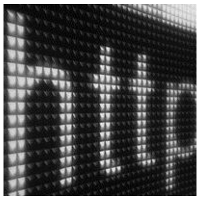
IS YOUR DATA SAFE?

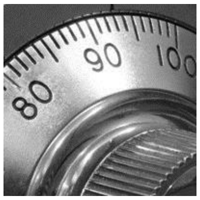
Questions and Answers About the Security of Your Data System

Your client information is more than just names and numbers— it's a precious commodity to both you and your clients. With concerns about computer hacking, identity theft and legislative compliance, your clients trust you to keep their sensitive information safe. And, to keep your company functioning efficiently, you need to ensure that your clients' information is intact and available, even when accidents or disasters occur.

However, keeping this information safe is more than just locking a file drawer or password-protecting your computer. How confident are you that your current system keeps your information safe?

With Zywave applications, you can rest assured that your data is protected from intrusion and readily available, and that your clients' sensitive information is secure.





Is your data transmitted and stored securely?

How does your current solution ensure data security?

What's your backup plan?

What if a fire or other disaster wiped out your computer system? Would you be able to restore all of your client information and get your company back on track?

How do you ensure privacy?

How does your current solution provider comply with legislative regulations and ensure that your clients' personal information stays private?

Is your solution provider HIPAA compliant?

Has your provider successfully implemented administrative, physical and technical safeguards to ensure full privacy of protected health information?

ZYWAVE

Is Your Data Transmitted and Stored Securely?

How does your current solution ensure data security? Zywave stores the information from its Web-based applications on its servers, so *Zywave* handles the security for that information.

Data Security During Transfer

All information sent to and from Zywave Internet applications is encrypted using Transport Layer Security (TLS) protocol, the successor to Secure Socket Layer protocol (SSL), in conjunction with industry-standard digital certificates.

These security features work together to provide users with a mutually authenticated communications path. Mutual authentication helps to ensure that only legitimate users can access the system, and that they see only the information they are intended to see.

This means that your information is protected during transit using current, proven security technologies.

Data Storage Security

All information stored on Zywave's servers is encrypted with a 256-bit Advanced Encryption Standard (AES).

Can You Keep Out the Bad Guys?

Zywave actively works to prevent hackers from gaining access to applications, systems and networks.

Secure Data Center

Zywave facilities offer ample redundancy to make applications available for you. Zywave's facilities feature:

Power – Uninterruptible Power Supply (UPS) units, backup generators and multiple utility feeds to provide 24/7 power.

Environmental Control – Climate-controlled spaces with backup HVAC systems regulate and monitor temperature and humidity.

Fire Detection and Suppression – A smoke, fire and particle detection system and pre-action sprinkler system help detect and suppress fires.

Security – Zywave's 24-hour security monitoring system consists of:

- Multiple levels of authentication, including card reader systems;
- Trained data center operations personnel; and
- Closed-circuit television cameras.

Secure Network

Zywave continuously monitors its network and systems to ensure that its applications are safe and available. Zywave's comprehensive security services include:

- Redundant firewalls;
- An industry standard intrusion detection platform;
- Centralized event logging;
- Continuous threat intelligence feeds;
- Regular vulnerability assessments; and
- Anti-virus and anti-malware protection.

Secure Email

If you send sensitive information by email, that information is at risk of falling into the wrong hands. To ensure secure transmission of sensitive information, Zywave uses a third-party tool to encrypt the content of emails sent through Zywave applications.

Each individual email address is associated with a secure email account, so you can be sure that only the intended recipients are seeing the message you sent.

What's Your Backup Plan?

What if a fire or other disaster wiped out your computer system? Would you be able to restore all of your client information and get your company back on track? Do you have a plan in case of such an accident or disaster? Our security model can help alleviate that concern.

The Zywave data center is hosted by trusted third-party partners like Microsoft and Amazon. Data centers provide multiple layers of physical security and at least 1+ redundancy for all environmental and electrical facilities. This means that any critical component can fail without affecting the entireoperation.

Zywave performs backups on a daily and weekly basis. Daily backups are differential, weekly backups are full backups. This ensures that your critical data is kept safe. It also means that we can restore data from backup files in the unlikely event of a data consistency issue during production.

Power Outage Protection

Multiple separate utility feeds power the data center, and multiple generators are set to provide backup power. In addition, to ensure consistent, clean levels of power to the computer equipment, multiple UPS systems provide protected power to the facility. The redundancy of the systems seamlessly and automatically continues to provide power if any of these power systems, or a module within a system, fails.

All power systems are continuously monitored for alarm conditions.

Preventive maintenance is performed regularly, as well as monthly generator tests. A full system test is performed yearly.

Disaster Recovery

In the event of a disaster, Zywave's applications and data are protected through industry standard disaster recovery solutions, including multiple local and off-site backups.

If a problem occurs, Zywave will work to ensure that you have access to its applications.

How do you ensure privacy?

How does your current solution provider comply with legal requirements and ensure that your clients' personal information stays private?

Zywave places a high value on the privacy of its clients and their expectation to keep client information confidential. In addition, Zywave recognizes that all employees, temporary workers and contractors have an ethical and legal obligation to keep certain information about clients confidential. They also have an obligation to protect and safeguard this information against tampering and unauthorized use or disclosure. For these reasons, Zywave earnestly works to make confidential information available only to people who have a legitimate right to access it. Contact your Zywave representative for a copy of our Corporate Privacy Policy.

Is Your Current Provider HIPAA Compliant?

Zywave® has successfully implemented administrative, physical and technical safeguards throughout its organization to ensure that its use and disclosure of protected health information (PHI) and electronic protected health information (ePHI) complies with the requirements set by the Health Insurance Portability and Accountability Act (HIPAA).

Because compliance is an ongoing process, Zywave continually devotes resources to reviewing and improving its business practices and policies to ensure the protection of all confidential information entrusted to it. As part of its compliance program, Zywave requires all employees to attend training on Zywave's Privacy Policies.

In the right-hand column of this page, we outline product features which address many of the most common security questions that partners have about compliance with various data security laws. We recommend that you consult with a licensed attorney in your state to determine how you can comply with your state's laws.

All storage at rest, regardless of the product, is encrypted with AES 256-bit encryption, and all data publically transmitted is encrypted using the TLS protocol.

BrokerageBuilder™

- If ePHI is uploaded by Zywave partners this would consist of documents.
- No ePHI is stored except for enrollment/employment information uploaded by a Zywave partner.
- Users have the option to encrypt emails.
- Partners are able to track sign-in attempts and application access through built-in reporting.
- If a URL is manipulated in an attempt to access data, the user is rejected and an "unauthorized access attempt" is logged.
- After six failed sign-in attempts, users are locked out

Decision Master® Warehouse

- No ePHI is stored in the application. ePHI is de-identified prior to any analytics occur in the application.
- After six failed sign-in attempts, users are locked out.
- Partners can cancel access to users.

HRconnection®

- Election/employment information is stored, but not ePHI.
- Date of birth and Social Security number fields are encrypted.
- If a URL is manipulated in an attempt to access data, the user is rejected and an "unauthorized access attempt" is logged.
- After six failed sign-in attempts, users are locked out.
- Zywave can provide a sign-in report to track user access (upon request).
- Partners can cancel access to users.

ModMaster®

- After six failed sign-in attempts, users are locked out.
- Users can set account-level security.
- Partners can cancel access to users.