

# CYBERSECURITY IN 2024

ANDREW LIN  
MOONEY, GREEN, SAINDON,  
MURPHY AND WELCH, PC

OWEN RUMELT  
CARY KANE PLLC

PREPARED FOR:



2024 ADVANCED ERISA SEMINAR

# CYBERSECURITY IN 2024

## 1. SOURCES OF LAW AND DUTIES

- a) For Attorneys – Rules of Professional Conduct
- b) Statutory Requirements
- c) EBSA Cybersecurity Guidance

## 2. ADVISING BENEFIT PLAN CLIENTS

- a) Plan Management
- b) Provider Management

## 3. RESPONDING TO DATA BREACHES

## 4. LOOKING FORWARD



# SOURCES OF LAWS AND DUTIES:

## ATTORNEY RULES OF PROFESSIONAL CONDUCT

*“Law firms are considered by attackers to be ‘one stop shops’ for attacks because they have high value information of multiple clients that is well organized, often with weaker security than clients.”*

*-David Ries, Clark Hill PLC*



# SOURCES OF LAWS AND DUTIES:

## ATTORNEY RULES OF PROFESSIONAL CONDUCT

Approximately 25% of law firms have experienced a security breach.

- 17% of 1-9 attorneys
- 35% of 10-49 attorneys
- 46% of 50-99 attorneys
- 35% of 100+ attorneys

-ABA Tech Report 2021



# SOURCES OF LAWS AND DUTIES:

## ATTORNEY RULES OF PROFESSIONAL CONDUCT



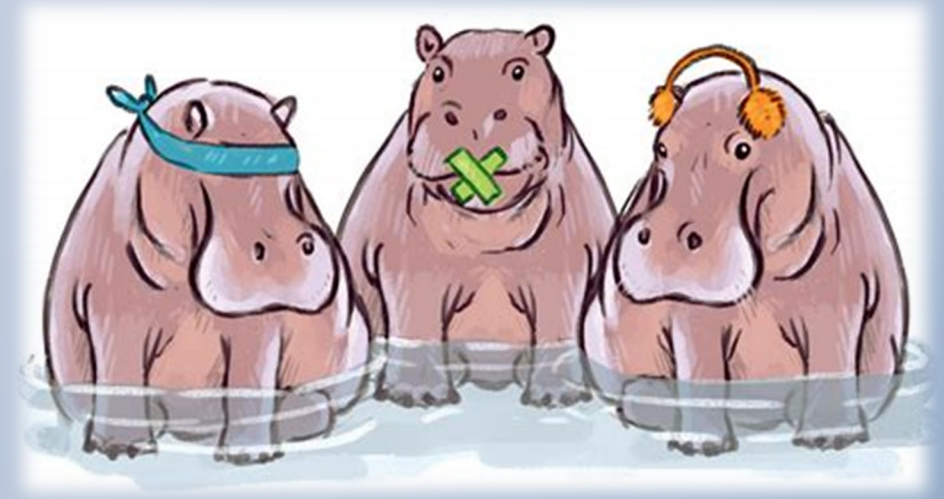
**RULES**

- **Model Rule 1.1 – Competence**
  - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
- **Model Rule 1.4 – Communications**
  - 1.4(a) A lawyer shall . . . (3) keep the client reasonably informed about the status of the matter;
- **Model Rule 1.6 – Confidentiality of Information**
  - 1.6(c) - A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client

# SOURCES OF LAWS AND DUTIES:

## FEDERAL LAW: HIPAA

- Provides security and privacy rules governing private health information
- Applies to covered entities and their service providers (business associates)
- Protected Health Information (PHI)
- Penalties range anywhere from \$100 to \$1.5 million per violation



# SOURCES OF LAWS AND DUTIES:

## FEDERAL LAW: ERISA

### § 404 Prudent man standard of care

[A] fiduciary shall discharge his duties with respect to a plan solely in the interest of the participants and beneficiaries and—

(A) for the exclusive purpose of (i) providing benefits to participants and their beneficiaries . . .

(B) 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 in the conduct of an enterprise of a like character and with like aims;

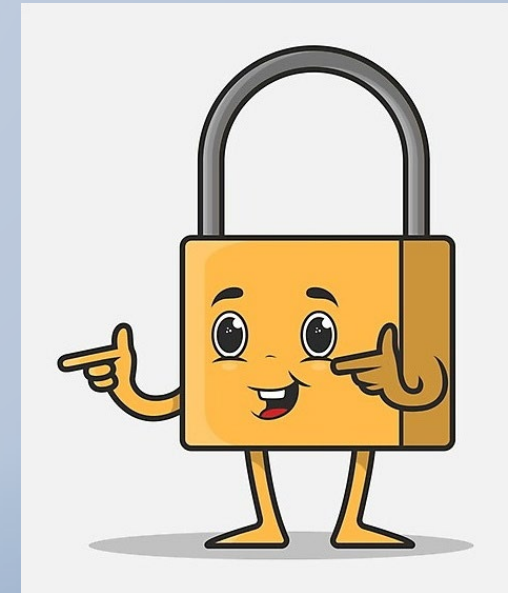
(D) in accordance with the documents and instruments governing the plan . . .



# SOURCES OF LAWS AND DUTIES:

## REGULATORY GUIDANCE: EBSA CYBERSECURITY BEST PRACTICES

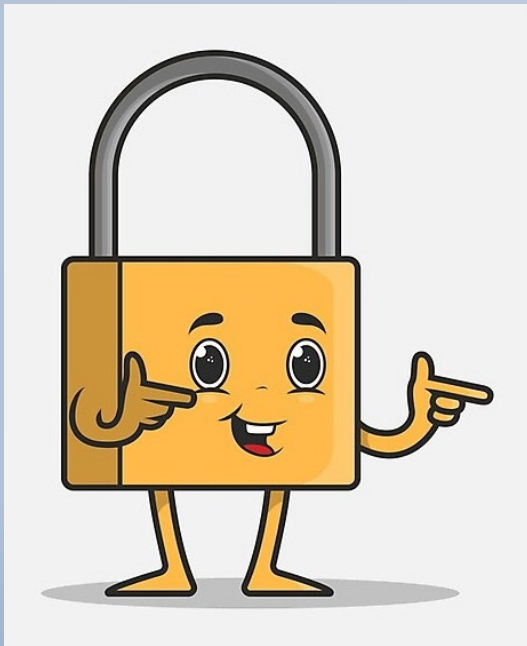
1. Have a formal, well-documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets and data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.





# SOURCES OF LAWS AND DUTIES:

## REGULATORY GUIDANCE: EBSA CYBERSECURITY BEST PRACTICES





7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.



# ADVISING BENEFIT PLAN CLIENTS: PLAN MANAGEMENT

Have a formal, well-documented cybersecurity program.

Have a reliable annual third-party audit of security controls.



# ADVISING BENEFIT PLAN CLIENTS: PLAN MANAGEMENT

Have strong access control procedures.

- All employees use unique, strong passwords.
- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
  - Deploy phishing-resistant Multi-Factor Authentication (MFA) if possible
  - Implement MFA on Internet-facing systems.
  - Require MFA to access areas of your network with sensitive information (PII, PHI, etc.)



# ADVISING BENEFIT PLAN CLIENTS: PLAN MANAGEMENT



Conduct periodic cybersecurity awareness training.

Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

# ADVISING BENEFIT PLAN CLIENTS: PROVIDER MANAGEMENT

Ensure that any assets and data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.

- EBSA Tips for Hiring a Service Provider with Strong Cybersecurity Practices (updated)
- Provider Questionnaires



# RESPONDING TO DATA BREACHES:

## 1. Initial Investigation and Assessment

- How? When? Where? Who?
- Affected participants / beneficiaries?
- What data? PHI?
- Is situation contained?

## 2. For provider breaches, review provider contract

## 3. Review of Legal Obligations



# RESPONDING TO DATA BREACHES:

## 4. “Internal” Notice

- Trustees, insurance carriers, IT/MS provider

## 5. Preparation and Issuance of Statutory Notices

- State data breach laws
- HIPAA

## 6. Incident Documentation



# RESPONDING TO DATA BREACHES:

## State data breach notice laws vary by:

- Threshold of affected residents triggering required action
- Kinds of protected data elements
- How much detail regarding the breach must be described
- Notice deadlines
- Whether regulators, attorneys general, media must be also be informed
- Whether consumer protection services must be offered
- Additional notices or terms that must be included in the notice



# CYBERSECURITY: LOOKING FORWARD



- Artificial Intelligence
- Role of Privacy Law
- Other Security Standards
- Broader Cyber Trends

# Questions?

