The Landscape of Cybersecurity in Private Orthopedics

Michael McWilliams SVP, Healthcare

Agenda

1. Challenges in Orthopedics
2. The Landscape of Cybersecurity in Private Orthopedics
3. Case Studies
4. Annual Security Risk Assessment (SRA)
5. The 5-Lines of Defense

MERIPLEX

Challenges in Private Orthopedics

Common Concerns in Orthopedics

Addressing these IT concerns is crucial for Orthopedic groups to maintain patient safety, operational efficiency, and regulatory compliance.

Data Security and Privacy

Securing sensitive patient information, including medical records, insurance information and financial data from cyber threats.

HIPAA Compliance

Adhering to HIPAA regulations is crucial to ensure patient privacy and avoid hefty fines.

IT Staffing and Support

Challenges in hiring and retaining IT talent is increasingly becoming harder.

Budget Constraints

Tight operational budgets make it challenging to prepare for IT expenditures that arise and IT spend it hard to predict.

Aging Technology Infrastructure

Maintaining up-to-date and supported infrastructure can lead to security vulnerabilities, performance issues and disruptions to patient care.

Outgrown Existing Support Model

Outgrowing your IT support model is a common challenge in orthopedics. The need for deep expertise in IT and cybersecurity is increasingly becoming more demanding.

Remote Workforce

Increase in desire for appropriate personnel to work from home full-time or part-time.

Interoperability and EHR Integration

Seamlessly sharing patient information between systems is essential for efficient patient care.

MERIPLEX

The Landscape of Cybersecurity in Private Orthopedics

Why are Private Groups a Prime Target?

Ransomware Groups find private practices more appealing than larger institutions for multiple reasons:

- **Lower Budget and Security Resources**
  - Malicious hackers are looking for unsophisticated IT groups with outdated systems and minimal security measures
- **Easier to Breach**
  - Historically easier to penetrate with common attack vectors like phishing or known software vulnerabilities
- **Less Resilient to Disruptions**
  - Private practices have fewer resources to quickly recover from a ransomware attack

Current Healthcare Statistics

Increased Frequency of Attacks

92%

Healthcare organizations experienced some sort of breach in the past 12 months

3x

Increase of ransomware attacks against healthcare entities from 2016 to 2024

Data Breach Severity

133 million

Healthcare records breached in 2023, a record

364,000

Average number of records breached per day in 2023

Cybersecurity Spending

$125B

Expected spend by healthcare on cybersecurity products and services

<10%

IT budget allocated to cybersecurity by 56% of healthcare organizations

Talent Shortages

53%

Healthcare organizations that lack in-house cybersecurity expertise

46%

Healthcare organizations that have insufficient IT staffing overall

Employee Error

31%

Healthcare organizations where carless users caused data loss and exfiltration

Department of Health and Human Services

Breach Portal: Notice to the Secretary of HH Breach of Unprotected Protected Healthcare Information

Cases Currently Under Investigation	Type & Location of Breached Info	Breach Submission Date
Vail Summit Orthopaedics	Hacking | IT Incident	7/31/2025
OrthoAtlanta	Hacking | IT Incident	7/21/2025
Integrated Orthopedics of Arizona	Hacking | IT Incident	8/11/2025
Gardner Orthopedics	Hacking | IT Incident	6/24/2025
Orthopaedic Specialists of Connecticut	Hacking | IT Incident	4/23/2025
Precision Orthopedics and Sports Medicine	Hacking | IT Incident	2/13/2025

U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

MERIPLEX

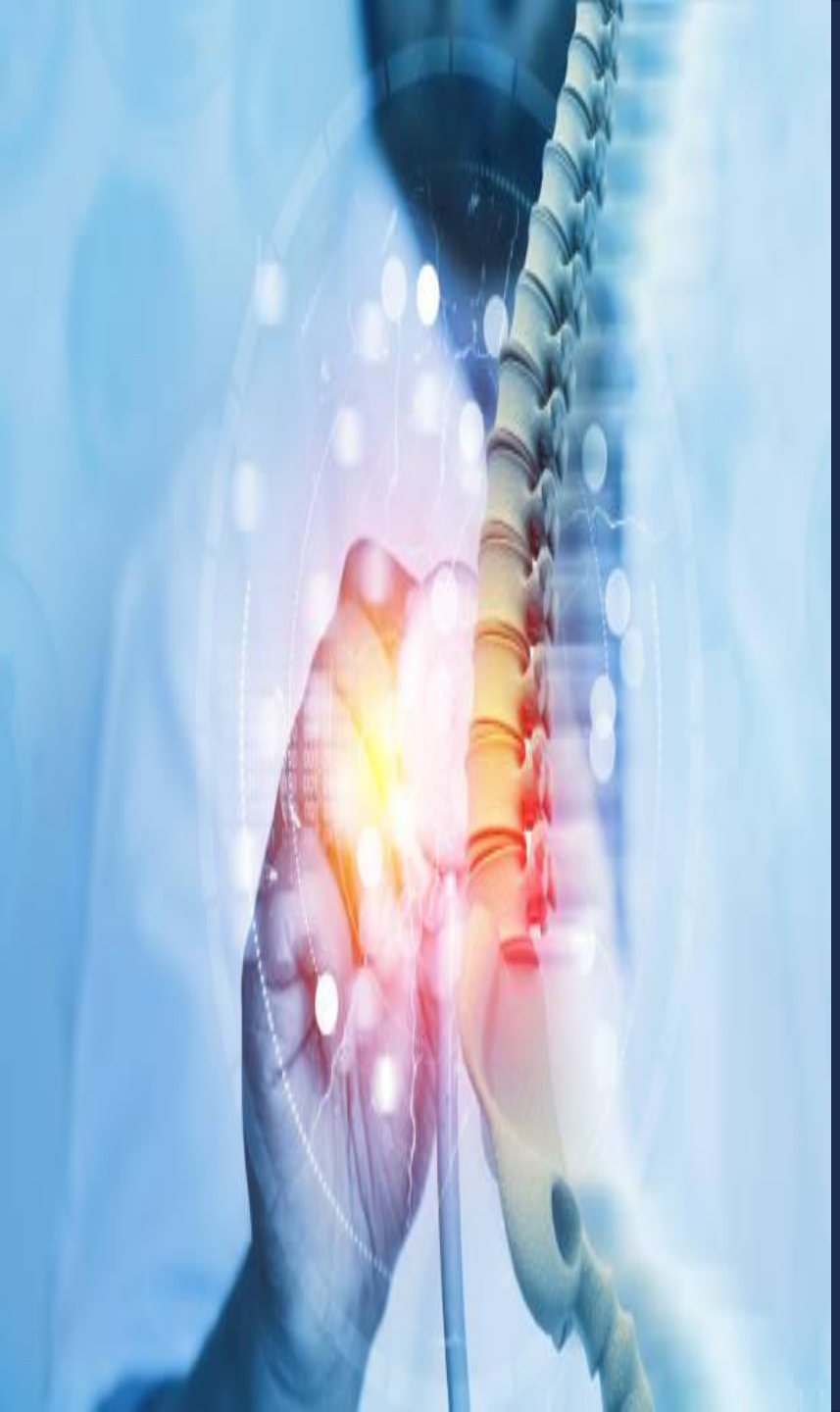
Case Studies

Anonymous Orthopedic Group

Practice Overview	In Actuality…	The Realization….
19 Providers	369 workstations ranging from 5-10 years old	No Standardization
175 Employees	44 Servers ranging from 6-12 years old ½ Windows | ½ Linux	No Backups
IT Director Recently Resigned	Firewalls all Linux based	No virus protection
	Switches were 7-15 years old using Netgear, Ubiquiti, HP and Cisco	Benchmarking against other groups, they were low end of IT spend
Management Stated:	No automated patching, all was done manually leaving countless workstations and servers unpatched	Linux dependent – minimal support, problems must be fixed yourself
"Trusted and liked current IT personnel"		Open-source platforms should not be running the practice
"Everything secure and in working order"		IT constantly "fighting fires" due to age of equipment and software chosen to run the practice
(3) IT people seemed busy "fighting fires," but they felt secure		
PMR – Athena		
200 Workstations		
10 Servers		

Florida Orthopedic Institute

- Hit with Ransomware in April 2020
- Every system was encrypted
- Hit with $99,000,000 Class Action Lawsuit in June of 2020
- Settled for $4,000,000 and $1,600,000 in legal fees in April 2022



Large Private Ortho Group – California

- Hit with Ransomware (5) times before engaging an IT/Security Partner
- Did not pay ransom and tried to rebuild with incomplete and inconsistent backups
- No EMR/PMR for (2) Months

Premier Bone & Joint

- Performed SRA in 2022
  - Did not have a ransomware-proof backup solution
- January 2023 – Hit with Ransomware
- Everything was encrypted
- Paid $94,575 ransom to a group out of Crimea
- Down for (3) weeks with no EMR

MERIPLEX

Annual Security Risk Assessment (SRA)

Annual Security Risk Assessment (SRA)

- Annual SRAs are critically important for several reasons:

  - HIPAA Compliance – they are required!
  - Data Protection
  - Proactive Risk Mitigation
  - Stronger Access Controls
  - Improved Data Encryption
  - Enhanced Employee Training
  - Disaster Recovery (DR) Planning
  - Improved Patient Trust
  - Reduced Financial Losses

How do you know you are getting the right Security Risk Assessment (SRA)?

- Customized for HIPAA
- Different set of questions and tests
- More than just a scan
- In-depth, 100s of labor hours

What Changes with HIPAA?

- HHS Responding to Increasing Cybersecurity Incidents within Healthcare Industry
- Strengthen ePHI Protections
- Items are No Longer Addressable - Now REQUIRED
- Providers and Business Associates Required to Adopt More Robust Cybersecurity Measures

What Changed with HIPAA Security?

- Eliminations of “Addressable” Specifications
- Mandatory Written Documentation
- Updated Definitions and Specifications
- Specific Compliance Timeframes

What to Expect with an SRA?

- Expert team approach
- Multiple tools and resources
- Executive and technical elements
- Granular detail with supporting documentation
- Sufficient for full remediation by a capable team

MERIPLEX

Security Risk Assessment

To Streamline and Protect Your Practice

Managing the complexity of your information technology is daunting. You want to focus on building a successful practice and serving the needs of your patients, not the technology that supports these endeavors. Let Meriplex provide peace of mind with a comprehensive security risk assessment.

Included in the assessment is the following:

- Risk Assessment and Treatment
- Security Policy Review
- IT Operations Analysis
- HIPAA Security Assessment
- Clinical Assessment
- Technology Plan
- Live Hacking / Penetration Testing

Get your Scorecard and Recommendations for Remediation

Once we've completed the assessment, we distill the information into an easy-to-understand scorecard that is color coded to highlight areas of concern. This provides a starting point for your planning. A representative example is shown below:

HIPAA	SIG	Issue	Finding	Severity	Impact	Security	LOE	2021	2022
7, 15, 40	H.4.2, G.15	S 1.1	Domain Password Policy	H	M	H	M	H	H
2, 10, 11, 34	H.1.2	S 1.2	Administrative Accounts	H	L	H	M	H	H
2, 10, 11, 34	H.1.2	S 1.3	Enterprise Administrator Group	L	L	M	L	N	N
2, 10, 11, 34	H.1.2	S 1.4	Schema Administrator Group	L	L	M	L	N	N
2, 10, 11, 34	H.1.2	S 1.5	Administrative Least Privileges	H	L	H	M	N	N
2, 10, 11, 34	H.1.2	S 1.6	Local Administrators Group	H	L	H	M	L	L
13	H.1.2	S 1.7	Domain Trust	L	L	L	M	N	N
2, 10, 11, 34	H.4.2, G.14	S 1.8	No Password Required Flag	M	L	M	M	N	N
7, 15, 40	G.15.19	S 1.9	Domain Admin Accounts	H	L	H	M	H	H
8, 15, 16, 22, 40	G.15.19	S 1.10	Default Administrator Account	M	L	H	L	N	N
2	G.15.1	S 1.11	Domain Name Services	L	L	L	M	N	N
2	H.1.2	S 1.12	Printer Access Permissions	M	L	M	M	N	N
2	G.15.1	S 1.13	Active Directory Inconsistencies	L	L	L	M	N	N
2	G.15.1	S 1.14	Bad Computer Accounts	M	M	M	M	N	N
7, 8, 15, 16, 40	G.15.2, I.3.4	S 1.15	Windows XP Computers	H	M	H	M	N	N
13	G.15.19	S 1.16	Employee Badges ID	H	M	H	H	N	N
2, 40	G.15.19	S 1.17	Single Sign-On (SSO)	M	M	M	H	N	N
4, 38	G.15.2, I.3.4	S 1.18	Windows Server 2003	M	M	M	H	N	N
13	K.3	S 1.19	Mail Delivery Redundancy	H	M	M	M	N	N
7, 15, 40	K.3	S 1.20	Mailbox Database Redundancy	H	M	M	M	N	N
13	G.20.3, I.6.2	S 1.21	USB Devices Enabled	H	M	H	M	M	M
19, 21	H.1.2	S 1.22	File Share Permissions	M	L	M	M	N	N
19, 21	G.20.14	S 1.23	Laptop and Desktop Encryption	M	M	M	L	H	H
10, 29, 31, 32	K.1	S 1.24	Business Continuity Plan	H	M	H	H	H	H
2, 10, 11, 34	K.1	S 1.25	Mail Archiving	M	M	L	M	N	N
42	G.7	S 2.1	Antivirus Deployment	M	L	M	M	L	L
17, 18, 19, 20, 21	G.15.2	S 3.1	Patch Management	M	M	M	M	M	M
17, 18, 19, 20, 21	G.15.4	S 4.1	Windows System Auditing	M	M	M	M	N	N
13	G.15.2	S 5.1	VMware Tools	L	M	M	L	N	N

High

Medium

Low

No Finding

N

MERIPLEX

The 5-Lines of Defense

Recommendations

How to improve your risk score..

- Remediate the issues listed in your Security Risk Assessment (SRA)
- Implement the 5-layers of defense

5-Lines of Defense

What are the 5-Lines of Defense?

1st Line of Defense	2nd Line of Defense (BAMP)	3rd Line of Defense	4th Line of Defense (Test and Assess)	5th Line of Defense
• Spam Filtering • Antivirus • Security Awareness Training • Dark Web Scan • Phishing • Identity Management (2FA) • Onsite Backup	• Backup (Ransomware Proof) • Antivirus (Artificial Intelligent Intelligent AV Driven Tool) • Monitoring • Patch Management • Cloud Detection and Response (CDR) • URL Filtering	• Security Information Event Management (SIEM) • Managed Firewall with IDS/IPS and Web Filtering • 24x7 Managed Security Operation Center	• Annual Security Risk Assessment with Penetration Testing	• Business Continuity & Disaster Recovery (Onsite or Cloud)

Questions?

Michael McWilliams
SVP, Healthcare
mmcwilliams@meriplex.com
303.908.5444