

HEALTHCARE'S PAYMENT CARD COMPLIANCE RISKS





Healthcare organizations are facing unprecedented cyberattacks that target sensitive information, including highly sought-after payment card data. Healthcare entities face financial penalties, legal costs, and brand reputational damage in the event that systems are breached and payment card data is exposed.



PENALTIES FOR FAILURE TO COMPLY WITH PCI-DSS REQUIREMENTS

- ✘ Breach fines (500k+ or \$5,000 - \$100,000 per month)
- ✘ Cost for a forensic investigation
- ✘ Associated costs for card re-issuing, fraud monitoring, etc.
- ✘ Transaction fee increases
- ✘ Potential cost of FTC audits for 20 years
- ✘ Potential litigation (some states have laws that protect affected individuals)
- ✘ Reclassification as a level 1 merchant (higher standard of compliance)
- ✘ Reputational damage
- ✘ Interchange rate increases or organization is no longer able to accept payment cards

WHERE IS PCI CARDHOLDER DATA PROCESSED FOR HEALTHCARE ORGANIZATIONS?

 Inpatient registration	 Outpatient office co-pays	 Web-based patient payments	 Fitness centers
 Gift shops	 Foundation and donations centers	 Cafeteria	 Pharmacy

WHAT SYSTEMS MANAGE PCI CARDHOLDER DATA?

- On-premises servers
- Payment card readers
- Workstations
- Third-party transaction processing applications
- Network devices (transmission)
- Web applications
- Call center applications and VOIP systems
- Fax machines and multi-function devices
- Shared drives
- Paper files
- Point-of-sale devices
- Email

COMMON CHALLENGES FOR PCI COMPLIANCE FOR HEALTHCARE ORGANIZATIONS

- Understanding and documenting payment card processes and credit card environment
- Lack of centralized processes and management
- No network segmentation; PCI controls subject to the entire environment
- Tracking and monitoring of access to payment card systems and data
- Security event monitoring across a disparate environment
- Encryption of payment card data
- Limited security capabilities of legacy systems and applications
- Lack of PCI contractual language for third-party service providers
- Obtaining management support to perform remediation
- Lack of skillset or personnel that understand PCI
- Lack of funding to support PCI compliance

MEDITOLOGY'S PCI-DSS CAPABILITIES

 PCI-DSS Qualified Security Assessor (QSA)	 Approved Scanning Vendor (ASV)	 Dedicated exclusively to the healthcare industry	 Full suite of PCI-DSS services
--	---	---	---

Ranked #1 Best in KLAS for Cybersecurity Advisory Services in 2019 and 2020, Meditology Services and Meditology Assurance are leading providers of information risk management, cybersecurity, privacy, and regulatory compliance consulting services, exclusively for healthcare organizations.