DEFINITI

DATA SECURITY

Is Your Service Provider Safeguarding Your Plan Data?

With cybercrimes on the rise, the Department of Labor released "Tips for Hiring a Service Provider with Strong Cybersecurity Practices." These six tips contain practical and timely ways to confirm how well a Third-Party Administrator (TPA) protects data.

Definiti takes its cybersecurity obligations seriously and invests heavily to keep client data secure. Definiti responds to each DOL tip here, outlining its recommendations and summarizing what to expect when you partner with Definiti.

DOL TIP #1

Ask about information security standards, practices and policies and audit results.

DEFINITI SAYS

Documented processes, confirmed by third-party expert audits, are crucial elements of an organization's security posture. Review the TPA's Information Security Policy (and check the version date to ensure it is current). You can also request a Service Organization Control (SOC) audit that validates operating procedures as well as a financial audit that confirms the firm's fiscal health.

Definiti has a comprehensive Information Security Policy and conducts annual third-party SOC and financial audits as part of its commitment to best-practice professional standards.

DOL TIP #2

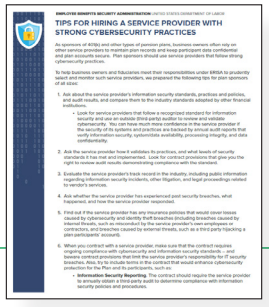
Ask how practices are validated, what levels of security standards are met and how results are audited.

DEFINITI SAYS

Have a conversation with the firm's Chief Information Officer to gain insight on security standards. Focus on the processes that are most critical to your relationship. For example, does the firm have written access controls? Screen every new employee? Mandate regular cybersecurity training? Safeguard systems and data with anti-virus software, program updates with robust backup and disaster recovery processes?

Definiti is proud to be one of the few TPAs with a dedicated Chief Information Officer; a highly secure, centrally managed cloud-based IT infrastructure; and comprehensive documented procedures and practices for information management.

Tips for Hiring a Service Provider With Strong Cybersecurity Practices


TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

Review the DOL's cybersecurity guidelines.

DOWNLOAD

DOL TIP #3

Evaluate the TPA's track record regarding information security, litigation and legal proceedings.

DEFINITI SAYS

Ask if the TPA ever experienced an information security breach or any litigation. It may be surprising what you will learn.

Definiti has a perfect track record of securing its information systems with no litigation or legal proceedings and is committed to keeping that record intact.

DOL TIP #4

Ask whether the TPA has experienced past security breaches, what happened, and how it responded.

DEFINITI SAYS:

The unfortunate reality is that data breaches are a matter of *when* not *if*. To understand if your TPA is prepared, ask: Who is authorized to lead the incident response? Are pre-screened, outside legal and cybersecurity experts on call? After such incidents, did the firm conduct a thorough postmortem to understand the root cause? How much is the firm investing to tighten security?

Definiti's Information Security Plan, regular upgrades and regular security reviews confirm it is poised for a swift, capable response if an event occurs.

DOL TIP #5

Find out if the TPA has insurance for cybersecurity, including breaches by internal or external actors.

DEFINITI SAYS

Cybersecurity insurance is increasingly important and especially vital for small TPAs that may not have the financial resources to recover from a cyberattack.

Definiti maintains comprehensive cybersecurity insurance, advised by brokers who specialize in the unique challenges of the retirement industry. Definiti has a solid foundation as a national firm with the financial resources to operate from a position of strength.

DOL TIP #6

Require ongoing compliance with cyber-security and information security standards.

DEFINITI SAYS

The TPA should address these important elements, especially if their information security posture is in question. Do not shy away from reviewing such documents as Information Security Plans, SOC audits and incident response procedures. Ask for proof of insurance coverage and talk with them regularly about their cybersecurity procedures in this quickly evolving technology environment.

Is the Service Provider Prepared to Protect Your Plan Data from Cyberthreats?

Too often, cybersecurity is presumed to be sufficient or ignored until it's too late. Start the dialog now with service providers – after all, it is a crucial part of being a responsible fiduciary and securing participants' assets.

Call or email to learn how Definiti responds to the DOL's cybersecurity recommendations. Your Retirement Plan Consultant or Regional Sales Consultant can put you in touch with Definiti's Chief Information Officer to discuss the procedures and policies that keep your data safe and secure.

1 (800) 882-4026

contact@definiti-llc.com