Patterson Advisors
Helping balance your means and your dreams.

Privacy Policy

including Physical Security and Cyber Security Policies

Patterson Advisors (PA) is committed to safeguarding the confidential information of its clients. All personal information provided to the firm is held in the strictest confidence. PA's Physical Security and Cyber Security polices describe a key part how we provide privacy for our clients' data. Below is a description of these two critical frameworks.

Physical Security refers to the security of PA's computers, printers, office equipment, furniture, supplies, PA working documents, written analyses and recommendations, and any of our client's physical documents.

Both Erin and Dave have **lockable** offices in their homes where they meet with clients on occasion. Each maintains folders in file cabinets (Dave's is lockable). Both Dave and Erin have monitored security systems for fire, medical and intrusion.

Physical documents provided by our clients are copied and scanned for encrypted storage on the servers holding all of the PA digital footprint. Once scanned and stored, client documents will either be shredded or returned to the client. PA has been moving in this direction the last few years.

Client documents older than five years will be shredded. All documents for past clients will be shredded once they are over five (5) years old. Ultimately (in five years' time) all of PA's client documents will be maintained only in encrypted digital format. This policy, once fully implemented, should safeguard 99% or more of client documents. In the interim, PA will encourage clients to only submit digital copies of their financial data. In fact, the majority of client data is already submitted to us in digital format.

Cyber Security refers to the security of all of PA's digitized assets including all of PA's business and client records.

Beginning in late 2024, PA began contracted service with JDCTek, (JDCTek.com) a highly respected provider of information technology services.

JDCTek was launched in May of 2007. They are an IT, Security and Compliance consulting company aiming to bring the highest level of technical expertise to small businesses around the Metro Detroit Area. They are continually advancing their service offerings as new technology trends evolve.

We have contracted JDCTek to implement the following:

- EDR (Endpoint Detection and Response) – which goes beyond traditional antivirus programs that detect and block known malware using signature-based detections. EDR continuously monitors endpoint activity in real-time to respond to more complex and emerging cyber threats.
- MDR (Managed Detection and Response) is a cyber security service that continuously monitors an organization's network and device's potential threats, analyzes suspicious activity and takes immediate action to respond and remediate security incidents.
- DNS Filtering -A DNS filter is a security tool that uses the Domain Name System (DNS) to block access to malicious websites by preventing a device from translating a website's name (like "google.com") into its corresponding IP address, essentially stopping one from reaching the site before it even loads. Hence DNS Filtering acts as a gatekeeper to protect against phishing and malware.
- Monitoring of our email to filter out phishing emails and quarantine emails from unsecure sites to prevent malware attacks, including ransomware attacks.
- Provide sharing of documents with clients, in either direction, utilizing Microsoft SharePoint to ensure privacy of the information.

We maintain secure password files and extra security biometrics and passwords to login to our computers. JDCTek maintains all of our software programs and ensure the latest software security patches are implemented on a timely basis. All digital data is encrypted using Axient x360Cloud. It is also backed up, recoverable and protected.

Please feel free to request more information from us regarding Axient x360 Cloud's key features, data policies and certifications.

Tyes of Client Data We Collect

In the course of working with clients, client information that is gathered is based on the objectives of the engagement. Information requested may include the following:

- personal information such as birth dates, health conditions, life expectancy, social security numbers (last four digits preferred), objectives, employment information, salary, etc.
- information on personal advisors
- financial, insurance and bank account information including balances, cost basis information, etc. Note that PA does not have access to client investment accounts.
- federal and state income tax information
- retirement plan and benefit information
- estate-planning information such as wills, trusts, powers of attorney, etc.
- budget information
- information on loans, accounts receivable, mortgages and credit cards
- information related to a client's business and other assets
- Any other information that could be pertinent to helping a client plan for their financial future.

Please Note: That this is not an exhaustive list. The information provided is unique to each client.

Other Access to Client Data

- PA has three information technology providers that provide services to PA: MoneyGuidePro®, a financial planning software vendor, Holistiplan®, a tax return analysis software vendor and JDCTek, our hardware, software and security management firm. All three providers have access to varying degrees of our client data. We share no data with MoneyGuidePro® that would allow access to clients' investment accounts or Social Security information. Holistiplan is used to analyze client tax returns. Social Security numbers are redacted before loading client's tax returns to their website. Client names and addresses can be redacted as well, if requested. JDCTeK monitors all aspects of our computer activities to protect our clients' data.
  `
- We try to redact all client Social Security numbers, but in rare cases, we may have a few unredacted SS numbers in our files. We have no access to client investment accounts or passwords. While all our data is encrypted, JDCTeK has the capability, if desired, to access the clients' data that we do have. Software vendors may require access to the client databases on rare occasions to aid in software problem resolution or with new software upgrades.

- Our vendors lifeblood depends on their reputation as information technology providers that take care to keep client data secure. They have all been in business for many years and have solid reputations. Because we limit our own access to your data, that limits our vendors access, as well. We have high confidence that your data is safe and has a low-risk exposure for your finances.

- On occasion, Federal and State regulators may review firm records as required by law.

- No client information of any kind is provided to mailing list vendors or solicitors.

- No client information will be shared with a client's attorney, accountant, insurance companies, investment representatives or similar parties without first obtaining the client's approval.

- As CFP® certificants, we may be asked to disclose client data to the Certified Financial Planner Board of Standards Inc. as part of complying with the CFP Board's *Code of Ethics and Standards of Conduct*. If you prefer that we do not disclose non-public personal information about you to the CFP Board, you may opt out of such disclosure by notifying us by email or by phone at (248) 895-0770. It should be understood that in the unlikely event that we are asked to disclose non-public information about you to the CFP Board, the Board would take all necessary steps to protect your privacy.

- Personally identifiable information about clients will be maintained through the client engagement and for the time thereafter that such records are required to be maintained by the Federal and State securities laws and consistent with the CFP Board Code of Ethics and Professional Responsibility. After this required period of record retention, all such information will be destroyed.