HIPAA Compliance Made Simple

A Guide for Growing Healthcare Practices

Lumen21

Why HIPAA Still Matters

HIPAA compliance isn't just a checkbox—it's about protecting patient trust, minimizing legal risk, and maintaining uninterrupted care. For growing healthcare SMBs, the challenge is doing it right without creating administrative chaos.

This guide simplifies the process, giving you the clarity and tools to assess your current standing, identify gaps, and take practical action.

HIPAA Self-Assessment Checklist

Use this checklist to evaluate how your current systems align with HIPAA requirements.

REQUIREMENT	STATUS	NOTES
Data is encrypted at rest and in transit	☐ Yes ☐ No	
Role-based access controls are in place	☐ Yes ☐ No	
Audit logs are enabled and regularly reviewed	☐ Yes ☐ No	
Security risk analysis is conducted annually	☐ Yes ☐ No	
Staff receive cybersecurity training	☐ Yes ☐ No	
Breach notification procedures are documented	☐ Yes ☐ No	
Automatic patching is implemented	☐ Yes ☐ No	

Want to keep a copy?
Download and fill it in digitally or print it for internal use.

Top 5
HIPAA Compliance Mistakes We See in SMBs

1

Too much trust, too little control

Giving admin access to all staff increases risk.

Solution: Use RBAC (Role-Based Access Control).

2

No proof of training

Informal training ≠ compliance.

Solution: Document and timestamp all staff trainings.

3

Insecure communication tools

Email or messaging apps aren't always HIPAA-compliant.

Solution: Use encrypted, certified platforms.

4

Lack of incident response plan

No clear steps = more downtime.

Solution: Create and test a response plan at least once a year.

5

"We didn't know" defense

Lack of awareness won't protect you from fines.

Solution: Conduct a risk assessment annually.

Lumen21

Lumen21, Inc. | sales@lumen21.com | www.lumen21.com

Lumen21 | Pro Tips

1- ***Automate compliance*** *wherever possible to reduce human error.*

2- *Use* ***dashboards*** *to track audit trails and employee access in real-time.*

3- *Choose vendors who* ***understand regulated industries****, not just general IT.*

4- *When in doubt,* ***document everything.***

Need help simplifying compliance?

Partnering with a Managed Security Provider like Lumen21 ensures your systems are aligned, monitored, and audit-ready—without overloading your team.

Schedule your free consultation

Lumen21

Lumen21, Inc. | sales@lumen21.com | www.lumen21.com

Lumen21 specializes in IT security and compliance. It offers a range of solutions and services for organizations that enable them to leverage the latest technologies and meet their regulatory and security responsibilities. Lumen21 facilitates the compliance process and enables companies to measure, monitor, report, and improve it. Lumen21 offers its O365+ Compliance Service, which leverages Microsoft products such as O365 Enterprise, Enterprise Mobility, Device Management, and Azure Storage, implementing the necessary controls, configuring and monitoring them to meet regulatory standards. Therefore, at Lumen21, we believe that regulatory compliance is not a simple declaration, but a continuous, verified, and certified process. You can learn more about our solutions that help you comply with regulations in your IT operations and improve your security. To do so, please contact us at sales@lumen21.com or visit us at www.lumen21.com