MaximEyes®

www.maximeyes.com
800-920-1940, Option 5
sales@first-insight.com

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

At MaximEyes®, we're committed to keeping your patient data safe in our cloud-based EHR and practice management software. We follow strict security, backup, and disaster recovery protocols to ensure your information stays protected. You can count on us to stay up to date with the latest privacy and security standards.

MaximEyes® Resource Links

6 Cybersecurity Tips to Protect Your Eye Care Practice

HIPAA Risk Assessment Checklist

HIPAA Compliance Guide

Industry Resource Links

How to Secure Your Practice Against the Current Heightened Risk of Cyber Attacks

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®?

COMPLETE THIS ONLINE FORM

How MaximEyes® 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.