WHITE PAPER

Maintaining Compliance

No matter what type of business you're in, you could be affected by sweeping laws and regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountabilty Act (HIPAA) and the Sarbanes-Oxley Act (SOX). While each of these laws and regulations address different issues, they all are essentially about two main things: data security and individual accountability. So even if your business isn't directly impacted by these laws and regulations, understanding the rules and what it takes to be compliant could potentially save you headaches or penatlties, or even give your business an edge down the line.

Read on for more information about these laws and regulations, plus guidelines on making sure you're compliant and secure.

Related guides:

Preventing security threats and stopping unwanted activities

Managing data storage

Protecting your data

Restaurant owner takes compliance off the back burner

OBJECTIVE

- Prevent future security breaches into point-of-sales system after security breach was discovered.

SOLUTION

- Restaurant performed forensic audit to determine source of security breach and to identify other potential risks.
- Upgraded point-of-sale systems to those from a certified compliant vendor.
- Changed processes to ensure ongoing compliance and minimize risk of another breach.

RESULT

- $110,000 later, the restaurant is still in business and has resolved its compliance issues.
- Owner now carries a far deeper understanding of the significance of compliance rules.

For the full case study, please see our *Maintaining compliance* brochure.

CenturyLink™
Business

Make sure you're compliant

Do you have an understanding of what compliance means? And are you doing everything to meet the laws and regulations? If not, you could find yourself in a tough spot in the event of a security breach, fraud or an audit. Here are the basics of what you need to know.

PCI DSS (Payment Card Industry Data Security Standard)

The PCI DSS is a multifaceted security standard that not only sets rules for protecting customer account data, it also establishes penalties should that data be compromised.

Maintaining Compliance

Payment processors like Visa and MasterCard levy hefty fines for non-compliant merchants of any size. You can find documented details regarding PCI compliance and data security rules and regulations at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. Before visiting the website, make sure you know the principles and accompanying requirements as outlined in the PCI DSS[1]:

PRINCIPLE	STEPS TO IMPLEMENT
Build and maintain a secure network	• Install and maintain a firewall configuration to protect data (see the *Preventing security threats and stopping unwanted activities* white paper for more on security measures) • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	• Protect stored data electronically by way of firewalls and passwords and also by controlling physical access to this information • Encrypt transmission of cardholder data and sensitive information across public networks (encryption software is widely available; make sure you purchase a system that addresses PCI key management requirements)
Maintain a vulnerability management program	• Use and regularly update anti-virus software • Develop and maintain secure systems and applications
Implement strong access control measures	• Restrict access to data by business need-to-know • Assign a unique ID to each person with computer access • Restrict physical access to cardholder data
Regularly monitor and test networks	• Track and monitor all access to network resources • Regularly test security systems and processes
Maintain an information security policy	• Maintain a policy that addresses information security (this is a written statement that very clearly outlines your security procedures, rules and steps to take in the event of a breach)

[1] Source: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA establishes national privacy standards for safeguarding certain protected health information (PHI) processed and transmitted electronically. HIPAA covers:

- Health care providers
- Health plan organizations
- Health care clearinghouses
- Health care plans

Maintaining Compliance

One challenge with HIPAA compliance is that it is far-reaching in scope. Therefore, compliance comes not from implementing certain software or systems, but rather a holistic, best practices approach. Here are some basic guidelines to consider:

1. **Put someone in charge**
   Assign a person to be responsible for coordinating HIPAA activities and ensuring compliance. Having one person tracking it all will help make sure things don't get missed.
2. **Assess your security**
   Look at everything from how and where you store PHI, to email and chat encryption, to firewall and network security. For more information, see the CenturyLink white papers *Protecting your data* and *Preventing security threats and stopping unwanted activities*.
3. **Document everything**
   Document as many of your policies, standards and technology measures as possible.
4. **Restrict information access**
   Give each individual a unique identifier and restrict physical and electronic access to PHI and sensitive information on a need-to-know basis.
5. **Prepare**
   Put procedures in place to identify and respond to security incidents, minimize harmful effects and document the incidents.
6. **Seek HIPAA-compliant partners**
   Such partners include plan claim administrators, billing services and others.

Sarbanes-Oxley Act (SOX)

SOX sets stringent financial reporting requirements for U.S. publicly traded companies.[2] Although it only strictly affects public companies, many investors consider compliance a requirement to demonstrate sound financial reporting even in privately held businesses. So if you're hoping to attract investors to buy your business at some point, it may be prudent to consider adopting SOX compliance measures as a best practice.

Maintaining compliance

SOX presents companies with perhaps the most challenging set of requirements for attaining and maintaining compliance, partly because of the system-wide controls and manpower required, and also because of the high cost of performing the required audits to demonstrate compliance. But here are a few basic practices that could be helpful:

Compliance Q&A

Q: I'm a small merchant with very few card transactions. Do I need to be compliant with PCI DSS?

A: According to payment brand rules, all merchants and their service providers are required to comply with the PCI Data Security Standard in its entirety. Visit https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions to access different levels of compliance obligations.

Q: Are there off-the-shelf software systems that I can buy to make my business HIPAA-compliant?

A: Unfortunately, no. The best approach is to take a holistic look at your processes and design every step with HIPAA in mind.

[2] Public companies with market capitalization less than $75 million are currently exempt from SOX assessment.

(SOX) cont.

1. Comprehensive backup and searchable archiving of email, documents and all financial records.
2. Documenting and tracking of policies, processes and even laws and regulations.
3. IT general controls to demonstrate a procedure or policy for the management of fundamental organizational processes, such as risk management, change management, disaster recovery and security.
4. IT application controls to demonstrate that software applications used for specific business processes (such as payroll) are properly maintained, are only used with proper authorization, are monitored and are creating audit trails.
5. To make sure that your business is SOX compliant, it might be a good idea to contact an auditor specializing in the Sarbanes-Oxley Act, as there are far more complexities than we could cover here. But getting a basic understanding of the law will give you a great start.

Tip: **Qualified Security Assessors (QSAs) can provide on-demand data security and PCI compliance solutions to help merchants determine if they are compliant (or what they needed to achieve compliance). See a list of qualified QSAs at www.pcisecuritystandards.org.**

Need more? We're with you.

Your community representative is always happy to help. You can count on them as a resource for compliance solutions to consider that fit your specific business needs, budget and level of expertise, as well as advice and resources on a range of small business technology issues.

Visit **http://centurylink.com/smb-resources** to contact your community representative, and learn more about how technology can boost your business. You'll find information sheets, videos, case studies and more.

Service not available in all areas. Contact CenturyLink for details.

CenturyLink™
Business