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

First Insight wants to help you understand how we protect your patient data in the MaximEyes.com 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.com Protects Your Cloud Data

- Advanced antivirus end point detection and Microsoft® Azure security protection with anti-malware, and Enterprise-grade 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.
- Automated responses to vulnerabilities and attacks.
- Country-level blocking, IP whitelisting, and restricted ports.
- Disaster recovery from a weekly backup of the last 60 days and point in time data backup of the last 14 days within 2 to 8 hours.

maximeyes

First Insight Resources (click a link below)

- 5 Questions to Ask About Cloud Security
- HIPAA Risk Assessment Checklist
- HIPAA Compliance Guide

Industry Resources (click a link below)

- How to Secure Your Practice Against the Current Heightened Risk of Cyber Attacks
- Shields up: U.S. health care system warned of Russian cyberthreat
- Ransomware explained: How it works/how to remove it
- Malware explained: How to prevent, detect, and recover from it
- What is Ransomware?
- HealthIT.gov Security Risk Assessment Tool
- National Security Agency Mobile Device Tips

Ready to migrate your EHR and practice management system to MaximEyes.com?

Complete Online Form:
www.first-insight.com/request-info

2/9/23