ZIRMED®
INNOVATING CONNECTED HEALTHCARE

Payment Card Industry Data Security Standards and ZirMed

"Businesses paid an average of $5.5 Million per data breach in 2011; that's an average of $194 per record."

–2010 Annual Study: U.S. Cost of a Data Breach
Ponemon Institute

Today, almost all healthcare providers are intimately familiar with HIPAA security and privacy standards—and have a wealth of training, procedures, and audits in place to ensure compliance and avoid embarrassing and expensive lapses in compliance or security.

Unfortunately, too many healthcare providers handle patients' sensitive financial information without equivalent controls and security. Just as HIPAA governs the security and access of personal health information, agreed-upon standards and requirements exist to guard patients' financial information.

One such standard is the Payment Card Industry Data Security Standard (PCI DSS), supported and audited by the PCI Security Standards Council (PCI SSC), an industry work group made up of all the leading credit card processors, including Visa, MasterCard, Discover, and American Express. The Council is responsible for managing the security standards, while the payment card brands enforce compliance.

The standards apply to all organizations that store, process, or transmit cardholder data—including all healthcare organizations that accept credit cards.

Because ZirMed has passed the most rigorous PCI DSS validation process, providers using ZirMed to process credit cards minimize their risks while still offering this invaluable payment option to their patients.

Features and Benefits

- Minimize brand, financial, and legal risk from a data breach
- Avoid the financial cost and operational drain of maintaining compliance directly
- Offer the convenience and cash flow advantages of credit card payments—without the risks
- Fully imbedded with all ZirMed solutions

Data Security/Compliance	
Process Controls	SSAE-16 Audit
Financial Data Security	PCI Compliant since 2007
Compliance Certification	EHNAC, CORE

ZIRMED®
INNOVATING CONNECTED HEALTHCARE

ZirMed Compliance

Credit cards offer convenience for patients and can improve cash flow for providers.

Because ZirMed has passed the most rigorous PCI DSS validation process and are fully PCI DSS compliant, using our solution to process credit cards minimizes your risks while maintaining the value of this payment option. In addition, ZirMed has also passed the rigorous SSAE-16 security and process audit, and is certified by both EHNAC and CORE, standards bodies that regulate the handling and processing of health information.

PCI DSS Guidelines

PCI DSS compliance provides assurances to patients and providers alike that personal financial information is being properly handled. For providers accepting credit card payments online, offline, or in the office, PCI compliance minimizes the risks associated with data compromises—including damage to reputation, financial losses, and legal ramifications.

The major PCI DSS guidelines include:

• **A secure technical network** must be established and maintained through which transactions can be processed.

• **Cardholder information must be protected** wherever it is stored, and if stored, fully encrypted. Credit card numbers cannot be written down and stored on paper, and they cannot be readable in their stored digital format. Authentication data such as magnetic stripe (or track) data, card validation codes, and PIN data may not be stored.

> Securing information continues to challenge organizations at all levels, but the vast majority of these breaches are preventable. Organizations must not only protect the data itself wherever it is stored or used, but also create a culture of security including training, policies and actions. The results of this study show that companies with information protection best practices in place can greatly lower their potential data breach costs.
>
> – Francis deSouza
> Senior Vice President
> Enterprise Security Group, Symantec

• **Technical systems must be protected** against malicious hackers and software by deploying and maintaining updated antivirus software and keeping all software up to date.

• **Access to systems should be restricted and controlled**, with unique logins and passwords governing access.

• **A formal information security policy** must be defined, maintained, and followed at all times and by all participating entities. Enforcement measures such as audits and penalties for non-compliance may be necessary.

About ZirMed®

Founded in 1999, ZirMed is the nation's premier health information connectivity and management solutions company, modernizing critical connections between providers, patients, and payers to improve the business and process of healthcare. ZirMed combines innovative software development with the industry's most advanced transactional network and business analytics platform to give organizations a clearer view of their financial and operational performance. ZirMed's industry-leading technology and client support have been recognized with awards from KLAS®, Healthcare Informatics, Best of SaaS Showplace (BoSS), and Black Book Rankings. Our nationwide network facilitates, manages, and analyzes billions of healthcare transactions, driving bottom-line performance with clinical communications, comprehensive analytics, eligibility, claims management, coding compliance, reimbursement management, and patient payment services—including credit card processing, online payments, statements, estimation, and payment plan management. For more information about ZirMed, visit **www.ZirMed.com.**