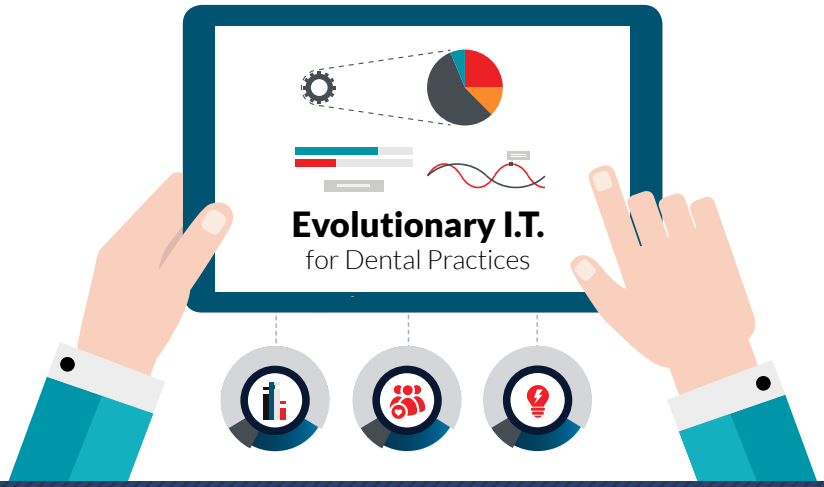
LEAP MANAGED IT



- HIPAA Technical Audit & Remediation Services
- Computer & Network Security Services
- On-site and Help Desk Support
- Cyber Security and HIPAA Standards Training

Gary Thomas
Leap ManagedIT

Gary is a small business leadership guru and sought after cyber security speaker. He successfully led the transformation of a near century old organization into a leading-edge technology company where he currently serves as president. Along with serving on several non-profit boards he is also a world class competitor completing 8 Ironman triathlons.

Michael Thomas
Leap ManagedIT

Michael is a Fortune 200 veteran where he led a nationwide group that was dedicated to teaching organizations how to leverage technology, insights and data to drive innovation. He is also the co-founder of an early stage drug development that is focused on developing 'smart' therapies. He devotes his free time to serving on a local youth sports board along with coaching basketball, lacrosse, and soccer.

3 MINUTES TO A STRONGER DENTAL PRACTICE

CEO Guide to Understanding IT

In this guide:

Security and HIPAA Compliance

LEAP MANAGED IT

Gary Thomas and Michael Thomas

leapmanagedit.com

Security & HIPAA Checklist

Information security and HIPAA compliance are like any aspect of your business backend: as the CEO, you don't need to know the details, but you do have the responsibility for oversight. After all, your computer systems and patient information are critical parts of your organization, and if anything goes wrong, it impacts your entire business.

In this 3-Minute Guide to a Stronger Dental Practice, you'll be able to quickly gauge where your practice stands.

Ask your IT manager to review this checklist with you.

QUESTION	RESULT
1. Have you performed a network risk analysis in the last 24 months?	
a) If so, were all the remediation items corrected and documented?	
2. Do you have clear policies in place to help your staff stay compliant with HIPAA standards?	
a) Are they reviewed on a semi-monthly basis?	
3. Have you selected and trained a staff member to serve as the HIPAA Compliance Officer?	
4. Do you have procedures to oversee employees working with ePHI?	
5. Do you have controls and procedures to ensure that employee's accessing ePHI is authorized?	
a) Can the employee's access be audited?	
6. Do employees share passwords?	
7. Are the following security best practices in place, are they regularly updated, and are the updates documented?	
a) Operating System Security Patching	
b) Anti-Virus	
c) Anti-Malware	
d) DNS Level Protection	
e) Firewall Protection	
8. Do you have a disaster recovery plan in place if your facility is inoperable?	
a) How long will it take to access ePHI data and critical systems?	
b) How often is the disaster recovery plan tested?	
9. Do you have a Business Associates agreement with outside organizations that might encounter ePHI?	
10. Do you have regular evaluations of the technical and non-technical elements of your ePHI security?	

leapmanagedit.com