

## 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.

## Are you prepared for a HIPAA audit?



The passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 outlined strict requirements as to how organizations in the healthcare industry—including healthcare providers, healthcare payers, and those providing healthcare billing services—handle electronic patient information. Implementing new, comprehensive security systems can seem daunting, but it doesn't have to be. A one stop shop for HIPAA compliance, Digital Info Security Company (DISC) simplifies the process by providing all of the IT solutions that your organization needs in order to be HIPAA compliant.

### Data Retention for HIPAA Compliance

RestoreRex™ ensures that electronic patient records are protected against data loss and unauthorized access. Running automatically in the background, RestoreRex backs up data on PCs and servers while meeting HIPAA's stringent access and portability requirements in order to maintain the privacy of patient data.

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.

### 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, 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.