
# The GDPR, State Privacy Laws, and the Pharmaceutical Industry

## Big Data in the Life Sciences Deal Space

20th Annual Pharmaceutical and Medical Device Compliance Congress
November 6, 2019

**Kim Gold, Partner**
ReedSmith

**Pearl Hsieh, Senior Counsel**
Smith+Nephew

# Kimberly J. Gold

**Partner**
**Reed Smith LLP**
New York
+1 212 549 4650
kgold@reedsmith.com

Kim's practice focuses on data privacy, digital health, and complex transactional matters (including M&A, private equity, and technology transactions). She advises clients in the life sciences, health care, retail, and technology industries on corporate governance, privacy compliance, cybersecurity incident planning and response, research and big data initiatives, and government investigations.

Kim regularly counsels clients on data privacy and cybersecurity issues relevant to:

- Federal, state, and global laws (e.g., HIPAA, state health care privacy laws, GDPR, CCPA, TCPA, and more);
- Digital transformation and innovation, including research collaborations, data sharing/analytics, and AI;
- Advertising and marketing;
- Health information technology and telemedicine; and
- Cloud services, mobile apps, and connected devices

# Pearl Hsieh

Pearl is Senior Counsel of Smith & Nephew, a leading medical technology company. Throughout her legal career, Pearl has counseled on data privacy and security matters in complex transactions to support operational expansion, sales growth, mergers and acquisitions in life sciences and technology industries. The data privacy and security matters encompass corporate governance and oversight programs, and risk assessments in compliance, prevention, detection and response initiatives.

**Senior Counsel**
Smith+Nephew
Columbia, Maryland
+1 443-545-1801
pearl.hsieh@smith-nephew.com

# Overview of the M&A Process: Stages

## Early Stages of the Deal


## Negotiation and Closing

# Deals of the Day:  Recent Life Sciences Transactions

**Smith & Nephew acquires Osiris Therapeutics**

**VSP Global acquires VisionWorks**

**Restoration Robotics merger with Venus Concept**

# Due Diligence: Elements

- Submit questionnaires to the target
- Document review
- Submit supplemental questions depending on review results
- Interview responsible representatives of target
- Providing detailed memorandum or shorter red flags report

# Privacy/Security Due Diligence Questions

**Generally, the goal is to understand:**

1. **How personal data is collected, used, stored, disclosed, and otherwise processed**
2. **What privacy and security laws the target or the personal data it collects may be subject to**
3. **Any red flag issues (e.g., data breaches)**

# Hypothetical #1

**While reviewing answers to the diligence questionnaire responses, you notice that the target experienced a data breach within the last year.**


# Data breach notification laws

- **Quick overview: state breach notification laws**
  - As of March 2018, all 50 states, D.C., Guam, Puerto Rico, and Virgin Islands
  - General Framework
    - Notification Trigger: Has a security breach been discovered for which notification is required under the relevant law?
    - Compliance Obligations: What steps are required to notify affected individuals and regulators?

# Data Room and Public Facing Material Review

- Contracts with Vendors, Suppliers, and Clients
- Business Association Agreements (BAAs)
- Data Processing Agreements
- Policies and Procedures
- Documentation of Security incidents
- Compliance documents
- Employee Training Documents
- Any Documents indicating Data Flows/Data Mapping

# Hypothetical #2

**During your independent review of the target's website and privacy policies, you discover that the company is collecting data from people located in the EU.**

# Quick Overview: Extra-Territorial Application of GDPR

- Applies to Data Controllers and Data Processors regardless of whether processing takes place in EU.
- Application is triggered when:
  - Goods or services are offered to individuals in the EU; or
  - Behavior of individuals in the EU is monitored or tracked through use of technology.

# Due Diligence Interview

- **Get a deeper understanding of answers to due diligence questionnaire. For example:**
- What are the purposes for collecting and/or processing personal information?
- Describe data privacy training provided to target employees.
- Does the target further disclose any personal information it receives? To whom?
- **Follow up on any red flag or outstanding issues.**

# Hypothetical #3

**During your diligence interview with the target, you determine that the target believes they are a covered entity under HIPAA and have taken measures to comply. However, you are not entirely sure the target is subject to HIPAA.**

# Due Diligence Memo

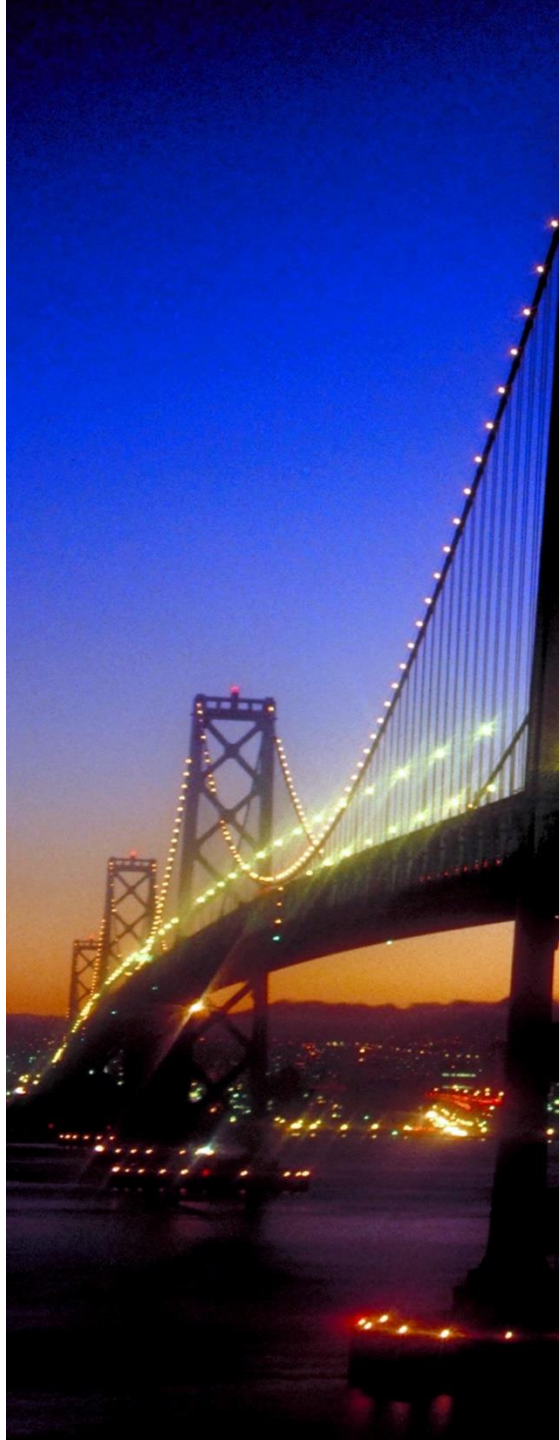
## Key Issues:

- **Data breach/security incidents**
- **Compliance with laws (HIPAA, CCPA/CMIA, GDPR)**
- **Ongoing investigations or enforcement actions**
- **Do data protection terms comply with applicable laws and/or sufficiently protect data?**
- **Employee/personnel trainings**

**Make Recommendations: what steps the company needs to take prior to or following closing to mitigate potential risk factors**

# Hypothetical #4

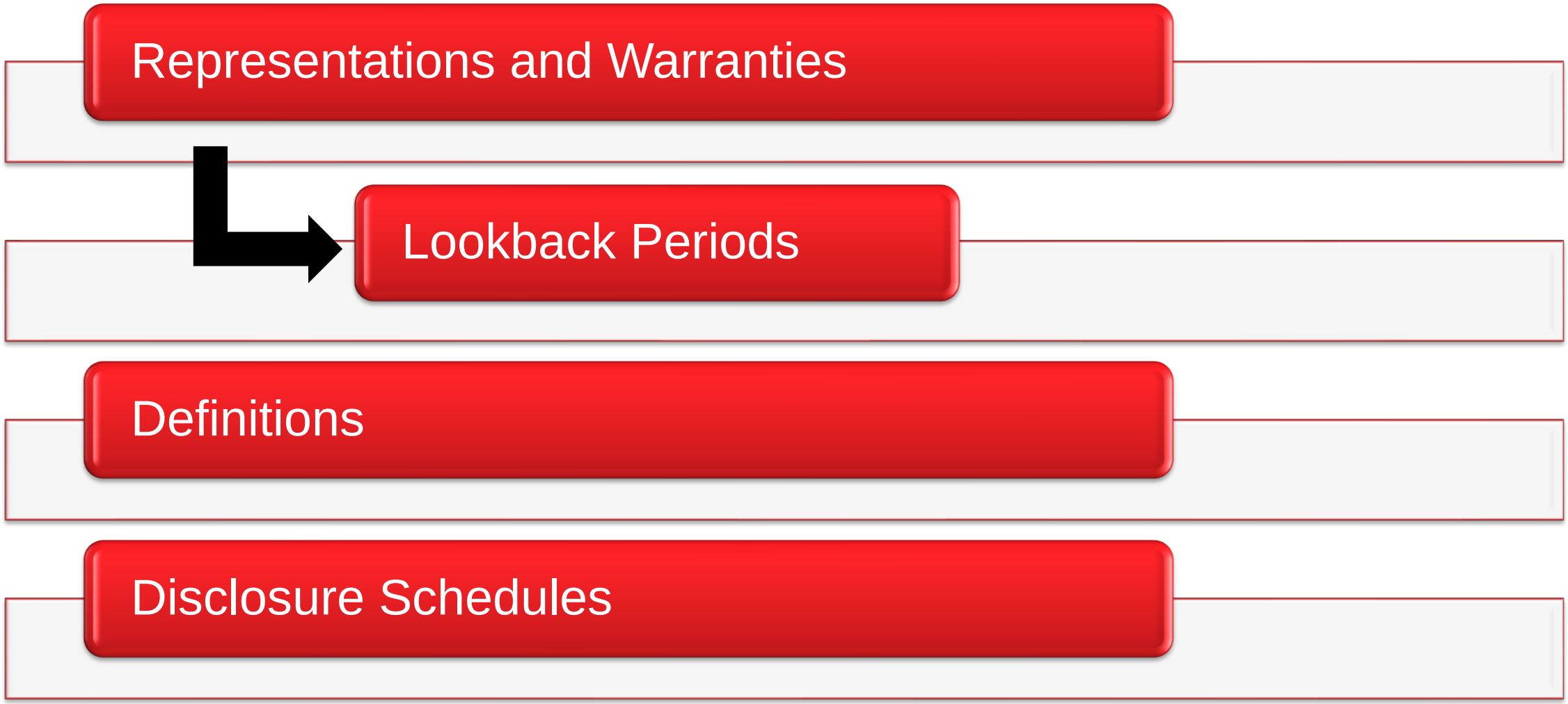
**When compiling your diligence memo, you discover the target may have a practice in California. However, the target has not taken any steps to comply with the CCPA.**



# Quick Overview: CCPA

- **General Responsibilities**
  - Expanded customer notifications and disclosures.
  - Compliance with verifiable consumer requests regarding Personal Information (PI).
- **Restrictions**
  - Cannot collect categories of PI other than those they have specified in their disclosures.
  - Cannot use PI for additional purposes unless consumer notified.
- **“Sale”** of data and **opt-outs**

# The Merger Agreement

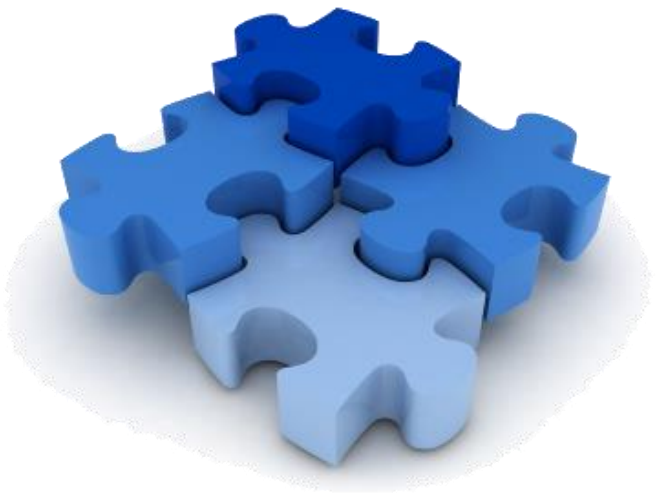


# Hypothetical #5

**You see the following definition when reviewing the proposed merger agreement:**

“Personal Information” means any non-public information that can reasonably be used to identify a person.

# Additional Considerations



- **Call Representations and Warranties Insurer**
- **Publicly traded companies (SEC filings)**
- **Post-closing integration**
  - Plan ahead to access acquired business units and identify priorities
  - Implement, monitor and enforce policies and procedures
  - Conduct regular employee compliance training
  - Review third party agreements to determine privacy and security obligations
  - Monitor vendors for compliance with contracts against data breach risks
  - Provide leadership support to privacy and security functions

# Hypothetical #6

**Your company is <u>not</u> subject to HIPAA but you now acquire a target company that is subject to HIPAA as a business associate.**

# Questions?