



# **BEST PRACTICES FOR COMMERCIAL COMPLIANCE**

## **CONTENTS**

OVERVIEW .....	3
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996 .....	4
SARBANES-OXLEY ACT (SOX) OF 2002 .....	4
GRAHAM-LEACH-BLILEY ACT (GLB) OF 1999 .....	4
PAYMENT CARD INDUSTRY (PCI) OF 2004 .....	4
CONCLUSION .....	5
EXAMPLES OF CARPATHIA'S DEFENSE-IN-DEPTH CONTROLS TO ENSURE COMPLIANCE: .....	5
APPENDIX A .....	6

## OVERVIEW

Since the passing of the Privacy of Information Act of 1974, both the U.S. Government and the private commercial industry have continued to pass laws and enact self-regulation to protect the confidentiality and integrity of personal or financial information housed on electronic information systems.



These compliance laws and regulations combine to protect different types of data—from Personally Identifiable Information (PII), to Protected Health Information (PHI), to financial reports such as banking statements, earning statements, balance sheets and account ledgers. And becoming compliant with these regulations is not simply an option. Failure to comply can subject a company or organization to punitive fines, imprisonment or the loss of the right to provide a service, such as credit card payments.

Information system professionals are on the front lines of regulatory compliance and are tasked with the responsibility of implementing the controls and countermeasures required to protect data and achieve a successful compliance accreditation. And that's not all—companies must also provide auditable evidence to

validate the controls. Most commercial organizations such as hospitals, financial firms and retail businesses must implement controls, policies and procedures that comply with one or more of the following regulations:

- ◆ Health Insurance Portability and Accountability Act (HIPAA) of 1996
- ◆ Sarbanes-Oxley Act (SOX) of 2002
- ◆ Graham-Leach-Bliley Act (GLB) of 1999
- ◆ Payment Card Industry (PCI) of 2004

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996

HIPAA was sponsored by Senator Ted Kennedy and was enacted by Congress in 1996 to protect health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.

Information system professionals are on the front lines of regulatory compliance and are tasked with implementing the controls and countering measures required to protect data.

The HIPAA Privacy Rule and the Security Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate IT security safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. Security Rule deals specifically with Electronic Protected Health Information (EPHI).

## SARBANES-OXLEY ACT (SOX) OF 2002

The Sarbanes-Oxley Act, also known as the "Public Company Accounting Reform and Investor Protection Act," "Corporate and Auditing Accountability and Responsibility Act" and commonly called Sarbanes-Oxley or SOX, passed on July 30, 2002 and is a United States federal law that sets new or enhanced standards for all U.S. public company boards, management and public

accounting firms. SOX contains 11 titles that describe specific mandates and requirements for financial reporting and only applies to publicly traded companies.

With the passing of SOX, the corporate board saw more responsibility to oversee and strengthen corporate accounting controls and reporting methods, or otherwise risk fines or imprisonment. Part of implementing these controls requires public corporations to protect the integrity and confidentiality of corporate information, meaning corporate IT departments must implement IT security controls that ensure access to information is auditable and protected from unauthorized disclosure or modification.

## GRAHAM-LEACH-BLILEY ACT (GLB) OF 1999

The Graham-Leach-Bliley Act (GLB) is a comprehensive federal law affecting financial institutions, requiring them to develop, implement and maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of customer information. GLB enforces and controls how financial institutions disclose, store and collect customers' personal information by outlining a list of financial privacy and safeguard rules that must be implemented by the information owner. Failure to comply may result in fines or imprisonment.

## PAYMENT CARD INDUSTRY (PCI) OF 2004

Payment Card Industry (PCI) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. Created to help payment card industry organizations that process card payments prevent credit card fraud, PCI compliance demands increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process or exchange cardholder information from any card branded with the logo of one of the card brands.

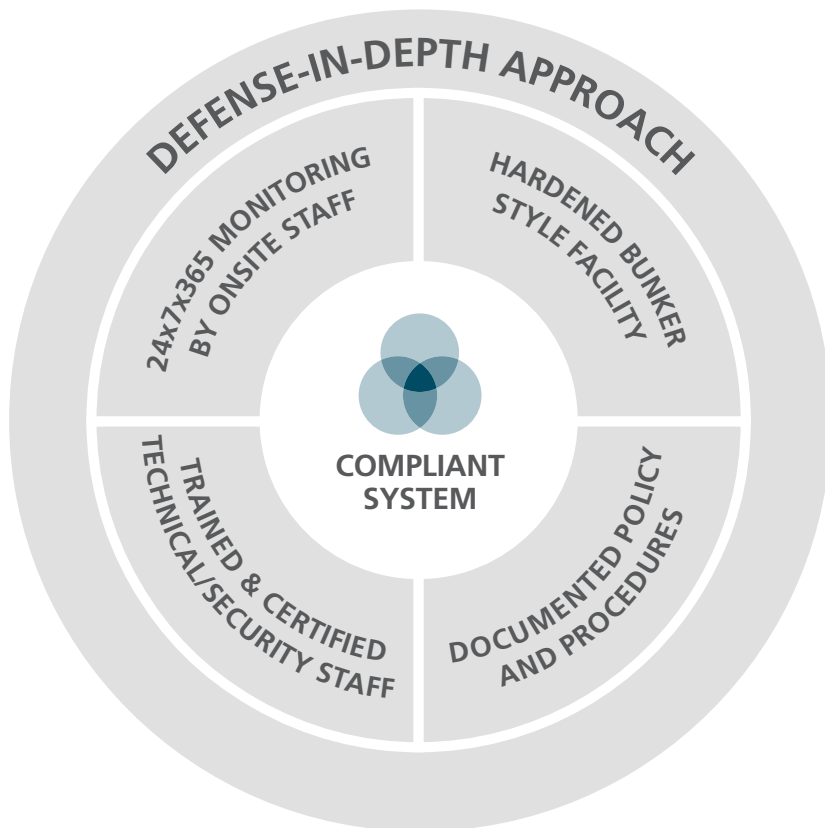
Validation of compliance can be performed either internally or externally, depending on the volume of card transactions the organization is handling. Regardless of the size of the organization, compliance must be assessed annually.

## CONCLUSION

So what do HIPAA, SOX, GLB and PCI have in common? Each regulation outlines controls that must be implemented to protect the integrity and confidentiality of personal and financial information. However, achieving HIPAA, SOX, GLB or PCI compliance can be costly and time consuming, as it requires a defense-in-depth approach—meaning the implementation of multiple layers of intrusion and access controls from the perimeter up to the system. Further, these regulations demand FTE's, compliant infrastructure and documented policy and procedures.

At Carpathia Hosting, we understand the challenges IT security professionals face in achieving compliance, managing risk and maintaining a secure and compliant baseline for the critical information systems.

We have oriented our entire business model around delivering infrastructure, services, policies and procedures that meet and exceed HIPAA, SOX, GLB and PCI compliance requirements. Our compliant solutions and controls have been independently validated across



a superset of commercial, federal and DoD compliance and regulatory requirements. Our compliant Tier III data centers and solutions are backed by 10 years of delivering 100% commercial, federal and DoD system compliance accreditations to our customers.

## EXAMPLES OF CARPATHIA'S DEFENSE-IN-DEPTH CONTROLS TO ENSURE COMPLIANCE:

### Physical

- ♦ Perimeter fencing
- ♦ Card Key or Biometric readers
- ♦ Security Guards
- ♦ CCTV
- ♦ Secure Media Handling
- ♦ N+2 on all critical infrastructure
- ♦ Fire and Smoke detection and suppression
- ♦ EMP and Tempest proof server rooms
- ♦ Access on need to know basis

### System

- ♦ 2 Factor Authentication
- ♦ Hardened OS
- ♦ Least privileges
- ♦ Account Management
- ♦ Anti-Virus and anti-malware
- ♦ HIDS
- ♦ Database encryption
- ♦ Backup and data archiving
- ♦ SNMP monitoring

### Network

- ♦ NIDS
- ♦ Firewalls on all external network perimeters
- ♦ DMZ's
- ♦ VLAN isolation

Carpathia's compliant solutions ensure that your information systems comply with commercial and federally-mandated requirements throughout the life-cycle of the system. And as a value add to our customers, Carpathia offers HIPAA, SOX and PCI certification and accreditation (C&A) professional services. For more information on our compliant services, visit our compliance website at <http://carpathia.com/compliantsolutions/index.html>.

## APPENDIX A

### Guidelines for Selecting a Compliant Hosting Provider

#### Guidelines

- ◆ Understand your compliance requirements
- ◆ Research data centers with past performance successfully achieving compliance accreditations.
- ◆ SAS 70 II certified
- ◆ Independently validate facility, people, process and services

#### Compliant facility

- ◆ Tier III facility
- ◆ U.S.-owned facility
- ◆ Hardened bunker style facility
- ◆ Mantrap
- ◆ Defense-in-depth
- ◆ N+2 on all critical infrastructure: Power and HVAC
- ◆ Emergency power shutoff at main entry doorways.
- ◆ 24x7x365 Roving guards
- ◆ Intrusion Detection: Card Key, Biometrics, CCTV, Door Alarms
- ◆ Fire prevention system
- ◆ Smoke Detection system
- ◆ Redundant and geographically diverse Internet Service Providers
- ◆ Low risk of Natural Disasters: Flooding, Hurricane or Earthquakes
- ◆ Armored Conduit
- ◆ Emergency lighting and facility evacuation diagrams
- ◆ Non-raised flooring
- ◆ Secure server rooms with need to know access

#### People who understand compliance requirements

- ◆ Experienced and compliance trained physical security staff
- ◆ Security engineer SME's
- ◆ Certification and Accreditation (C&A) professionals who understand compliance
- ◆ Experienced facility engineers who understand compliance
- ◆ Trained and certified systems engineers
- ◆ Trained and certified technical operations personnel

### GUIDELINES TO SELECTING A COMPLIANT HOSTING PROVIDER

- ✓ Compliant Facility
- ✓ Trained and Certified Personnel
- ✓ Compliant Policy and Procedures
- ✓ Compliant Services
- ✓ Compliant Hosting Qualifications

#### Compliant policy and procedures

- ◆ Documented policy and procedures that map to compliance controls and procedures.
- ◆ Physical access control policy
- ◆ Visitor access control policy
- ◆ Contractor access control policy and procedure
- ◆ Background Investigation on all employees
- ◆ Foreign National policy and procedure
- ◆ Secure median handling policy and procedure.
- ◆ Incident response policy and procedure.

#### Services

- ◆ Physical penetration testing
- ◆ Physical security services
- ◆ Secure media handling: GSA rated safes
- ◆ Strict adherence to compliance mandates
- ◆ Certification and Accreditation Services
- ◆ Compliant system and network engineered solutions
- ◆ Risk and vulnerability management
- ◆ NIDS and HIDS intrusion detection services
- ◆ Remediation services
- ◆ 24x7x365 technical support
- ◆ Patch management services
- ◆ Change management services
- ◆ Asset management services
- ◆ 24x7x365 system monitoring and alerting
- ◆ Compliant managed or colocation services
- ◆ Shipping and receiving services

Carpathia Hosting is a leading provider of managed hosting services, delivering secure, reliable and compliant IT infrastructure and management for some of the world's most demanding enterprises and federal agencies. Founded in 2003, Carpathia is a growing, profitable business run by a seasoned management team with deep experience in delivering enterprise hosting solutions including colocation, managed services and cloud computing. Carpathia's suite of services is designed for organizations seeking scalable, secure, robust and enterprise-grade hosting solutions that can be quickly provisioned or tailored to meet unique requirements. Backed by its E3 Promise, Carpathia consistently delivers an experience that exceeds customers' expectations. Carpathia qualifies as a small business. Contact Carpathia at 1.888.200.9494, or visit [www.carpathia.com](http://www.carpathia.com) for more information. References to other products are made to show compatibility. All companies and/or products mentioned in this document are registered or trademarked by their respective organizations. The inclusion of third party products does not infer endorsement by these parties, unless otherwise noted.