WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PALO ALTO SAN FRANCISCO CHICAGO PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

WFG® CLE

# Addressing COVID-19 Cybersecurity, Privacy, and IP Risks in the Pharma and Biotech Industries

**Elizabeth P. Gray | Tiffany Lee | Heather M. Schneider | Philip F. DiSanto**

**October 27, 2020**

## Elizabeth P. Gray

*Partner, Co-Chair of Securities Enforcement Practice Group*

Elizabeth P. Gray is a partner in the Litigation Department and Co-Chair of the Securities Enforcement Practice Group. Elizabeth represents investment advisers, investment companies and their boards, accounting firms, broker-dealers, self-regulatory organizations, public companies and senior executives facing examination, investigation and litigation by financial regulators. She counsels clients on cybersecurity regulation and breach response, and conducts investigations on behalf of audit committees and other committees of the board.

## Tiffany Lee

*Partner, Managing Partner of Willkie Palo Alto Office*

Tiffany Lee is a partner in the Corporate & Financial Services Department and Managing Partner of the firm's Palo Alto office. She focuses on a wide variety of technology transactions. Her practice includes counseling and advising clients on intellectual property issues, and drafting development, licensing, manufacturing, distribution, and other agreements in a wide range of industries including life sciences, healthcare, electronics, semiconductor, and media and entertainment.

## Heather M. Schneider

*Partner, Intellectual Property*

Heather M. Schneider is a partner in the Intellectual Property Department. Heather's practice focuses on patent litigation, as well as antitrust issues involving intellectual property. Her litigation experience encompasses an array of technologies, including pharmaceuticals and biologic products, computer software, medical devices, and chemical products. Her practice also includes client counseling on patent issues, as well as intellectual property issues associated with transactional work including licensing, mergers, and bankruptcy.

## Philip F. DiSanto

*Associate, Litigation*

Philip F. DiSanto is an associate in the Litigation Department. His focus includes complex commercial litigation and counseling, internal investigations, and government enforcement actions. Phil has represented clients across the financial sector, including investment banks, hedge funds, and private equity firms, as well as clients in the technology, manufacturing, and pharmaceutical industries. His practice includes counseling clients in connection with data security incidents and advising clients concerning cybersecurity and privacy risk management.

# Presentation Summary

I. Mounting Cybersecurity, Privacy & IP Risks

II. Protecting Research and Development

III. Cybersecurity Programs and Disclosures

IV. Questions & Answers

# I. Mounting Cybersecurity, Privacy & IP Risks

# Pharmaceutical and Biotechnology Organizations in the Cyber Crosshairs

- Pharmaceutical and healthcare organizations have long been high-value targets of cyberattacks:
  - **June 2013**: Chinese state-sponsored group known as "APT 18 (Wekby)" begins targeting biotech- and pharmaceutical-related organizations, likely with the goal of exfiltrating non-public cancer research.
  - **June 2017**: Merck's global network taken down by NotPetya ransomware, likely released by Russian military intelligence.
  - **July 2019**: Roche confirms that it was targeted by "Winnti" malware, which likely gave a Chinese state-sponsored group remote access to its network.

# The Substantial Cost of Cybersecurity Incidents

- The costs of a data breach continue to mount each year as both technology and the legal landscape become more complex.
- Recent studies indicate that organizations subject to more rigorous regulatory requirements, such as those in financial services and healthcare, have higher per-incident costs.
- In addition, smaller businesses in the United States had some of the highest per-record and per-individual data breach costs.
- While malicious attacks are among the costliest and most common root causes of data breaches, ***nearly a quarter of all breaches are caused by human error, and another quarter are caused by failures in IT systems and business processes***.

**Healthcare Industry Average Cost of a Data Breach: $6.45 million**

**Pharmaceutical Industry Average Cost of a Data Breach: $5.2 million**

(Source: 2019 Cost of a Data Breach Report, Ponemon Institute.)

## People's Republic of China (PRC) Targeting of COVID-19 Research Organizations

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the threat to COVID-19-related research. The FBI is investigating the targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors and non-traditional collectors. These actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. The potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options.

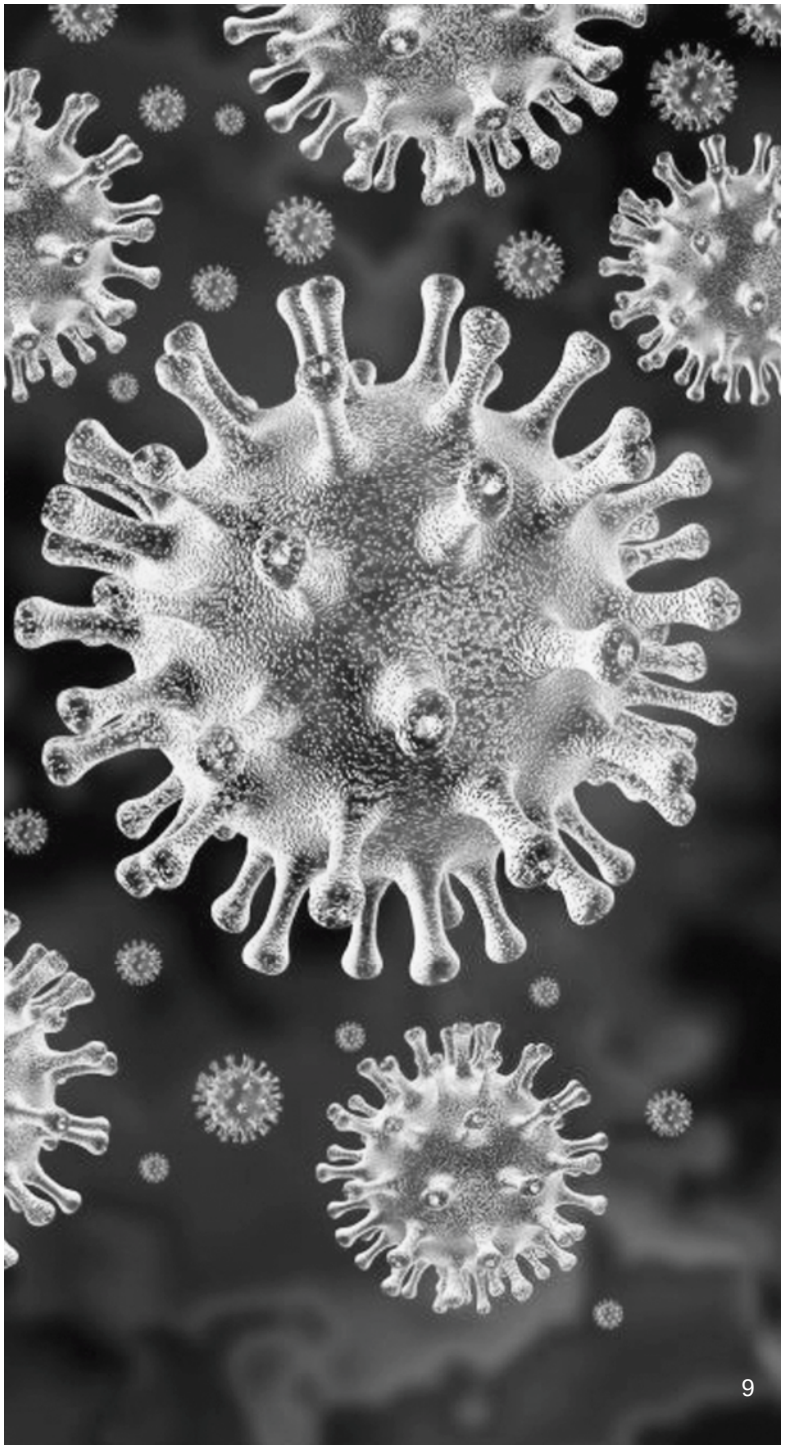
The FBI and CISA urge all organizations conducting research in these areas to maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material. FBI is responsible for protecting the U.S. against foreign intelligence, espionage, and cyber operations, among other responsibilities. CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. CISA is providing services and information to support the cybersecurity of federal and state/local/tribal/territorial entities, and private sector entities that play a critical role in COVID-19 research and response.

**"The FBI and CISA urge all organizations conducting research in these areas to maintain dedicated cybersecurity and insider threat practices to prevent surreptitious review or theft of COVID-19-related material"**

Source: https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf

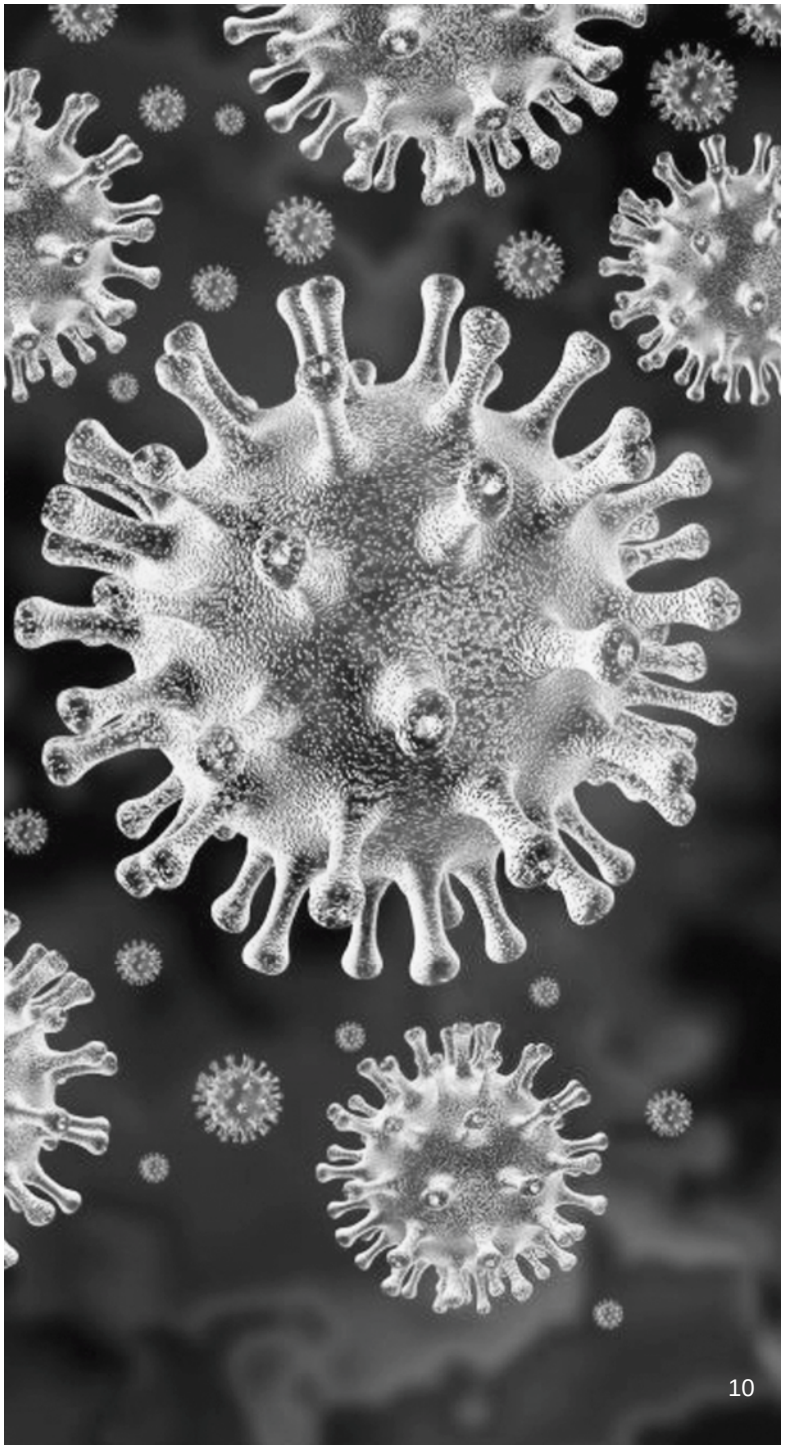
# Pandemic High-Risk Cyberattack Targets

- Pharmaceutical Companies
- Biotechnology Companies
- Contract Research Organizations
- Research Universities
- Pharma and Biotech Investors
- Healthcare Providers



# Pandemic Cyberattack Motivations

- Theft of Intellectual Property
- Theft of Material Non-Public Information
- Nation-State Competition
- Cyberterrorism



# The Full Picture: Risks in COVID-Related Mergers, Acquisitions, and Partnerships

- COVID-19 research may drive mergers, acquisitions, and partnerships
- Importance of due diligence for cybersecurity, privacy, and IP risks
- Legal and business consequences
- Protections in M&A agreements and collaboration agreements

Addressing Cybersecurity, Privacy and IP Risks

# II. Protecting Research and Development

# Overview

- Increased risk of misappropriation of IP emphasizes the importance of obtaining registered, broadly enforceable IP rights
- Think about filing for and registering IP protections broadly in jurisdictions with the higher risk of misappropriation (e.g., China, Russia, etc.)
- Even if the IP is misappropriated, registered, enforceable IP will provide better protection and broader remedies (such as injunctions)
- Registering IP has the added effect of putting parties on notice of what technologies you own

# Patent Protection

- To obtain a patent, invention must be new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof.

- Patent protection may be only way to protect certain pharmaceutical information such as the composition and method of use of a drug, which are required to be disclosed in New Drug Applications for drugs to be used in humans.

- Threshold for patentability with respect to biotechnology raised by *Association for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107 (2013) and *Mayo Collaborative Sciences v. Prometheus Laboratories, Inc.*, 132 S. Ct. 1289 (2012).

# Patent Protection, *Cont'd*

- If eligible, consider seeking patent protection on inventions that previously would have been maintained as trade secrets, but that are at risk of misappropriation.

- Consider filing PCTs more broadly than before to ensure greater availability of remedies like injunctions, importation restrictions, and monetary damages.

- Different jurisdictions may have different eligibility requirements and technologies ineligible for patent in the U.S. may be eligible in other jurisdictions (e.g., the slightly broader scope of patentability for isolated naturally occurring sequences in the EU compared to in the U.S.)

# Copyright Protection

- Consider whether registering any of your software code or other copyrightable technologies should be registered for broader copyright protection.

- While in the U.S. and in many other countries, copyright protection arises by law regardless of whether or not the work is registered, broadly registering such copyrights will make enforcing them faster, easier, and will increase the availability of remedies like injunctions and monetary damages.

# Copyright Protection, *Cont'd*

- Remember that if a computer program or source code contains trade secrets, the U.S. copyright office allows for deposit of only certain portions of the work or deposit of the whole or portions of the work with trade secret portions redacted (although redaction may not exceed half of the total lines of code).

- Copyright protection admittedly may not be as useful to biotechnology and pharmaceutical companies as it is to software companies; although commentators (starting with Irving Kaytom in 1982) have been increasingly calling for the copyrightability of recombinant or synthetic DNA sequences, such protection is not yet available in the U.S. or, as far as we have seen, anywhere else.

# Trade Secret Protection

- Trade secret protection is the form of protection most susceptible to misappropriation, since its eligibility for protection depends upon its secrecy.

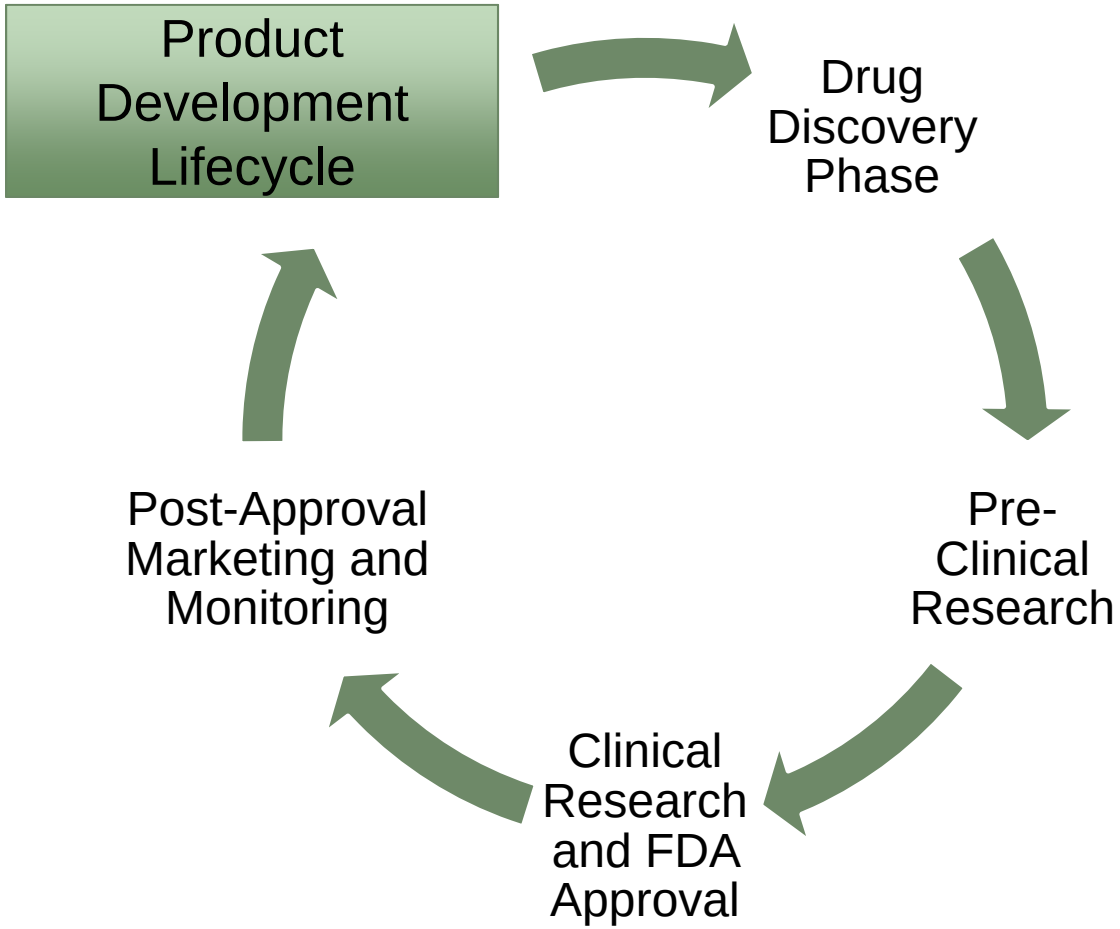
- Certain activities better protected as trade secrets (e.g., preclinical development of products to the FDA).

# Trade Secret Protection, *Cont'd*

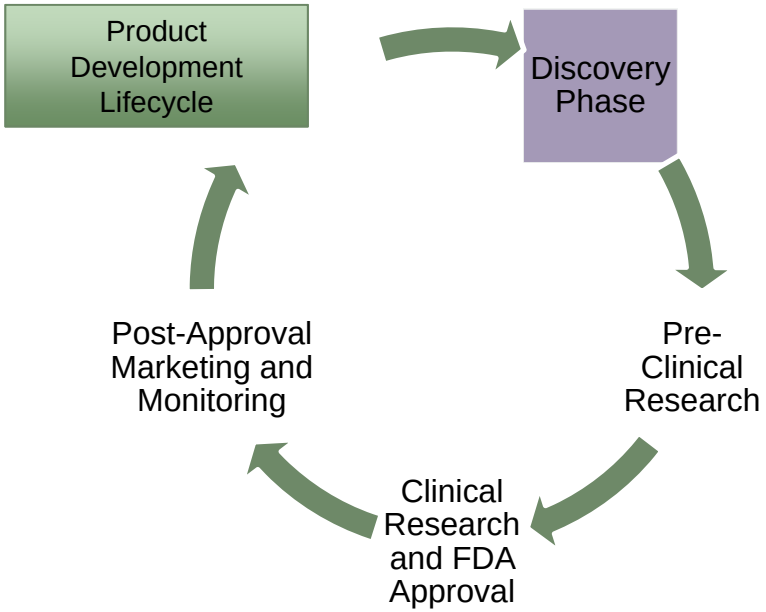
- Other activities better protected as patents (e.g., any biotechnology and pharmaceutical inventions that can be easily reverse engineered) since reverse engineering is a defense to a claim of misappropriation of trade secrets.

- Use of trade secret information may constitute a "public use" under 35 U.S.C. section 102(b) barring filing for patent protection later.

# Synthesizing IP and Cybersecurity Strategies



# Synthesizing IP and Cybersecurity Strategies, *Cont'd*



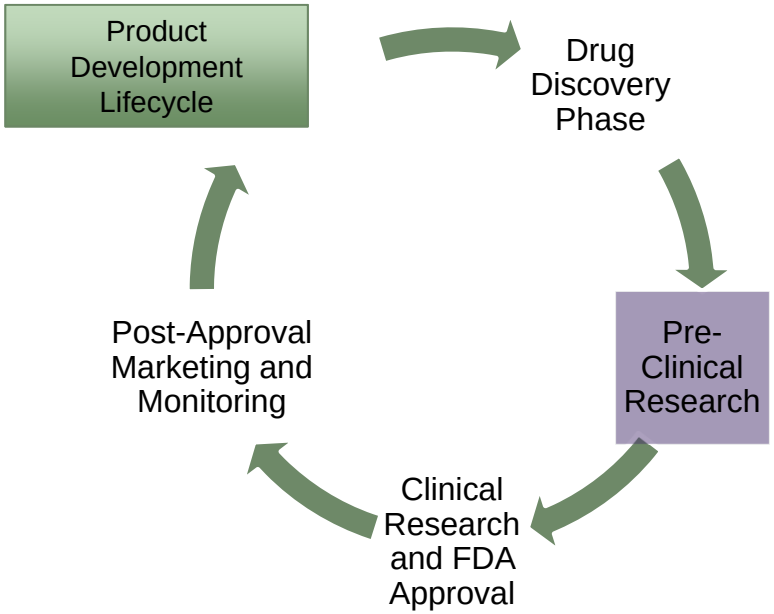

**Intellectual Property Considerations**

- Identify and pursue strategy for patent protection or assess potential barriers to generic or biosimilar approval.

**Cybersecurity Considerations**

- Ensure industry standard technological safeguards are in place while developing an IP strategy to protect theft of preliminary research and confidential business information.

# Synthesizing IP and Cybersecurity Strategies, *Cont'd*



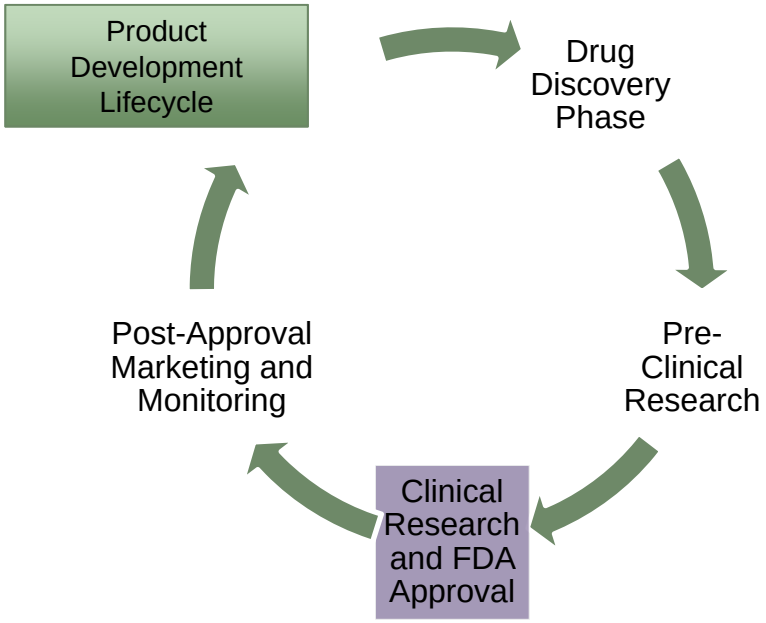

**Intellectual Property Considerations**

- Perform in vitro and in vivo preclinical research pursuant to good laboratory practices (GLP).

**Cybersecurity Considerations**

- Incorporate cybersecurity best practices into pre-clinical QA process and monitor research environment for incidents.

# Synthesizing IP and Cybersecurity Strategies, *Cont'd*



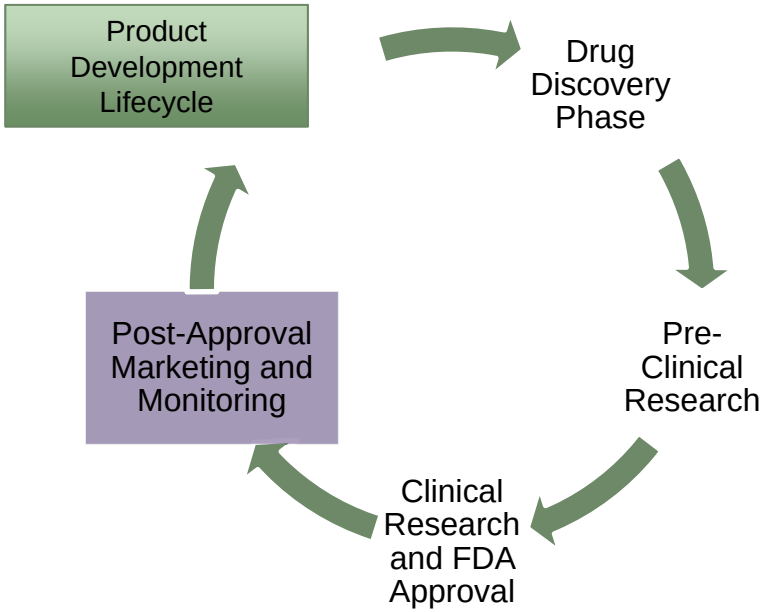

**Intellectual Property Considerations**

- Perform clinical trials in support of NDA, ANDA, or BLA.

**Cybersecurity Considerations**

- Continue monitoring research environment for cybersecurity threats or contamination. Ensure compliance with all applicable privacy regulations.

# Synthesizing IP and Cybersecurity Strategies, *Cont'd*




**Intellectual Property Considerations**

- Distribute FDA approved product and continue to monitor and evaluate safety during routine use.

**Cybersecurity Considerations**

- Ensure that manufacturing and research environment is secure, protect highly confidential business information, monitor internet and market for counterfeit products.

# Due Diligence Considerations

**Intellectual Property Issues**

- Potential Infringement
- Broken Chain of Title
- Unclear Data Ownership
- Vulnerable Trade Secret Safeguards
- Confidentiality Issues
- Open Source Licenses (e.g., in Medical Device Software)

**Cybersecurity/Privacy Issues**

- Non-Compliance with Data Protection Laws
- Improper Use of PII
- Weak Contractual Provisions
- Inadequate Safeguards
- Liability for Prior Cyber Incidents
- Pending Government Investigations or Enforcement Actions

# Mitigating Risks Identified in Due Diligence

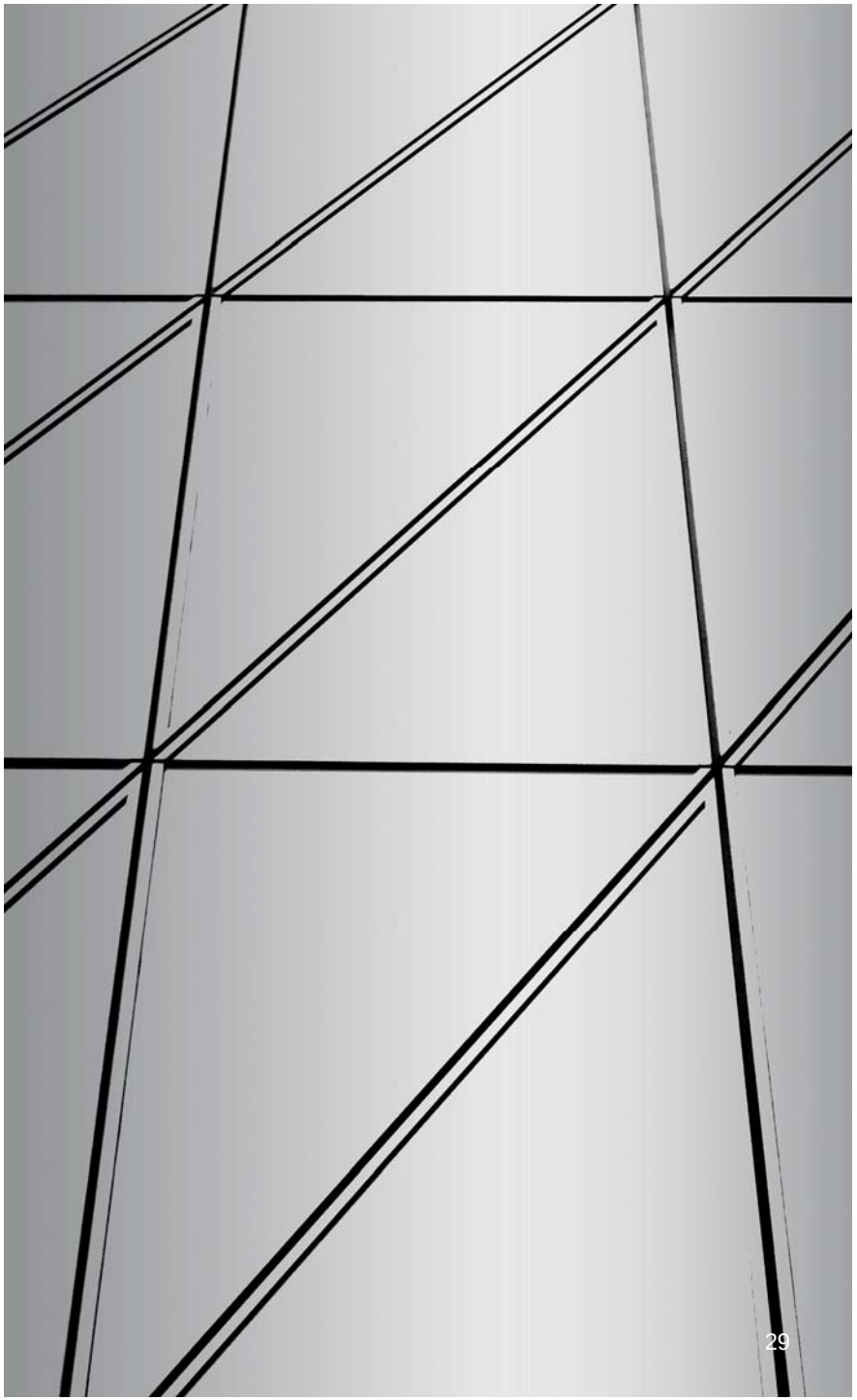
- Representations and Warranties
- Invention Assignments and Confidentiality Agreements
- Registering IP
- Addressing Cyber Vulnerabilities
- Indemnification Agreements
- Remediation Plans

Addressing Cybersecurity, Privacy and IP Risks

# III. Cybersecurity Programs and Disclosures

# Importance of Developing a Cybersecurity Program

- Compelling business reasons
- Mitigating civil litigation risks
- Avoiding government investigations and enforcement actions, including by:
  - Securities and Exchange Commission (SEC)
  - Federal Trade Commission (FTC)
  - HHS Office for Civil Rights (OCR)
  - U.S. State Attorneys General
  - U.K. Information Commissioner's Office (ICO)
  - German Federal Commissioner for Data Protection
  - French Commission Nationale de l'informatique et des Libertés (CNIL)



# SEC Cybersecurity Guidance (2018)

Companies expected “to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure.”

# U.S. Public Company Disclosure Obligations

- **Risk Factors**:
  - Adequacy of cyber protections, associated costs, relevant laws and regulations, potential for reputational harm, and litigation or similar costs.
- **MD&A of Financial Conditions and Results of Operations**:
  - Consider actual or potential costs associated with cybersecurity risks or incidents when preparing its MD&A.

# U.S. Public Company Disclosure Obligations, *Cont'd*

- **Board Risk Oversight**:
  - A company must disclose information concerning its board of directors' role in cybersecurity risk management and engagement with management on cybersecurity issues, if such issues are material to the company's business.

# U.S. Public Company Disclosure Obligations, *Cont'd*

- **Incident Response Plan**:
  - Cybersecurity program should also include an Incident Response Plan to establish key elements of response and recovery from a cyber incident
- **Business Email Compromises:**
  - Key component of cybersecurity program is guarding against BEC scams.

# SEC Cybersecurity and Resiliency Observations (2020)

- Conduct vendor due diligence
- Monitor and oversee vendors and contract terms;
- Assess how vendor relationships are considered as part of the organization's ongoing risk assessment; and
- Assess and test how vendors protect any accessible client information.

# Example: Cybersecurity Incident at Major Contract Research Organization

- In March 2019, a major contract research organization providing both preclinical and clinical services to the pharmaceutical and biotechnology industries suffered a cybersecurity incident. The CRO reported in an SEC filing that "**client data was copied by a highly sophisticated, well-resourced intruder**."

- Cybersecurity incidents involving pharmaceutical and biotechnology vendors can have significant financial and reputational impacts on both the vendors themselves and their clients. Such incidents can result in:
  - Terminated contractual relationships;
  - Disruptions to ongoing research and development;
  - Potential legal claims, including commercial and insurance disputes;
  - Investigations by government regulators and enforcement agencies.

(Source: Form 8-K, Apr. 30, 2019.)

# Privacy Compliance Programs

- Establish formal responsibilities for privacy compliance
- Analyze and map the organization's data
- Mandate preliminary and periodic privacy risk assessments
- Implement key policies and internal controls concerning compliance with applicable laws and regulations

# Privacy Compliance Programs, *Cont'd*

- Address third-party and vendor risk management issues
- Provide ongoing privacy training to employees and vendors
- Monitor and audit compliance with the comprehensive program
- Mandate periodic review of the privacy compliance program

# Testing Preparedness With Tabletop Exercises

## Cyber Scenario Review (5-10 minutes)

- Draft a cybersecurity incident scenario that is realistic and tailored to the specific organization's risk profile.
- Scenario can be distributed in advance or at the outset of an exercise depending on goals.
- Scenario can either be distributed to all members of the Cyber Incident Response Team simultaneously, or to a member of the team to test escalation and communication channels.

## Facilitated Discussion (1-2 hours)

- Either the coordinator of the IRT or an outside advisor should lead discussion of the scenario using a pre-determined list of questions or agenda.
- Maintain flexibility to respond to participants' reactions and concerns.
- Suggest variations of the core scenario to test internal triggers, such as those related to escalation and notification procedures.

## Conclusion / Findings (25 minutes)

- Discuss findings concerning the IRT discussion and suggest topics for further testing.
- Encourage IRT participants to offer feedback and request additional training, if necessary.
- Consider feedback from external advisors, such as

Willkie Farr & Gallagher LLP

# Questions & Answers

Willkie Farr & Gallagher LLP

# Thank you!