FAXCORE®

Compliance:

Breaking down the misconceptions,
and how an advanced fax solution can help

Contents

Introduction

Businesses today have their work cut out for them when it comes to sending and receiving sensitive information. Whether this data belongs to customers, or is the company's own intellectual property, it represents a valuable target for hackers.

What's more, it isn't just external factors that organizations have to consider - there are also standards governing the practices of enterprises within specific industries, including health care and retail. Any firm that deals with sensitive patient data is beholden to the Health Insurance Portability and Accountability Act (HIPAA); similarly, all organizations that accept customer payments by credit or debit cards must adhere to the rules from the Payment Card Industry Data Security Standard (PCI DSS) or risk losing their merchant account.

These rules require specialized protection for sensitive, personal data, and many companies are turning to advanced fax solutions as a simple, streamlined and secure way to support their compliance.

Defining Compliance: HIPAA

HIPAA impacts organizations inside and outside the health care sector. Overall, it is a set of rules - including the Privacy Rule, Security Rule, Enforcement Rule and Omnibus Rule - that creates an industry standard for the privacy and security of health care patients and their sensitive, personal information.

HIPAA requires that health care institutions and any firm dealing with the personally identifiable information (PII) of patients must take special precautions when sending and receiving this data, or participating in electronic health care transactions.

The rules included help health care providers and other organizations ensure the confidentiality, privacy and security of sensitive information, even as advances in technology threaten it.

Defining Compliance: PCI DSS

PCI DSS affects every company and agency that accepts, stores or processes payment card information. Similar to HIPAA, the standards included work to ensure that customers' sensitive information - including their payment card and PIN - is safeguarded during all physical and digital transactions.

PCI standards include requirements for:

- ✓ Creating and maintaining a secure network environment.
- ✓ Protecting cardholder data with encryption and other safeguards.
- ✓ Maintaining vulnerability management through anti-virus and other protections.
- ✓ Implementing robust access controls, including restricting digital and physical access.
- ✓ Monitoring and testing the network and security systems.
- ✓ Creating and maintaining an information security policy.

Misconceptions Surrounding Compliance

Organizations inside and outside the health care, retail and banking industries should understand these standards and the responsibilities they hold according to these rules. However, there are a few misconceptions regarding overall compliance with HIPAA and PCI DSS:

There is a federal organization governing compliance:

While there are certain groups – including the U.S. Department of Health and Human Services, as well as the Payment Card Industry Security Standards Council – that are highly involved with HIPAA and PCI DSS, there is no single governing body that businesses must go through in order to achieve compliance.

Certain hardware and software solutions are compliant:

Although some providers tout their solutions as "compliant," no hardware or software is inherently compliant. These systems can, however, be installed, implemented and utilized in a way that helps support an organization's compliance with industry standards like HIPAA and PCI DSS.

Transmitting sensitive data: Specialized protection required

Overall, compliance is about aligning a company's practices with the rules and requirements included in industry security and privacy standards. This includes ensuring that there are certain specialized protections in place for transmitting sensitive data like payment card information or patient details.

Encryption is the primary method of achieving security and privacy - and is required for sensitive data in transit or at rest within servers under PCI DSS and HIPAA. However, encryption can be difficult for users to implement, and additional protections are needed to properly ensure that only authorized users have access to sensitive PII.

The Problem with Email and Unsecured Public Internet

Many users beholden to HIPAA or PCI DSS wonder why traditional email isn't a viable option for sending or receiving sensitive data. The issue here not only lies within the needed encryption, but also the connection over which emails are sent.

The majority of emails – unless there is an MPLS connection between sending and receiving email servers are transmitted over public internet, which is inherently vulnerable and does not provide the proper data protection for compliance. Sensitive information must be properly safeguarded during transmission and while at rest. In this way, a sender emailing an unencrypted document containing sensitive data over public internet, and the receiver who stores it in their email folder, are both noncompliant. This puts both at risk of a security breach, as well as other negative consequences like noncompliance penalties and fines.

What Today's Businesses Need for Compliance

In order to meet compliance with HIPAA and PCI DSS, businesses require a secure system that:

- Does not transmit sensitive, personal data over unsecured public internet connections, i.e. non-https connections.
- Features automated document encryption and strong access controls to provide data security
- Helps support other compliance requirements for user access controls, security and data privacy.

All of this and more is achievable through an advanced fax solution that can support an organization's compliant workflows concerning personal health information or payment card data.

Secure Fax Solutions to Support Compliance

FaxCore is the leader in secure fax solutions, and understands what it takes to implement a system that helps businesses achieve and maintain compliance.

FaxCore provides options for **traditional, on-premise fax and cloud-based fax,** which can be deployed and accessed in a secure and compliant manner.

As noted, while hardware and software elements themselves cannot be compliant, FaxCore helps ensure that even organizations leveraging cloud fax servers can maintain their PCI DSS and/or HIPAA compliance:

- ✓ Automated document encryption and strong access controls support data security.
- ✓ Users can access the advanced cloud fax server through a HTTPS-secured browser, enabling them to easily view, download and receive faxes in a safe and compliant manner.
- ✓ Businesses can also opt for Office 365 email server in the cloud, which when used alongside a TLS secure link connecting the company's instance of Office 365 and the FaxCore server, can enable protection and compliant email-to-fax transmissions.

Whether your organization is beholden to the standards of HIPAA or PCI DSS - or both - FaxCore has the technology and expertise to support security and compliance. Connect with us today to* request a demo and learn more *about how FaxCore helps you ensure compliance.

www.faxcore.com