

PENALTIES FOR HIPAA VIOLATIONS

Civil Penalties

- Violations can result in civil monetary penalties of \$100 per violation, up to \$25,000 per year

Criminal Penalties

- Fine of up to \$50,000 and imprisonment for one year for those who knowingly disclose individually identifiable health information
- Fine of up to \$100,000 and up to five years in prison for offenses committed under false pretenses
- Fine of up to \$250,000 and up to 10 years imprisonment for offenses committed with the intent to sell, transfer or use information for commercial advantage, personal gain or malicious harm

REAL WORLD PENALTIES

- On July 17, 2008 the Department of Health and Human Services levied a \$100,000 fine on Seattle-based Providence Health and Services for alleged violations of HIPAA Privacy and Security rules

OTHER REGULATIONS

Federal Rules of Civil Procedure (FRCP) - Requires organizations to be able to accurately produce emails during litigation.

Sarbanes-Oxley Act – Requires email records to be retained for 7 years. Penalties include fines of up to \$20 million and imprisonment for up to 20 years.

You are probably aware of the multitude of compliance regulations governing organizations—HIPAA, SOX, FRPC, etc. You may even have a solution or two in place to meet them. But how can you keep track of all of your employees' activities? What would it cost your company in fines or litigation if one of your employees accidentally or intentionally sent out private patient information to the wrong recipient? What if we said we could prevent this from happening? What if we said that we are the only company in the market with one comprehensive solution to meet all of your compliance, discovery and security needs? Meet Digital Info Security Company (DISC), the only company with your complete compliance solution.

Email Scanning for HIPAA Compliance

DISC's premier email compliance solution, PolicyBridge™, actively scans email messages for sensitive information, including personal identifiable information (PII) and protected health information (PHI) and can automatically enforce policies to block, quarantine, and log or encrypt the flagged message.

Email Encryption for HIPAA Compliance

DISC offers two methods of encryption for protecting private information. Using policy-based encryption, PolicyBridge can automatically encrypt messages that contain sensitive information as identified by the lexicon during custom content scanning. This method eliminates human error and prevents data leaks.

DISC also offers an email encryption plug-in, which encrypts a message from desktop-to-desktop using point-to-point encryption. This plug-in also allows for digital rights management.

In order to meet data retention requirements, PolicyBridge also has the ability to archive all email messages and attachments.

Flash Drive and Removable Device Security

SecureFlash® Enterprise- Enterprise encryption (AES 256 encryption) for USB Flash and Removable Drives

Portable and easy-to-use encryption and decryption with enterprise level administrative control for added protection

Highlighted features- Detailed audit trail, revocation of lost drives, automatic user identity/ password management, and easy to use drag-and-drop functionality

SecureFlash® Administrator Server- Command Center for Removable Drive Security

Comprehensive administrative control and policy enforcement for USB drives

Highlighted features- Dynamically revoke access to lost or stolen devices, administrative audit trail, and ability to configure and enforce policies for out of network and offline use

USB Device Control and Removable Drive Security

DeviceDefender™ Hosted edition- Affordable, transparent, and controllable detection management and encryption of USB port devices

Highlighted features- Blocks unauthorized devices, automatic encryption of approved devices, supports all manufacturer devices and media, FIPS 140-2 certified encryption, and the ability to revoke access to lost or stolen devices

Administrator server edition- Comprehensive administrative control and policy enforcement for removable drives and media

Highlighted features- Administrative audit trail, ability to dynamically revoke access to lost or stolen devices, ability to configure and enforce policies for out of network and offline device use

SecurServer

SecurWrap Security Server provides consolidated user management, identity management and key exchange between senders and recipients of sensitive content. The SecurWrap Security Server is a powerful tool that maintains a secure communication protocol with any sensitive data. It is controlled in a permission wrapper and provides a comprehensive audit trail on sensitive data in use throughout and outside of the enterprise.

This audit trail includes user actions on the data, how that data has been shared, where it is located, and which users have access to it.

Administrators may also revoke or expand user permissions directly from the Security Server console.

Encrypted Data Retention for Compliance

RestoreRex™ ensures that electronic patient records are protected against data loss and unauthorized access. Running automatically in the background, RestoreRex encrypts and backs up data on PCs and servers to an offsite location while meeting HIPAA's stringent access and portability requirements in order to maintain the privacy of patient data. A user-friendly web-interface gives you access to your file anywhere that you have an internet connection.

Prevents Unauthorized Access – Only a designated administrator holds the encryption key to data

Data Retention – Automatic backups preserve records offsite in an unalterable state. Healthcare records must be archived for 6 years according to the HIPAA privacy ruling.

Secure Transmission – Data is encrypted while in transit over the Internet to DISC's data center