IT FOR HEALTHCARE: REDUCE RISKS—AND OPERATING COSTS

THE MSP SOLUTION: SECURITY, COMPLIANCE, AND COST CONTROL IN ONE INTEGRATED PACKAGE

OLS: TECHNOLOGY

HOW FLEXIBILITY QUIETLY SHIFTED FROM ADVANTAGE TO RISK

Serving communities from coastal towns to suburban hubs, a network of medical clinics spanning Western Washington prided itself on accessibility and compassion. Their telehealth usage began to skyrocket. Flexibility became their competitive advantage—until it simultaneously began introducing undetected but consequential risk.

Billing and coordination teams were increasingly working from kitchen tables rather than clinic offices. Meanwhile, physicians reviewed charts on mobile devices between site visits, and care coordinators logged into patient portals from public Wi-Fi while traveling up and down I-5.

Every one of these conveniences improved patient access—but also multiplied security vulnerabilities

THE PRICE TAG ON SECURITY VULNERABILITIES FOR REGULATED INDUSTRIES

Healthcare compliance regulations such as HIPAA and HITECH are unforgiving. As outlined by *HIPAA Journal*, even **a single lost, unencrypted device** can be classified as a reportable breach, forcing **public disclosure** and fines ranging from **$50,000 to $1.5 million per violation.**

The leadership team realized they didn't *just* need IT support. They needed a technology partner with deep experience supporting regulated industries, like healthcare services providers.

PROACTIVE MSP SUPPORT: REDUCE ORGANIZATIONAL RISK. PROTECT PATIENTS. LOWER IT COSTS.

Risk Area	With Break/Fix IT Support	The MSP Solution
Device Security	Personal devices without encryption	Device management, remote wipe & enforced encryption
Authentication	Shared passwords & single-factor logins	Role-based access & MFA across all systems
File Sharing	Ad-hoc via email & unvetted cloud & AI tools	HIPAA-compliant cloud collaboration with audit logs
Access Management	Delayed offboarding of contractors & staff	Instant provisioning & revocation via MSP access control
Staff Awareness	No formal security education for the team	Quarterly security & phishing simulations

360.993.0600 olstechnology.com Vancouver | Portland | Seattle

A QUICK COMPLIANCE ASSESSMENT FOR THE HEALTHCARE INDUSTRY

If your healthcare organization allows remote work, telehealth access, or even flexible administrative logins, take this three-question assessment.
If the answer to any of these questions is no, you need HIPAA-compliant IT support for healthcare providers.

ARE ALL ACCESS POINTS—INCLUDING PERSONAL DEVICES—ENCRYPTED & MONITORED?

LOST OR STOLEN DEVICES ARE AMONG THE TOP CAUSES OF PHI BREACHES (HHS)

In healthcare environments, every point of access creates potential exposure—especially when staff use personal phones, home computers, or tablets for remote work, patient communication, scheduling, or telehealth. Without full-disk encryption, device-level monitoring, and enforced login security, protected health information (PHI) can be compromised in seconds.

CAN YOU PROVE HIPAA COMPLIANCE IF AUDITED TOMORROW?

OVER 80% OF AUDITED HEALTHCARE ORGS FAIL TO MEET BASIC HIPAA SECURITY RULE REQUIREMENTS (OCR)

Documentation is just as important as security itself. HIPAA requires organizations to maintain evidence of risk assessments, access controls, staff training, policies, and technical safeguards. If an audit occurred tomorrow, could you quickly produce those records? Many SMB healthcare providers struggle with this because compliance is complex and time-consuming without a structured IT framework.

IF A DEVICE WAS LOST TODAY, COULD YOU REMOTELY LOCK OR WIPE IT?

STOLEN OR LOST DEVICES ACCOUNT FOR A SIGNIFICANT PORTION OF REPORTED HIPAA VIOLATIONS (HHS)

When a laptop, tablet, or phone goes missing, minutes matter. Without a remote wipe or lock capability, a lost device becomes a serious data-exposure event—especially if it contains stored emails, patient messages, or system logins. HIPAA requires organizations to safeguard PHI against unauthorized access, and a lost device without remote-wipe protection is considered a major compliance failure.

OPERATIONAL & FINANCIAL ROI: THE VALUE OF AN MSP

- **Eliminated PHI & PII data exposure**
- **Insurance premiums dropped by 8%**
- **Compliance reporting dropped by 40%**
- **Remote work became more productive & secure**
- **IT costs became predictable & annual spend dropped**

MANAGED IT ISN'T JUST TECH SUPPORT - IT'S THE ENGINE DRIVING GROWTH.

Investing in the right IT approach doesn't just solve technical problems—it accelerates your business. From cost control and uptime to cybersecurity and scalable growth, SMBs that leverage modern IT services are positioned to compete more effectively in a digital-first economy. Whether you're navigating growth, protecting your assets, or optimizing daily operations, a strategic IT partner can help you future-proof your business.

READY FOR IT THAT'S SECURE, SCALABLE, AND DRIVES GROWTH?
REACH OUT TO ON LINE SUPPORT FOR A STRATEGIC ASSESSMENT TODAY.

360.993.0600 olstechnology.com Vancouver | Portland | Seattle

OLS: TECHNOLOGY

PREDICTABLE. EFFICIENT. SAFE. IT that's more than tech—it's fuel for growth.

OLS Technology helps Pacific Northwest SMBs grow with managed IT and cybersecurity built for the real world. We focus on what matters most to your teams and your bottom line: predictable pricing, reliable tech and uptime, smarter workflows, and secure data and communication.