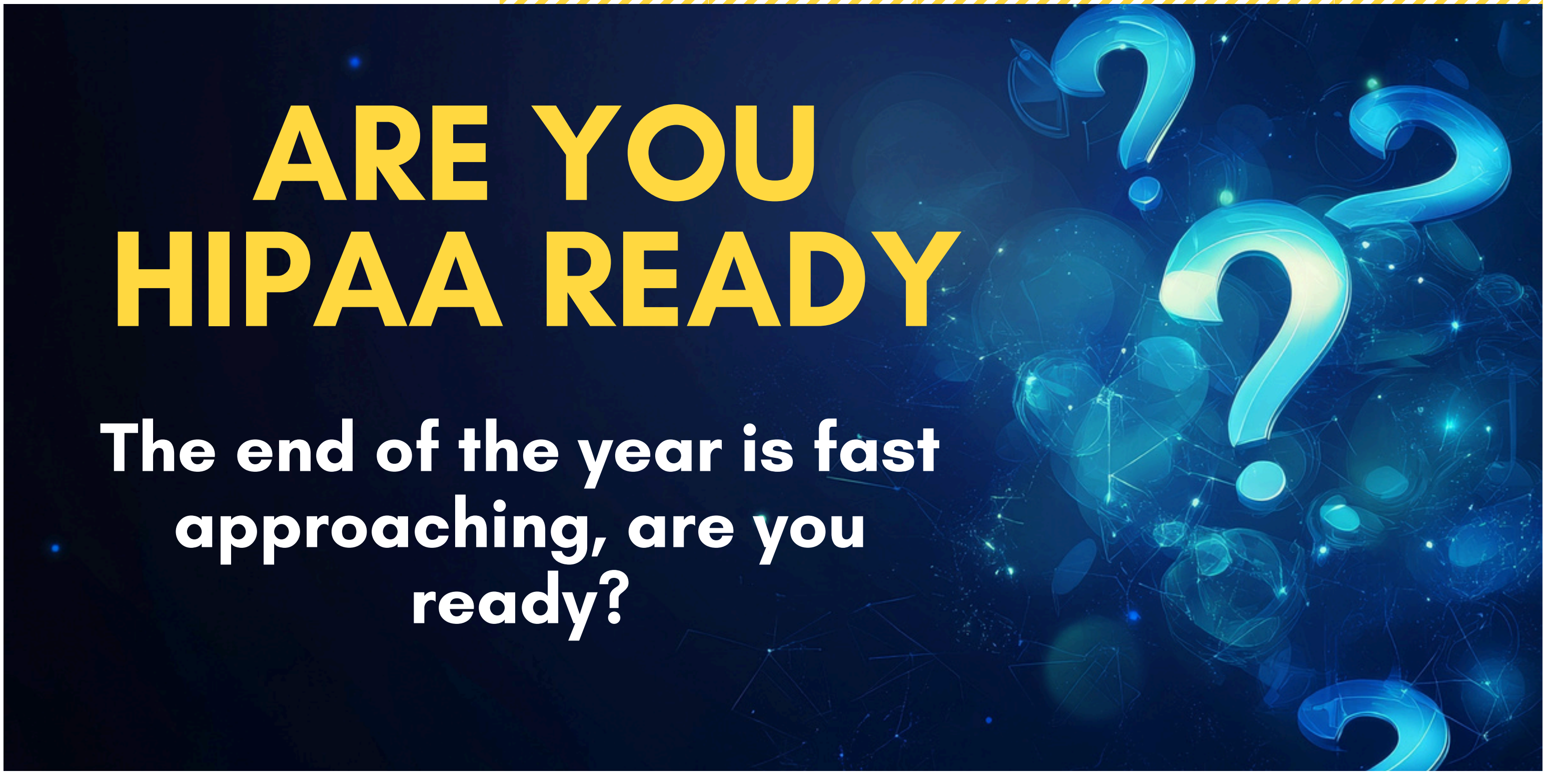
www.umercs.com October 2025

uMercs Cybersecurity News Digest

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



ARE YOU HIPAA READY

The end of the year is fast approaching, are you ready?

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law that mandates the protection of sensitive patient health information, known as protected health information (PHI). Its Security Rule (45 CFR § 164.308) requires covered entities (e.g., healthcare providers, insurers) and their business associates to implement robust administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI). While HIPAA does not explicitly require penetration testing, it is a critical best practice for compliance, particularly under the rule's mandates for ongoing risk analysis, assessment, and management (§ 164.308(a)(1) and § 164.308(a)(8)).

Key Reasons Penetration Testing is Essential:

1. **Identifying Vulnerabilities Proactively:**

Penetration testing simulates real-world cyberattacks to uncover weaknesses in IT systems, networks, applications, and human processes that could expose ePHI. HIPAA demands regular security evaluations to detect risks before they lead to breaches, which have resulted in over $10 billion in fines since 2003 (per HHS data).

2. **Risk Management and Mitigation**:

The Security Rule requires entities to conduct periodic risk assessments and implement measures to reduce identified threats. Pen testing provides actionable insights (e.g., via reports on exploitable flaws like unpatched software or weak access controls), enabling organizations to prioritize fixes and demonstrate due diligence during audits or investigations by the Office for Civil Rights (OCR).

3. **Preventing Costly Breaches and Penalties:**

Healthcare data breaches are rampant—over 700 major incidents affected 100+ million records in 2023 alone (HHS Breach Portal). Non-compliance with HIPAA can lead to fines up to $1.5 million per violation annually, plus reputational damage and lawsuits. Regular pen testing helps maintain the "reasonable and appropriate" safeguards required by HIPAA, reducing breach risks by up to 70% according to industry studies (e.g., from Verizon's DBIR).

4. Supporting Broader Compliance Frameworks:

Pen testing aligns with HIPAA's emphasis on technical safeguards (e.g., access controls, encryption, audit logs) and integrates with standards like NIST SP 800-53, which the Security Rule references. It's often required in HIPAA risk management plans and can fulfill obligations under related regulations like HITECH.

uMercs Cybersecurity News Digest

Breach in September 2025 related to HIPAA compliance

Veradigm (formerly Allscripts), a Chicago-based healthcare software provider, disclosed on September 22, 2025, a data breach from unauthorized access to a storage account around December 2024, detected July 1, 2025, via a customer's separate incident. Attackers used stolen customer credentials to access sensitive data, isolated to this account with no misuse detected. Exposed information included names, contacts, DOB, medical records (diagnoses, meds, tests, treatments), insurance, payments, and limited SSNs/DL numbers, varying by individual. At least 70,000 affected in Texas and South Carolina; broader impact unclear. Veradigm blocked access, notified authorities, engaged experts, added safeguards, and offered free credit monitoring/identity protection. Not yet on HHS OCR portal.

How a Penetration Test Could Have Stopped This Attack

A penetration test (pentest) simulates attacks to uncover vulnerabilities, potentially preventing this credential-theft-enabled breach by identifying and fixing access control gaps in Veradigm's and customers' system.

Credential Vulnerabilities:
Pentest could simulate theft/phishing to test MFA absence, privilege escalation, or reuse, enabling fixes like MFA or zero-trust to block entry (high impact).

Storage Security:
Probe for misconfigurations, weak encryption, or poor monitoring in storage (e.g., cloud buckets), revealing needs for least-privilege access and alerts on anomalies (medium-high impact).

Supply Chain Risks:
Simulate customer breaches propagating via APIs/integrations, prompting better vendor controls and barriers like token auth (medium impact).

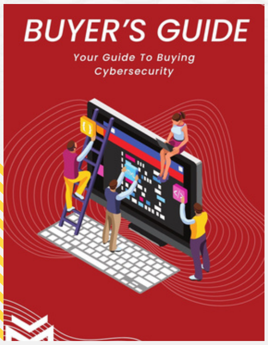
Overall:
An annual pentest pre-2024 could have addressed 80-90% of issues per HIPAA standards, preventing exposure via defense-in-depth. Limitations: Misses novel attacks; requires remediation. Recommend integrating into safeguards, focusing on cloud/credentials for healthcare compliance.

Source: https://www.hipaajournal.com/veradigm-data-breach/

BUYER'S GUIDE

What Every Small-Business Owner Must Know About Purchasing And Protecting Their Company's Critical Data

When exploring cybersecurity solutions with Uncommon Mercenaries (uMercs), focus on these key areas:
Penetration Testing: uMercs offers expert penetration testing to identify vulnerabilities by simulating real-world attacks. Look for their certifications and methodologies to ensure they provide thorough assessments and actionable insights.
Market Pricing: uMercs provides competitive pricing tailored to your organization's needs. Compare their pricing models with industry standards to ensure transparency and value, avoiding hidden costs.
Monitoring and Maintenance: Cybersecurity requires ongoing effort. uMercs delivers continuous monitoring, incident response, and regular updates to keep your defenses strong against evolving threats. Evaluate their monitoring frequency and support responsiveness to ensure effective protection.
By considering these aspects, you can confidently choose uMercs as your cybersecurity partner, safeguarding your organization against cyber threats.



Claim Your FREE Copy Todat At www.umercs.com

CARTOON OF THE MONTH

"Unfortunately, not only have they stolen your identity, they're also living your best life."