


ERISApedia.com  
Get Answers. Win Clients.

## DOL Cybersecurity Guidance is Out: Now What?



**Alison J. Cohen, J.D., APR**

FERENCZY BENEFITS LAW CENTER  
ERISA  
We are your guide to solutions.

---

---

---

---

---

---

---




---



---

---

1

## Your Co-Hosts

- Joanne Pecina 
- Maureen Pesek 
- Tim McCutcheon 

2

---

---

---

---

---

---

---

---



---

---

2

## During the Webinar

- All attendees' lines are muted.
- Question board is available and monitored - look for Q&A icon on webcast toolbar. Please do not use chat to ask questions.
- Slides and a recording of the webinar are also available on the ERISApedia.com webcasts webpage.
- Please note that you must access the live video portion of the webcast to get CE credit.
- Merely listening on a call-in line or watching a webcast recording is not sufficient for CE credit.

3

---

---

---

---

---

---

---

---



---

---

3

### During the Webinar

- Credit is offered for ERPA/ASPPA-ARA/NIPA.
- Those who attend the requisite time in the video portion of the webcast today will receive a certificate by email in a few days (ERPA will take several days longer). Please check your spam folder.
- Questions about CE credit: [support@erisapedia.com](mailto:support@erisapedia.com).
- After the main presentation, please join us for a brief educational session on how to find more information on today's topic on ERISApedia.com.
- After, you will be presented with a short Google Forms survey. Please let us know how we are doing.

---

---

---

---

---

---

---

---

4

### Your Presenter Today

**Alison J. Cohen, APA., APR**  
**Ferenczy Benefits Law Center**






---

---

---

---

---

---


---



---

5

### Agenda

- DOL Guidance Released April 2021
- Where Should a TPA Start?
- Cyber Insurance
- IT Audits
- Cyber Policies – internal and external



---

---

---

---

---

---

---

---

6

### CyberSecurity in the News

- The Government Accountability Office (GAO) has issued a report calling for federal action
  - Cited the vast amount of personal data involved
  - Covers 106 million Americans & \$6.3 trillion
  - Global cyber crime has more than doubled since 2015
  - Calls for comprehensive cybersecurity strategy, federal response initiatives, national data standards





---

---

---

---

---

---



---

---

7

### CyberSecurity in the News (Cont.)

- GAO Report calls for Department of Labor to take on the initiative
- Could become a cited plan fiduciary responsibility under ERISA
- Hearings for Deputy Secretary of Labor, Julie Su, spent time on the subject
- Currently, each state has its own set of laws/notice requirements which can make timely responses to an incident more difficult

---

---

---

---

---


---

---



---

8

### DOL Guidance Released April 2021



- Guidance came in three forms:
  - Tips for Hiring a Service Provider – designed for Plan Sponsors
    - Service Providers should understand what Plan Sponsors will be asking for
  - Cybersecurity Program Best Practices – designed for Service Providers
    - Detailed information on what providers should have
  - Online Security Tips – designed for Individuals/plan participants

---

---

---

---

---

---

---

---

9

## Tips for Hiring a Service Provider

- Look for service providers that follow a recognized standard for information security and use an outside auditor to review and validate the cybersecurity
- Ask how the provider validates its practices, what levels of security standards it has met and implemented
- Evaluate the providers track record in the industry
- Ask about any prior security breaches
- Make sure the provider has cyber insurance!!!
- Provider contract should require ongoing compliance with cyber/info security standards



10

10

---

---

---

---

---

---

---

---

## Best Practices for Providers

- A formal, well documented cybersecurity program
  - Identify the risks
  - Protect each of the assets, data, & systems
  - Detect and respond to event
  - Recover from the event
  - Disclose the event
  - Restore normal operations & services



11

11

---

---

---

---

---

---

---

---

## Best Practices for Providers (Cont.)

- Prudent Annual Risk Assessments
  - Identify, assess, and document how identified risks or threats are evaluated & categorized
  - Establish criteria to evaluate the confidentiality, integrity, & availability of the systems
  - Describe how the program with mitigate or accept the risks identified
  - Facilitate the revision of controls due to changes in technology or emerging threats
  - Be kept current to account for changes to systems



12

12

---

---

---

---

---

---

---

---

### Best Practices for Providers (Cont.)

- Reliable Annual Third-Party Audit of Security Controls
  - “EBSA would expect to see:”
    - Audit reports, audit files, penetration test reports and supporting document, and any other analyses
    - Audits and audit reports prepared/conducted in accordance with appropriate standards
    - Documented corrections of any weaknesses identified in the independent third-party analyses



13

13

---

---

---

---

---

---

---

---

### Best Practices for Providers (Cont.)

- Strong Access Control Procedures
  - Access to systems is limited to authorized users, processes, devices, activities, and transactions
  - Access privileges are limited based on role of the individual
  - Access privileges are reviewed at least every 3 months
  - All employees use unique, complex passwords
  - MFA is used wherever possible
  - Policies, procedures, and controls implemented to monitor the activity of authorized and unauthorized access
  - Procedures to ensure participant data matches employer data



14

14

---

---

---

---

---

---

---

---

### Best Practices for Providers (Cont.)

- Clearly Defined and Assigned Info Security Roles and Responsibilities
  - Do you have a Chief Information Security Officer?
- Any Data Stored in Cloud Environment Must be Subject to Appropriate Security Reviews
  - Require risk assessment of third-party service providers
  - Periodically assess third party service providers based on potential risks
- Cybersecurity Awareness Training Conducted Annually for All Personnel (& Updated to Reflect New Risks)



15

15

---

---

---

---

---

---

---

---

## Best Practices for Providers (Cont.)

- Secure System Development Life Cycle Program (SDLC)
  - Practices for creating internal systems to ensure protections are built-in
- Business Resiliency Program
  - Disaster Recovery, Business Continuity, and Incident Response Plans
- Encryption of Sensitive Data Stored and in Transit
- Strong Technical Controls Implementing Best Security Practices
  - Hardware, software, and firmware kept up to date
- Responsiveness to Cybersecurity Incidents or Breaches



16

---

---

---

---

---

---

---

---

16

## Where Should a TPA Start?

- Wow. That's quite a list!
- Step One: Review list and determine which boxes you already check
  - Likely, you already use secure portal or email
- Step Two: If you don't already have cybersecurity insurance, don't hesitate – call your agent today!
  - Don't believe that you can never be a target of cyber attacks



17

---

---

---

---

---

---

---

---

17

## Where Should a TPA Start? (Cont.)

- Step Three: Build Your Binder
  - A good Incident Response Plan is both electronic and in paper
    - If your database becomes corrupted, you won't be able to get to the electronic version
  - Binder Contents:
    - Copy of Cybersecurity Insurance Policy
    - Contact Information – attorney, insurance carrier, IT team, contacts at system vendors, etc.



18

---

---

---

---

---

---

---

---

18

### Where Should a TPA Start? (Cont.)

- Step Three: Build Your Binder (cont.)
  - Binder Contents:
    - Written policy/procedure for handling incident response
    - Pre-written communications for clients that have been approved by legal/insurance
      - Include out of office replies if email has to go down
    - Checklist for returning business to normal after cleared by IT
- Step Four: Start building your policy/procedures



19

---

---

---

---

---

---

---

---

19

### Understanding CyberSecurity Insurance

- This is NOT your E&O Coverage Policy
- Separate coverage will need to be obtained
- Average costs of a PII breach incident:
  - Initial mailing - \$1.50 per participant
  - 25% will request identity monitoring (costs range from \$25 - \$75 per participant)
  - If any participant experiences theft actions, then \$100 - \$125 per contact



20

---

---

---

---

---

---

---

---

20

### Understanding Cybersecurity Insurance

- Coverage for data corruption, Malware, or ransomware attack is separate from breach of participant data
- Coverage from identity theft is also separate
- Cyber insurance generally includes media liability coverage
  - Access to IT forensic specialists and the breach notification services for customers



21

---

---

---

---

---

---

---

---

21

## IT Audits

- No current standards or terminology like 'full scope versus limited scope' that you may be used to
- Try asking your cyber insurance provider for a list of their preferred vendors
  - May be entitled to a discount on services or premiums for doing the audit
- Asking fellow TPAs or attorneys for recommendations



22

22

---

---

---

---

---

---

---

---

## IT Audits (Cont.)

- Assessments/Tests generally included:
  - Data gathering
  - Current state analysis
  - Risk assessment
  - Vulnerability assessment
  - Penetration testing
- Vendor may also make 'white hat' hacking services available (if you can take the heat)



23

23

---

---

---

---

---

---

---

---

## IT Audits (Cont.)

- Written report to be delivered with the results
  - Meeting should be held to review the results and hear the suggested changes
  - DON'T get defensive, these folks are here to help
- Document any changes made by the organization based on the review
- Plan on having an annual or bi-annual review of the system because threats change constantly!



24

24

---

---

---

---

---

---

---

---



## External Cyber Policy

- Don't give away the keys to the kingdom
  - External policy document shouldn't explain details of safety protocols in place
- Use the DOL guidance to create the key points that will be asked for in proposal requests
- Policy must be honest (don't say you have cyber insurance, if you don't)
- Outline steps being taken to protect information in general terms



25

---

---

---

---

---

---

---

---

## Internal Cyber Policy

- Recommended general outline:
  - Identify who is responsible for what
  - Who should be notified and when
    - Before you disclose to your client(s), talk to your legal counsel
  - Security Protocols in place and schedule for review/updates
  - Schedule for independent third-party IT audit

26

---

---

---

---

---

---

---

---

## Internal Cyber Policy (Cont.)

- Recommended general outline:
  - Levels of security access for personnel
  - Schedule for access review
  - Removal of access procedures for terminated personnel
  - Response protocols
    - Communication content/procedures
    - When and how to bring down your system
    - Recovery process after IT clears the threat

27

---

---

---

---

---

---

---

---

## Internal Cyber Policy (Cont.)

- Recommended general outline:
  - Response protocols should be created for different types of threats
    - Ransomware/System Malware
    - Stolen PII
    - Identity Theft – unique participant impact
  - Outline operations during system shutdown
    - What will you expect from your employees?
    - Can you handle partial shutdown easier?



28

28

---

---

---

---

---

---

---

---

## Common Questions from TPAs

- Do I really need cyber insurance?
- We use XXX as our software vendor, so what should we do to make sure they are safe?
- Do you think the DOL will make this mandatory?
- Does my service agreement have the necessary language?
- How quickly do we need to have all of this in place?



29

29

---

---

---

---

---

---

---

---

## Questions?



30

30

---

---

---

---

---

---

---

---

### Contact Information

**Alison J. Cohen, J.D., APR**

Co-Author of Plan Corrections eSource

678.399.6604 (V)

404.320.1105 (F)

acohen@ferenczylaw.com



31

31

---

---

---

---

---

---

---

---

---

---

### CE Credit

- Credit is offered for ERPA/ASPPA-ARA/NIPA
- Those that attended the requisite time in the live video portion of the webcast today will receive a certificate by email in a few days (ERPA will take longer).
- Please check spam folder.
- Any questions? Email: support@erisapedia.com.
- After the webcast you will be presented with a short Google Forms survey. Please let us know how we are doing.



32

32

---

---

---

---

---

---

---

---

---

---

### For Further Study

Joanne Pecina will demonstrate how to find more information on today's topic from the ERISApedia.com resources.



33

33

---

---

---

---

---

---

---

---

---

---