# Cybersecurity for Employee Benefit Funds: What you need to Know

XPAN LAW

# Panelists

Rebecca L. Rakoski, Esq.
Managing Partner
XPAN Law Partners

Adam Boston, Esquire
Chief Legal Officer
Data Privacy Officer
IUPAT, Pension Fund

# Themes for Today

- Why cybersecurity and data privacy matters to employee benefit funds
- What the legal and fiduciary standards apply to employee benefit funds
- Third Party Information Management
- Playbook for good cyber-governance

XPAN
LAW

# Cybersecurity and Data Privacy Matters to Employee Benefit Funds

# Target Rich Environment

- Electronic transactions
- Multiple platforms and multiple players
- Electronic access to account information
- Protected Health Information
- Remote work and access
- Member data (and their beneficiaries too)

# Audience Poll

- Who is responsible for development, implementation, and oversight of cybersecurity and data privacy program now?
- Who is responsible for Vendor Management Program?
- How many vendors / service providers hold or have access to my Fund's participant data?
- Do you discuss oversight and monitoring of cybersecurity and/or data privacy at Trustees meetings?

# Legal and Fiduciary Standards that Apply to Employee Benefit Funds


- ERISA requires plan fiduciaries to act with the “care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use.” ERISA § 404(a)(1)(B) (29 U.S.C. § 1104(a)(1)(B)).

- When applying ERISA’s prudence requirement, courts and the Department of Labor (DOL) generally focus on whether the fiduciary followed a *good process*.


# *FTC Regulation in Cybersecurity*

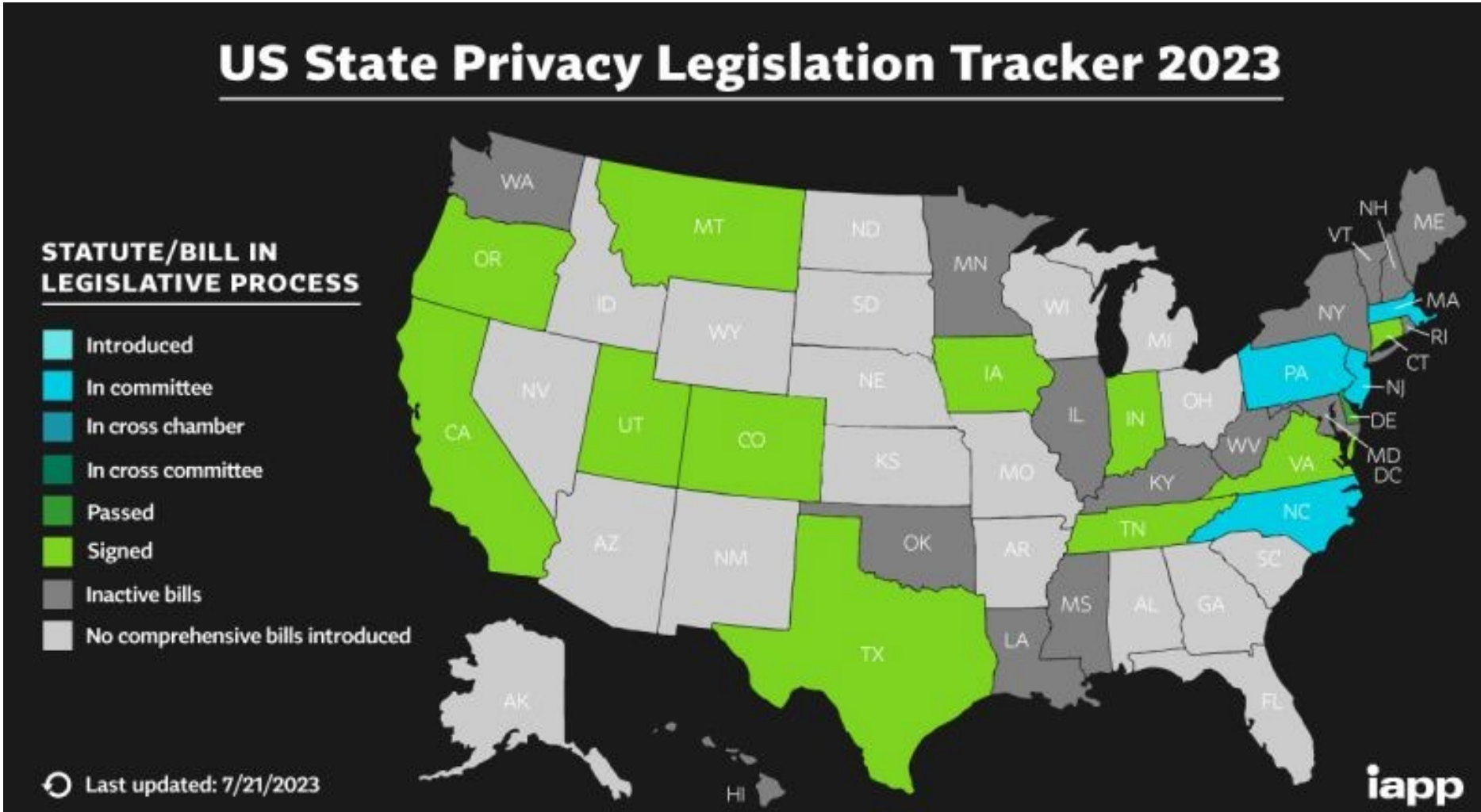
FTC has authority under Section 5 of the FTC Act to regulate cybersecurity and data privacy:

> declares illegal “unfair or deceptive acts or practice in or affecting commerce.” 15 U.S.C. § 45(a)(1).

# Common Law Causes of Action

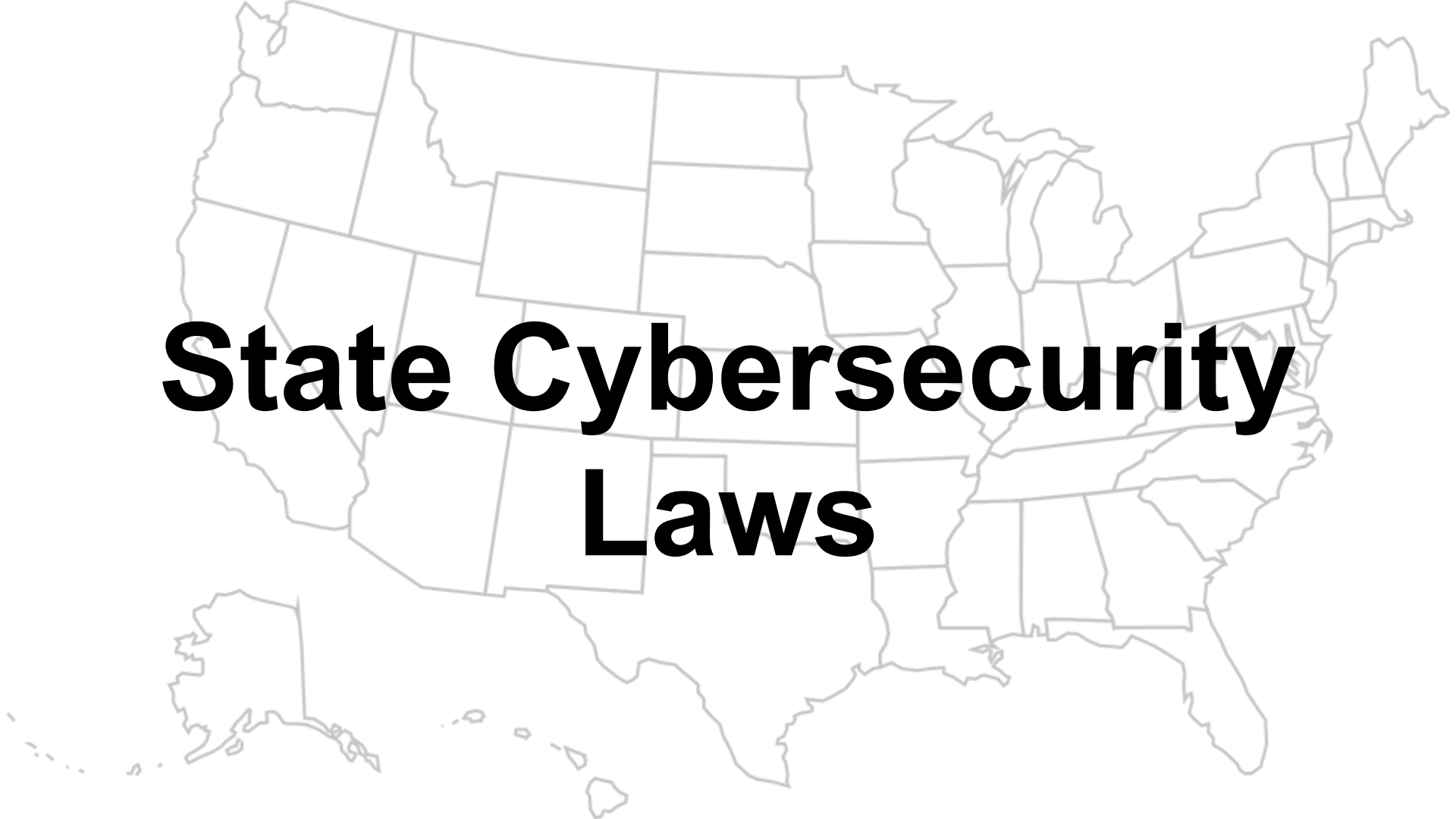
- Breach of Fiduciary Duty
- Breach of Contract
- Breach of Implied Contract
- Negligence
- Negligence *Per Se*
- State Consumer Fraud Statutes

# US State Privacy Legislation Tracker 2023



# State Privacy Laws

| | | |
|---|---|---|
| California Consumer Privacy Act | 2018 | July 1, 2023 |
| Colorado Privacy Act | 2021 | July 1, 2023 |
| Connecticut Data Privacy Act | 2022 | July 1, 2023 |
| Indiana Consumer Data Privacy Bill | 2023 | January 1, 2026 |
| Iowa Data Privacy Law | 2023 | January 1, 2025 |
| Montana Consumer Data Privacy Act | 2023 | October 1, 2024 |
| Tennessee Information Protection Act | 2023 | July 1, 2025 |
| Texas Data Privacy and Security Act | 2023 | March 1, 2024 |
| Utah Consumer Privacy Act | 2022 | December 31, 2023 |
| Virginia Consumer Data Protection Act | 2021 | January 1, 2023 |



# State Cybersecurity Laws

# Cybersecurity Requirements

| | | |
|---|---|---|
| Alabama | Kentucky | Ohio* |
| Arkansas | Louisiana | Oregon |
| California | Maryland | Rhode Island |
| Colorado | Massachusetts* | South Carolina |
| Connecticut | Michigan | Texas |
| District of Columbia | Minnesota | Utah |
| Florida | Nebraska | Vermont |
| Illinois | Nevada | |
| Indiana | New Mexico | |
| Kansas | New York* | |

# DOL Cybersecurity Guidance

- Applies to plan sponsors, **plan fiduciaries**, record keepers and plan participants on best practices for maintaining cybersecurity.
- Directed at plan sponsors and **fiduciaries** regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries.
- Goal is to protect the retirement benefits of America's workers. (***THIS MEANS MEMBERS COME FIRST***)

# Fiduciary Obligation

Duty of Prudence:

- Fiduciaries must act prudently and solely in the interest of the plan, participants and beneficiaries.
    - Prudently develop policies and procedures to protect information that is handled, processed, collected, transmitted, and stored (not just PHI – PII and participant data too).
    - Prudently prepare for and respond to a breach scenario.
    - Third party procedures (protect, notify, and remediate)

# DOL Cybersecurity Guidance

The Guidance relates to three (3) main areas of focus:

1. Third-Party Service Providers
2. Cybersecurity Best Practices
3. Online Security Tips

# Tips for Hiring Service Providers

- Selecting a qualified and experienced service provider is a critical step in a successfully establishing a secured environment.
- Directed towards plan sponsors, the guidance focuses on best practices for hiring service providers.
- EBSA outlines the responsibility to “prudently select and monitor” service providers with strong cybersecurity practices to fall upon the **employers and fiduciaries**.
- All potential service providers should be evaluated and closely monitored.

# Tips for Hiring Service Providers

- Helps plan sponsors and fiduciaries prudently select a **service provider** with strong cybersecurity practices and monitor their activities, ***as ERISA requires***.
- Help business owners and fiduciaries meet their responsibilities ***under ERISA*** to prudently select and monitor such **service providers.**

# Tips for Hiring Service Providers

- Ask about security standards, practices and policies, and audit results.
- Ask the service provider how it validates its practices.
- Evaluate the service provider's track record in the industry.
- Ask about past security breaches.
- Does service provider have insurance policies.
- Create contract language around requirements.

# Sample Audit Questions: Third Parties

- All documents constituting or reflecting the plan's cybersecurity program, and all documents reflecting the components of that program.
- All documents constituting or reflecting the plan's access control procedures for its cybersecurity system or security controls.
- **All documents stating or describing the roles and responsibilities of each person having responsibility for any aspect of the plan's information security, cybersecurity or security controls, and all documents stating, describing, or reflecting the definition of each person's roles and responsibilities.**

# Sample Audit Questions: Third Parties

- All documents constituting or reflecting any security reviews and/or **independent security assessments** performed that relate to assets or data stored in a cloud or managed by a third party service provider.
- All documents constituting or reflecting any **third-party audits** of the plan's cybersecurity system or its security controls, including any annual or periodic audits, performed by any outside party or entity.
- All documents constituting or relating to any **contracts** with any third-party service providers that provide services relating to the plan's information security, cybersecurity, or security controls.

# Cybersecurity Program

- This guidance is a **fiduciary responsibility** of the plan to protect the participants' data.
- The DOL provided a "road map" for each of the twelve areas of the Cybersecurity Best Practices.
- The responsibility for a cyber program DOES NOT rest solely with the service provider.
- Plans should have a written information security program in place that **INCLUDES** the requirements for service providers.

# Cybersecurity Program

- **Documented Cyber Program**
- **Annual Risk Assessment**
- **Annual third party audit of security controls**
- **Clearly define security roles and responsibilities**
- **Access control procedures**
- **Appropriate security reviews and assessments of cloud storage providers**

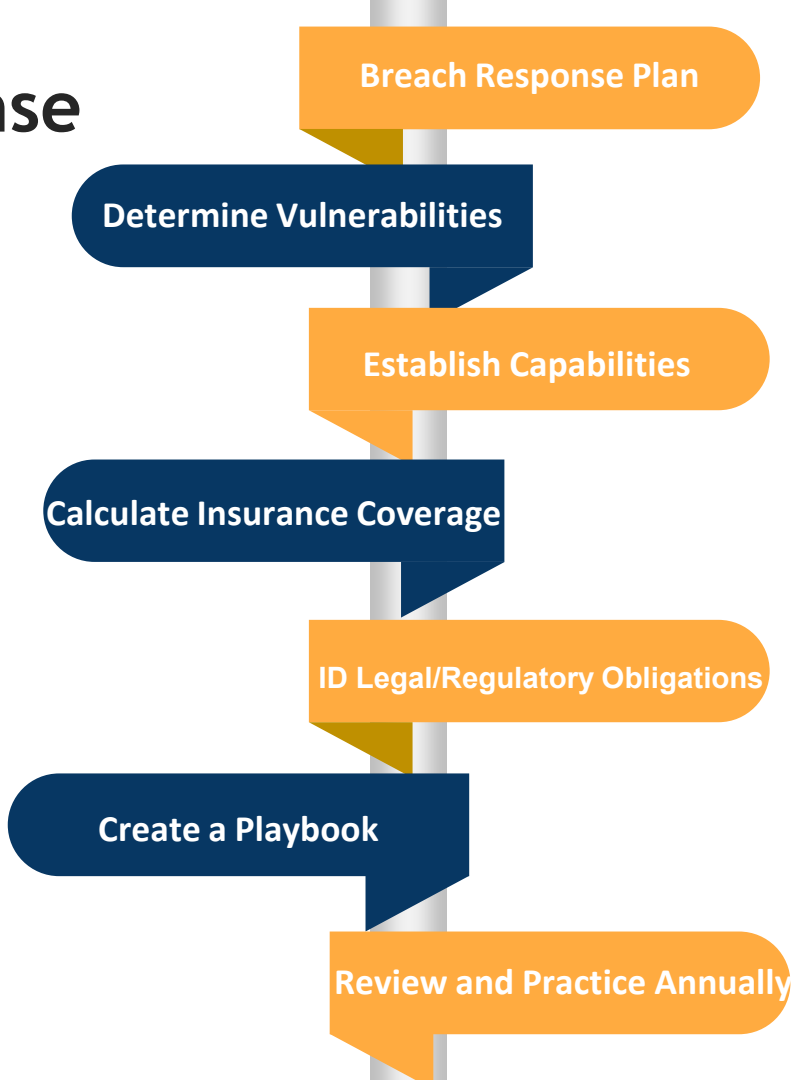
# Cybersecurity Program

- Conduct cyber awareness training
- Implement and manage a security system development life cycle program
- Have business resiliency program addressing business continuity, disaster recovery and incident response
- Encrypt sensitive data in transit and at rest
- Implement technical controls
- Respond to past cyber incidents

# Sample Audit Questions: Cybersecurity Program

- All documents constituting or reflecting the conduct of any **risk assessments** of the plan's cybersecurity system, including all documents reflecting the conduct of annual or other periodic risk assessments.
- All documents constituting or reflecting the performance of any **internal audits** of the plan's cybersecurity system or its security controls, including any annual or periodic audits.
- All documents constituting or reflecting the conduct of **cybersecurity awareness training**, including all periodic cybersecurity awareness training.
- All documents constituting or reflecting any **business resiliency program or business continuity program** relating to the plan's cyber system or its cybersecurity, including processes for business continuity, disaster recovery, and incident response.

# Data Breach Response



# Sample Audit Questions

- All **documents** reflecting the plan's implementation of **technical controls** for its cybersecurity program.
- All **documents** constituting or reflecting the implementation and/or management of a secure **system development life cycle (SDLC) program**.
- All **documents** reflecting the occurrence of any **cybersecurity incidents, breaches, or suspected incidents or breaches**, and the actions taken in response to each.
- All documents constituting or reflecting the **plan's processes** for the encryption of sensitive data, stored and in transit.
- All documents constituting or reflecting any **business resiliency program or business continuity program** relating to the plan's cyber system or its cybersecurity, including processes for business continuity, disaster recovery, and incident response.

# Sample Audit Questions

- All **documents** reflecting the plan's implementation of **technical controls** for its cybersecurity program.
- All **documents** constituting or reflecting the implementation and/or management of a secure **system development life cycle (SDLC) program**.
- All **documents** reflecting the occurrence of any **cybersecurity incidents, breaches, or suspected incidents or breaches**, and the actions taken in response to each.
- All documents constituting or reflecting the **plan's processes** for the encryption of sensitive data, stored and in transit.
- All documents constituting or reflecting any **business resiliency program or business continuity program** relating to the plan's cyber system or its cybersecurity, including processes for business continuity, disaster recovery, and incident response.

# Third Party Vendor Management

# Third Party Breaches

MOVEit

Eye Care Leaders' EMR

80% of surveyed organizations last year experiences at least one data breach caused by a third party.

More than 30% of all breaches were third-party breaches. 23% of breaches to Software Publishers were through third parties.

Okta

PracticeMax

A hydra-headed breach centered on a single American software maker (MOVEit) compromised data at more than 600 organizations worldwide.

SolarWinds

# Third Party Management

1. Regulatory Requirements
2. Due Diligence and Questionnaires
3. Vendor Contracts
4. Risk Mitigation

# Regulatory Requirements

- FTC
- HIPAA
- DOL Guidelines
- State Cybersecurity Laws
- Privacy Laws

# Due Diligence and Questionnaires

- Security Standards
- Documented Policies and Procedures
- Audit/Assessment Results
- Independence of Validation
- Past Security Breaches
- Track Record in Industry
- Insurance
- Contract Language

# Vendor Contracts

- Data Security Requirements
- Data Privacy Requirements (as per Reg)
- Risk Allocation
- Third-Party Vendor Relationships
- Contract Termination/Dispute
- Vendor Assessments
- Regulatory Compliance
- Insurance Obligations

# Critical Parts of a Contract

**Clear and concise "Definition Section"**

- Data Exchanged/Shared
- Role in Data Transaction
- Specific Identification of Personal Data
- Data Law
- Data Subject Rights
- Security Incident

XPAN LAW

# Critical Parts of a Contract

**Data**

- Type of data being impacted
  - PHI
  - Personal Data
- Role in data transaction
  - Covered Entity
  - Business Associate
  - Subcontractor of Business Associate

XPAN LAW

# Risk Mitigation

- Vendor Tracking
- Vendor Auditing
- Vendor Ranking and Rating
- Comparison of Professionals

XPAN
LAW

# Playbook

# Challenges-Overall

- **One size does not fit all.**
- **Multiple obligations dealing with multiple laws.**
- **Dynamic regulatory environment.**
- **Rapidly evolving technology landscape.**
- **Heavy reliance on third-party support creates increasing risk and liability to fiduciary.**
- **Lack of understanding of data. (Sensitive Data vs. Healthcare Data vs. Children's Data vs. Personal Data vs. FERPA-Related Data)**

# Challenges-Overall

- **Lack of experienced professionals.**
- **No definition of plan assets by courts or regulators.**
- **Plan fiduciaries are on notice**
- **Limits of insurance.**
- **Insurance coverage based on procedures and implementation becoming intertwined.**
- **Increase in regulatory oversight that will lead to more laws, fines, lawsuits, obligations… the parade of horribles.**

# Challenges-Third Party

- **All of the above…PLUS**
- **Lack of engagement with third-party vendors**
- **Complaints and inconsistencies in questionnaire responses**
- **Insufficient resources to respond, track, and monitor (Vendor and Fund)**
- **Cost (time and money)**
- **No direction- what do I do with this?**

# Vendor Assessments

- Contractually Required
- Ranking of Vendors
- Periodic Assessments
- Review of Access Controls
- Review of Encryption Protocols
- Review Incident Response Plan
- Testing
- Personnel and Training

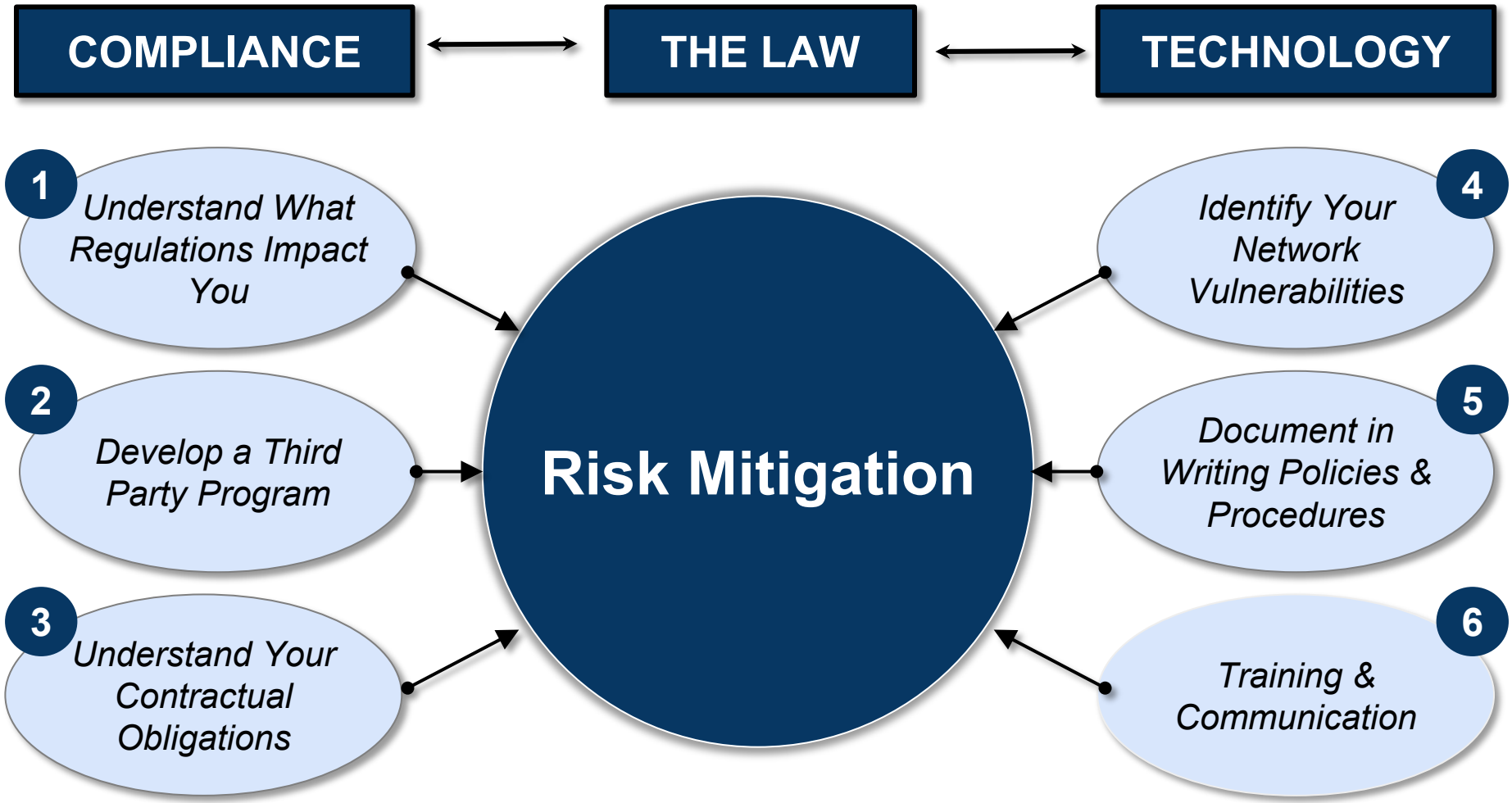
XPAN LAW

# What Should You Do

- Have a data privacy and cybersecurity impact assessment performed.
- Map your organization's data.
- Ensure online Privacy Policy and Terms of Use/Service is up-to-date.
- Penetration Testing.
- Obtain appropriate cyber-liability and data privacy insurance.
- Create appropriate documentation to demonstrate compliance (internal controls) with any applicable data privacy law/regulation and cybersecurity best practices.

# What Should You Do

- Employee TRAINING
- Data breach response plan
- Incorporate data privacy and cybersecurity language into contracts and engagement agreements.
- Create a formalized third-party management program with clear metrics
- START TODAY!!!


COMPLIANCE
THE LAW
TECHNOLOGY
1
Understand What Regulations Impact You
2
Develop a Third Party Program
3
Understand Your Contractual Obligations
Risk Mitigation
4
Identify Your Network Vulnerabilities
5
Document in Writing Policies & Procedures
6
Training & Communication