DIGITAL DEFENSE DIGEST

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

INSIDE THIS ISSUE

This monthly publication is provided by Black Belt Secure

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

WHY HOSPITALS ARE CYBERCRIMINALS' NUMBER ONE TARGET — AND WHAT YOU CAN DO ABOUT IT

Healthcare has become the most targeted sector in the entire cybersecurity landscape. Ransomware gangs, nation-state actors, and opportunistic hackers all share one thing in common: they know that hospitals and health systems cannot afford even minutes of downtime, hold some of the most sensitive and valuable data on the planet, and have historically underinvested in cybersecurity relative to the risks they face.

That equation is finally beginning to shift — yet the threat landscape is accelerating faster than most organizations can adapt. Sophisticated attacks are growing more frequent, more targeted, and more destructive, often blending ransomware with data extortion and operational disruption. Patient lives, trust, and regulatory compliance are all on the line.

This month's Digital Defense Digest is dedicated entirely to the healthcare sector. Inside, we examine the most pressing threats currently bearing down on hospitals and health systems, unpack the latest regulatory changes reshaping HIPAA compliance and beyond, and deliver practical, actionable steps your organization can take right now to defend patient data, preserve care continuity, and stay on the right side of the law.

We've also partnered with industry leaders to bring you an exclusive, in-depth resource — the Black Belt Secure Healthcare Cybersecurity Report 2026. This comprehensive report dives deep into tailored risk frameworks, proven incident response playbooks, and step-by-step compliance roadmaps specifically designed for healthcare organizations. Whether you're a CISO, IT director, or compliance officer, this report provides the strategic and tactical guidance you need in today's high-stakes environment. You can download the full report for free at: blackbeltsecure.com/healthcare-report-2026

continued on page 2...

...continued from cover

THREAT LANDSCAPE

THE HEALTHCARE CYBERSECURITY CRISIS: BY THE NUMBERS

93%
of healthcare orgs experienced a cyberattack last year

$3.9M
average cost per healthcare cyber incident

36%
surge in ransomware attacks in late 2025

7,419
large healthcare data breaches reported to OCR since 2009

RANSOMWARE: STILL THE APEX PREDATOR

Ransomware remains the single most destructive threat facing hospitals today. Criminal gangs — many operating from overseas — specifically target health systems because they know that even hours of downtime can mean diverted ambulances, canceled surgeries, and compromised patient care. That pressure creates a strong incentive to pay. Tactics are evolving. Rather than simply encrypting files and waiting for a ransom, threat actors are now exfiltrating patient data first and threatening to publish it publicly — a double-extortion approach that creates regulatory exposure on top of operational chaos. Some groups have moved to pure data-theft extortion, skipping encryption altogether to speed up the attack and reduce the chance of
detection. Ransomware in 2026 is a when, not if, scenario for most healthcare organizations.

THE INTERNET OF MEDICAL THINGS (IOMT): A HIDDEN ATTACK SURFACE

The average hospital today manages between 10 and 15 connected medical devices per bed — totaling as many as 350,000 IoMT devices in a single facility. Smart infusion pumps, wireless patient monitors, imaging systems, and surgical robotics all sit on hospital networks, and many were never designed with cybersecurity in mind.
89% of healthcare organizations have the highest-risk IoMT devices — those with known exploitable vulnerabilities linked to active ransomware campaigns — connected directly to the internet somewhere on their network. By 2026, smart hospitals are expected to deploy over 7 million connected medical devices industry-wide. The explosion in connected care is revolutionizing patient outcomes. But it has also created a sprawling, poorly mapped attack surface that most security teams simply cannot keep up with.
A 2025 survey of hospital CISOs found that 43% identified 'complete device visibility' as their single most urgent unsolved problem — ahead of ransomware detection and compliance. Clinical engineering teams frequently deploy new devices without notifying IT security, creating shadow IT at scale, where potentially life-critical equipment sits on the network unmonitored.

BREAKING

Stryker Cyberattack — March 11, 2026

Medical technology giant Stryker was hit by a global cyberattack that disrupted its Microsoft environment. While the company believes the incident has been contained and initial reports indicated no ransomware or malware, the attack triggered immediate coordination between Stryker, the American Hospital Association, and federal government officials to assess impact on hospital operations and supply chains. The incident is a stark reminder that the healthcare supply chain — not just the hospital itself — is a major attack vector.

AI-POWERED ATTACKS & SUPPLY CHAIN RISK

Cybercriminals are now using artificial intelligence to automate reconnaissance, bypass identity controls, and craft highly convincing spear-phishing emails targeted at healthcare professionals. AI-enhanced attacks can adapt dynamically to evade detection tools that rely on known signatures — and can scale across dozens of organizations simultaneously with minimal human involvement.
Supply chain risk has become one of the most pressing challenges in 2026. A breach at a single health IT vendor in 2024 compromised data for roughly 190 million Americans. Every third-party software vendor, cloud provider, and business associate connected to your network is a potential entry point. OCR's current enforcement initiative is specifically focused on HIPAA risk analysis failures, and supply chain due diligence sits at the heart of that standard.

HIPAA 2026: THE MOST SWEEPING SECURITY RULE CHANGES IN OVER A DECADE

For the first time since 2013, the HIPAA Security Rule is being fundamentally overhauled. A Notice of Proposed Rulemaking issued by HHS on December 27, 2024 sets the stage for changes that will reshape how every covered entity and business associate protects electronic protected health information (ePHI). The final rule is expected to be published in May 2026, with a 240-day compliance window following finalization. If your organization has not started preparing, the clock is already running.

The End of 'Addressable' Safeguards

Perhaps the single biggest shift in the proposed rule is the elimination of the 'addressable' implementation specification category. Under the current rule — in place since 2003 — organizations have been allowed to assess their unique circumstances and decide whether certain security controls were reasonable and appropriate to implement. This flexibility created significant inconsistency across the sector, with some organizations skipping controls entirely while properly documenting a business justification. The revised rule eliminates that flexibility. Nearly all implementation specifications will become mandatory, with only narrow exceptions. Regulators have made clear that the existing 'addressable' framework directly contributed to the rise in ransomware attacks and data breaches by allowing organizations to rationalize away critical security controls. Multifactor authentication (MFA), encryption, network segmentation, and audit logging will all be required — not optional.

KEY NEW REQUIREMENTS AT A GLANCE

Requirement	What It Means for Your Organization
MFA Mandatory	Multi-factor authentication will be required for all access to ePHI systems — no longer addressable.
72-Hour Recovery	Organizations must demonstrate the ability to restore critical systems within 72 hours of an incident. Paper disaster recovery plans are not sufficient — restoration must be tested and repeatable.
Annual Risk Assessments	Risk assessments must be more detailed, thoroughly documented, and conducted every 12 months — not just 'periodically.'
Network Segmentation	Technical network segmentation is a mandatory control, designed to contain breaches and limit lateral movement by attackers.
Vendor Verification	Covered entities must obtain written verification at least annually confirming that business associates have implemented required technical safeguards. A signed BAA alone is no longer enough.
Stricter BAAs	Business associate agreements must now specifically enumerate all cybersecurity requirements — MFA, encryption, incident reporting timelines, penetration testing requirements, and more.
24-Hour BA Breach Reporting	Proposed rules include a requirement for business associates to report breaches to covered entities within 24 hours of discovery.
Penetration Testing Required	Regular penetration testing will become a mandatory component of the security program, not an optional best practice.

WHAT HAPPENED ON FEBRUARY 16, 2026

A separate compliance deadline that passed on February 16, 2026 also deserves attention. The 42 CFR Part 2 Final Rule — which governs the confidentiality of substance use disorder (SUD) patient records — came into effect, with OCR immediately beginning active enforcement. Organizations subject to these regulations must now update their Notices of Privacy Practices to explain heightened protections for SUD records, obtain broader patient consent for uses and disclosures, and ensure staff are trained on the new requirements.

ENFORCEMENT IS GETTING MORE AGGRESSIVE

As of January 31, 2026, OCR has 978 data breach investigations open or pending – a backlog that continues to grow. To address this, OCR has narrowed its enforcement focus specifically to HIPAA risk analysis failures, the most commonly cited Security Rule violation. The result: organizations that have failed to conduct proper, documented risk analyses are now the primary targets of OCR investigations and financial penalties. Multi-million dollar fines are possible when violations have persisted for years or reflect systemic non-compliance.

12 STEPS HEALTHCARE ORGANIZATIONS SHOULD TAKE RIGHT NOW

Whether you run a large hospital system, a regional clinic network, or a specialty practice, the following steps represent the highest-impact actions your IT and security team can take to reduce risk, protect patients, and prepare for the new HIPAA requirements heading your way.

Foundational Security Controls

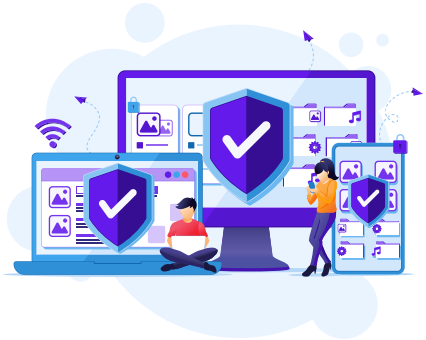
- Conduct a formal HIPAA Security Risk Assessment — right now. If your last one is more than 12 months old, it does not meet the incoming standard. Document everything thoroughly. This is OCR's primary focus in enforcement actions.
- Implement multi-factor authentication (MFA) on all systems that access ePHI. Under the new Security Rule, this will be mandatory. If you have not deployed MFA broadly, start immediately.
- Segment your network. Isolate clinical systems — including connected medical devices — from general administrative networks. Lateral movement from a phishing email should not be able to reach your EHR or patient monitoring systems.
- Inventory every connected device. You cannot protect what you cannot see. Begin a full IoMT asset discovery exercise if one does not exist. Work with clinical engineering to create a process for registering new devices with IT security before they go online.
- Test your incident response plan. Tabletop exercises are no longer enough. You must be able to demonstrate that critical systems can be restored within 72 hours of a ransomware attack — that is the new standard. If you cannot, your business continuity planning has a gap

Vendor and Supply Chain Risk

- Review all business associate agreements. Your BAAs must be updated to specifically enumerate the cybersecurity controls your BAs are required to implement — MFA, encryption, incident reporting timelines, and more. Generic language will not survive an OCR audit under the new rule.
- Obtain annual written verification from business associates that they have implemented required safeguards. A signed BAA is no longer sufficient. You need documented proof of actual implementation.
- Assess your most critical vendors for cybersecurity posture. The Stryker attack in March 2026 is a reminder that a breach at a medical technology vendor can cascade directly into hospital operations. Know which vendors have access to your systems and what their security controls look like.

Detection and Response

- Invest in 24/7 monitoring. Many healthcare organizations, particularly mid-sized hospitals and specialty providers, do not have continuous monitoring. Today's attacks — particularly data-exfiltration-first ransomware — can be detected and potentially stopped if you can identify unusual data movement early.
- Train staff on AI-powered phishing. Your team members are the first line of defense. Modern phishing campaigns are increasingly sophisticated, personalized, and convincing. Regular, realistic training exercises reduce the likelihood of a successful initial compromise.
- Maintain offline, immutable backups. Ransomware groups specifically target backup systems. Backups that are air-gapped or write-protected and that have been tested for restoration are your last line of defense when all else fails.
- Plan for 30-day offline operations. The American Hospital Association recommends that hospitals prepare to deliver safe, quality care for up to 30 days without connected technology. What are your paper-based fallback procedures? Are staff trained on them?



GO DEEPER :THE HEALTHCARE CYBERSECURITY REPORT 2026

This newsletter covers the highlights. Our full Healthcare Cybersecurity Report 2026 goes much further — with detailed risk frameworks, HIPAA compliance road maps, incident response playbooks, IoMT security guidance, and case studies from real-world healthcare breaches.

Download your free copy at:
blackbeltsecure.com/healthcare-report-2026