CanDoTech Consulting Inc.
Fully Managed Small Business IT Services
Your Outsourced IT Department

AVOIDING HIPPA, PCI, AND DSS RISKS AND VIOLATIONS.

To avoid HIPPA (health insurance portability and accountability act), PCI (payment card industry), and DSS (data security standard) risks and violations, organizations handling protected health information (PHI) and payment card data should implement the following measures:

1. HIPAA COMPLIANCE:

A. RISK ASSESSMENT: Conduct regular risk assessments to identify potential vulnerabilities and risks to PHI. Address any identified weaknesses promptly.

B. ADMINISTRATIVE SAFEGUARDS: Implement administrative controls, including policies, procedures, workforce training, and access controls, to ensure the confidentiality, integrity, and availability of PHI.

C. PHYSICAL SAFEGUARDS: Secure physical access to PHI storage areas with appropriate measures like access controls, video surveillance, and visitor management.

D. TECHNICAL SAFEGUARDS: Implement technical measures like access controls, encryption, audit logs, and secure messaging to protect phi during transmission and storage.

E. BUSINESS ASSOCIATE AGREEMENTS: Establish and maintain business associate agreements with third parties handling PHI to comply with HIPAA.

2. PCI DSS COMPLIANCE:

A. NETWORK SEGMENTATION: Isolate systems that handle cardholder data from other networks to minimize the scope of PCI DSS requirements.

B. SECURE CARDHOLDER DATA STORAGE: Encrypt cardholder data, both in transit and at rest, to protect it from unauthorized access. Implement strong access controls and secure storage mechanisms.

C. REGULAR VULNERABILITY SCANNING AND PENETRATION TESTING: Conduct periodic scans and tests to identify vulnerabilities in the network infrastructure and applications. Promptly address any findings.

D. ACCESS CONTROLS: Limit access to cardholder data on a need-to-know basis. Assign unique IDs to each person with computer access and implement strong authentication mechanisms.

E. REGULAR MONITORING AND LOGGING: Use robust logging to track access and monitor cardholder data. Monitor for suspicious activity and compromise indicators on systems and networks.

3. DSS COMPLIANCE:

A. BUILD AND MAINTAIN A SECURE NETWORK: Install and maintain a firewall configuration to protect cardholder data. Regularly update firewall software and implement strong access controls.

B. PROTECT CARDHOLDER DATA: Encrypt cardholder data during transmission over public networks. Use secure protocols (such as TLS) for data encryption.

C. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM: Implement a process for identifying and addressing security vulnerabilities through patch management, vulnerability scanning, and remediation.

D. IMPLEMENT STRONG ACCESS CONTROL MEASURES: Restrict access to cardholder data on a need-to-know basis. Assign unique user ids and implement two-factor authentication.

E. REGULARLY MONITOR AND TEST NETWORKS: monitor network access and data, use intrusion detection/prevention systems, and conduct security tests regularly.

Review HIPAA, PCI DSS, and DSS requirements for compliance. Engage with experts and conduct regular audits to stay informed of updates and changes for ongoing adherence and effective protection of sensitive data.