MaximEyes Adheres to Secure Cloud Data Protection, Backup, and Disaster Recovery

In light of the recent news about ransomware attacks, First Insight wants to help you understand how we protect your patient data in the MaximEyes cloud solution.

Rest assured that First Insight monitors and adheres to secure data protection, backup, and disaster recovery measures. We will continue to stay current with privacy and security measures to protect your data.

How MaximEyes Protects Your Cloud Data

- Advanced antivirus, Microsoft® Azure security protection with anti-malware, and firewall technologies detect and stop ransomware threats from encrypting files
- Data at rest and data backups are encrypted
- Multi-factor and module-level authentication logins
- Scheduled Windows® and security updates
- Disaster recovery backup of the last 30 days within 2-8 hours

First Insight Resources (click a link below)

- 5 Questions to Ask About Cloud Security
- ROI Advantages of Using a Cloud-Based EHR
- 10 Benefits of Moving Your EHR System to the Cloud
- HIPAA Risk Assessment Checklist
- HIPAA Compliance Guide
- EHR Risk Assessment Checklist (Cloud)
- EHR Risk Assessment Checklist (Traditional Server)

Industry Resources (click a link below)

- Ransomware explained: How it works/how to remove it
- Malware explained: How to prevent, detect, and recover from it
- Learn about ransomware, how it works/attacks, and how to protect against them

maximeyes

Ready to migrate your EHR to the cloud?
Complete Online Form:

www.first-insight.com/request-demo