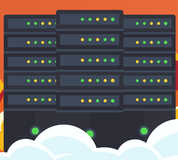
MEDITOLOGY SERVICES

FIRE IN THE CLOUDS

NEW FEDERAL GUIDANCE FOR HEALTHCARE CLOUD SECURITY

Healthcare's critical applications have ascended from ground-level on-premises data centers into distributed cloud environments.

Attackers have shifted the cyber battle theater from ground-level fighting to aerial warfare, targeting cloud-hosted platforms. The resulting cloud-based cyber fires are spreading rapidly across the healthcare landscape.



The U.S. Health Sector Cybersecurity Coordination Center (HSCC) has released new guidance on cloud security for healthcare organizations.[1] Here are the summary takeaways:

What Is the Goal of Cloud Security?

- Recover data in the event of data loss
- Ensure the privacy of data across networks
- Protect networks against malicious activity
- Minimize human error that could cause data loss
- Reduce the overall impact of compromises

Cloud Misconfigurations

According to the NSA, some of the most common cloud misconfigurations include:

- Unrestricted inbound and outbound ports
- Disabled monitor and logging capabilities
- Unsecure API keys
- Internet Control Message Protocol was left open

[1] https://www.hhs.gov/sites/default/files/cloud-security-analyst-note-tlpwhite.pdf

TOP CLOUD RISKS

Cloud Credentials & Phishing
Cloud services use email for verification and access; attackers are sending more phishing attempts to steal cloud credentials

Shadow IT
Business units are buying and deploying cloud-hosted solutions without IT or security's knowledge

Cloud Hijacking
Cyber criminals are taking over compromised cloud accounts

Identity & Access Management
Minimum necessary access with routine monitoring is essential to protecting cloud ecosystems

Lack of Cloud Visibility
Tenants cannot see cloud traffic hosted off-site, making alerting and incident response more problematic

Cloud Compliance
Security and privacy standards and controls are not consistently applied to cloud applications

PROTECTING THE CLOUD

- Use a cloud service provider that encrypts data
- Conduct compliance audits
- Implement a zero-trust model
- Set up your privacy settings
- Use two-factor authentication
- Establish and enforce security policies
- Maintain cloud visibility
- Understand cloud compliance, requirements, and regulations
- Install updates to your operating system
- Avoid using public Wi-Fi

MEDITOLOGY'S CLOUD SECURITY FIRE FIGHTERS

Meditology has a proven track record of helping healthcare entities evaluate, design, configure, and certify cloud-hosted applications and third-party business associates.

Our cloud security services incorporate our real-world experience, leading regulatory requirements, and industry standards, including HIPAA, HITRUST CSF, NIST CSF, the Cloud Security Alliance (CSA), and more.

Meditology's Cloud Security Services for Healthcare

- Cloud security risk assessments
- Office365 security
- Penetration testing for cloud environments
- Cloud implementation validation & consulting
- Cloud security strategic planning
- Cloud vendor risk management
- HITRUST and SOC 2 certifications for cloud-hosted systems
- Cloud security remediation management
- Cloud subject matter expert staff augmentation
- Cloud API inventory, security assessment, and technical testing

Meditology Services is a top-ranked cybersecurity, privacy, and risk consulting firm dedicated to the healthcare industry.

Contact us if you have any questions or if there is any way we can support you and your cloud security needs.

MEDITOLOGY SERVICES
info@meditologyservices.com
MEDITOLOGYSERVICES.COM