# Questionnaire

www.commwestcorp.com

## Compliance with Data Privacy and Security

## Compliance is not a cost of doing business; it's an investment in staying in business.

The following is a broad list of what a firm needs to comply with. Yes- depending on your industry, size, location, and other variables, your specific needs may change.

- Legal and Regulatory Compliance
- Financial and Tax Compliance
- Employment and Labor Law Compliance
- Occupational Safety and Health Administration Standards
- Data Privacy and Security Compliance
- Environmental Compliance
- Contractual Compliance
- Ethical and Corporate Governance Compliance

While we are unable to provide advice on every one of these compliance-related duties, we can speak into the part of your business technology: **Compliance with Data Privacy and Security.**

Here are two **FACTS**:

1. Your company must comply with regulations to safeguard the private data of your clients and staff. (SOX, PCI, HIPAA, and GDPR)
2. Your company must have cybersecurity safeguards in place to shield private information from breaches, illegal access, and other threats.

This means you need to think about **HOW** you are meeting these requirements and complying with standards. To get you started, here is a variety of questions:

### *General Business Administration & Policy*

- Do you know your company's compliance requirements?
- Have you established and upheld BAAs with vendors or suppliers who have access to your electronic health information?
- Do you have a cybersecurity insurance plan? Are you meeting the cybersecurity requirements for the plan?
- When was your last complete risk assessment performed?
- Do you have a disaster recovery plan? Is it accessible in an emergency?

CommWest
Your Communications • Our Business

## *Adminstration of Users & Devices*

- Does each user have a unique user ID, a complicated password, and multi-factor authentication when accessing systems containing sensitive data?
- Is a VPN or remote access program used to gain remote access to systems containing sensitive data?
- Do all devices (including BOYD) have antivirus software installed and properly overseen?

## *Protecting Your Business Data*

- How are you backing up your critical data? (Encryption keys, break-glass passwords)
- How long can you afford to be down? How much data can you lose without critical impact on your business?
- Is all private information encrypted both in transit and at rest?
- Are employees receiving training on phishing prevention and email security awareness?
- How are software and operating system patches found, applied, and validated?

## *Cloud Systems*

- Do your on-premises systems and cloud resources receive the same security considerations?

### Compliance is not a one-time event; it's an ongoing process.

Addressing these compliance questions proactively can save you time, money, and headaches in the long run. Don't wait until it's too late. Contact us for a consultation, and we'll guide you through the process, providing advice and referrals to trusted partners who can help you achieve full compliance with Data Privacy and Security.