - Download/upload logs
      - Salesforce/other CRM audit logs
      - Login/logoff data for web-based accounts, like VPNs
      - IP addresses responsible for the above
    - Texts/calls using company-issued devices
    - Web/local artifacts that may remain on the former employee's company devices

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Responding to potential trade secret misappropriation

- Offboarding best practices:
  - Exit interview covering ongoing confidentiality obligations
  - Ensure return/destruction of all company devices/materials
    - Signed certification
  - Disable physical/electronic access
  - Review (30-90 days) of account activity that might reflect misappropriation
  - If high-risk departure, notify relevant stakeholders internally, gauge their assessment of risk of malfeasance
- Engage a third-party forensic expert?
  - May be better equipped to capture important forensic evidence
  - Consider how internal InfoSec employees would perform on the stand
- Aggravating factors to watch out for:
  - Deletion of files/emails on company devices/cloud storage spaces
  - Refusal to sign certification/notice of ongoing obligations
  - Contentious departures, especially when employee had sufficient time to prepare
  - Moving into directly-competitive role
  - Pre-departure access to sensitive material without business need
  - Failure to run document transfers of “personal documents” through prescribed company practice

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Responding to potential trade secret misappropriation

- When to escalate?
  - Engage outside counsel sooner rather than later
    - A false positive is much better than a false negative
- What escalation steps are appropriate?
  - Sending cease and desist letter
    - To former employee only? Also to subsequent employer?
  - File formal Complaint
  - Move for TRO? PI?
  - Delicate balance: time spent collecting evidence vs. moving quickly to prevent irreparable harm

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Key Takeaways

"The best time to establish proper trade secret protection controls was yesterday. The next best time is today."

- **Worst case scenario**:
  - You suspect a former employee misappropriated your trade secrets, but you either
    - did not adequately protect them to confer trade secret status or
    - cannot *prove* misappropriation
- If you are at the enforcement stage and realize your processes were not sound, **it is likely too late**.

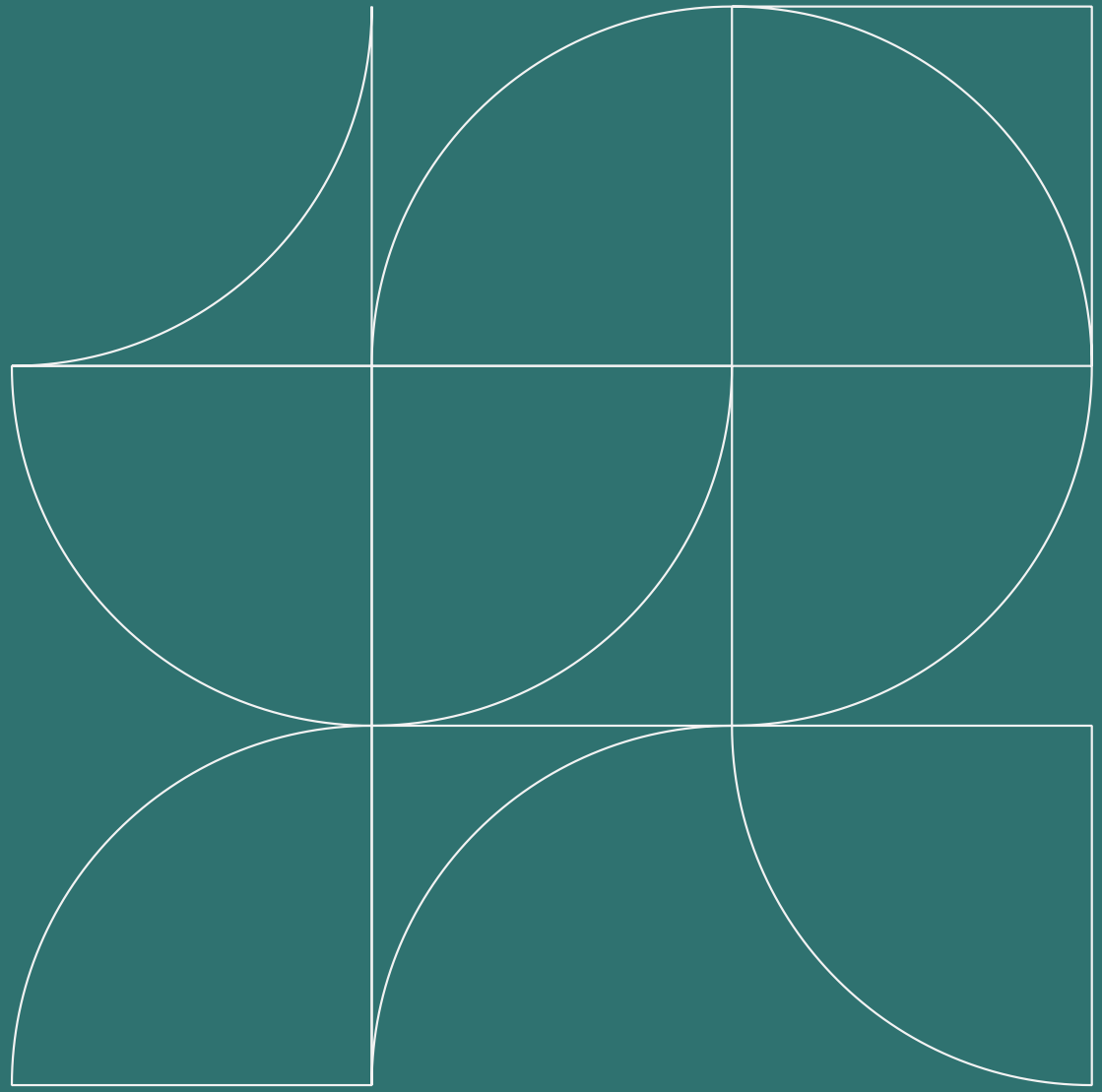
©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Key Takeaways

- **<u>Build tomorrow's litigation record today.</u>**
  - How?
    - Carefully identify and define trade secrets
    - Control and track who has access to trade secrets
    - Institute clear policies regarding handling/transfer of trade secrets
    - Institute appropriate controls to protect trade secrets and monitor for potential exfiltration
    - Timely execute SOPs to capture and preserve evidence when a potential misappropriation incident occurs
    - Don't sleep on your rights today, or they may be gone tomorrow

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

Questions?



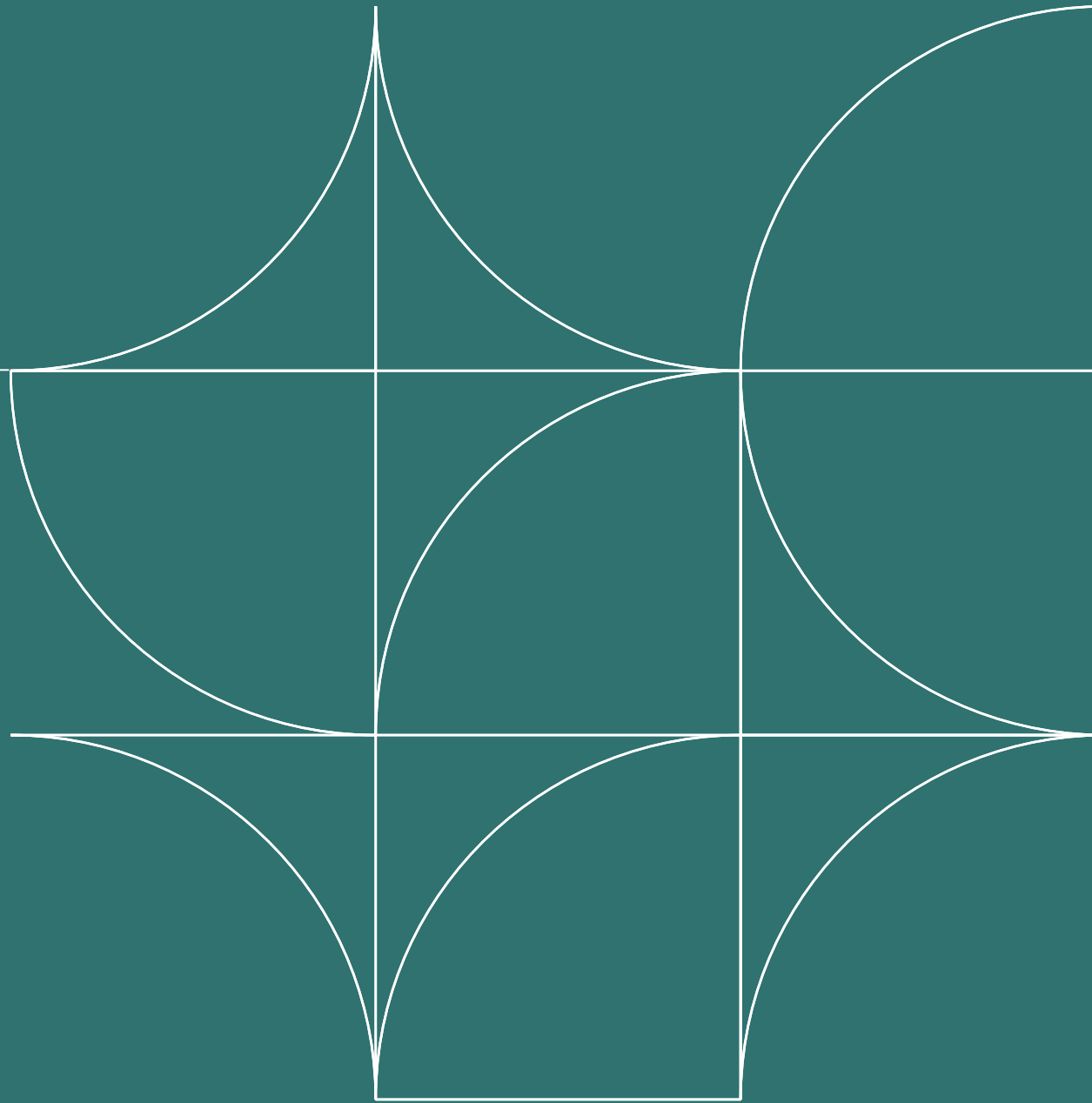
©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential

thank you

Tricia Macaluso
Email: TMacaluso@seyfarth.com

Francis Wilson
Email: fwilson@seyfarth.com

Puya Partow-Navid
Email: PPartowNavid@seyfarth.com



SCAN ME

VERIFICATION FORM

Please scan the QR code to complete the digital attendance verification form to receive CLE credit for this program.

QR code directs you to our electronic form which can also be found in the calendar invite that was sent to you for this program.

You will need:

1. **Title:** Protecting Life Sciences Trade Secrets: From Development to the AI Era
2. **Date Viewed:** November 5, 2026
3. **Attendance Verification Code:** SS4996

State-specific CLE credit information can be found in the form.

©2026 Seyfarth Shaw LLP. All rights reserved. Private and Confidential