Healthcare Compliance in 2026: What Your Organization Needs to Know

Regulatory pressure on healthcare organizations is accelerating across CMS policy, workforce law, and cybersecurity. Debra Carpenter (Blue Eagle Consulting), Rebecca Tipton (BMSS Advisors & CPAs), and Jonathan Perz (Abacus Technologies) outline the highest-priority compliance areas your leadership should be addressing today.

CMS REGULATORY UPDATES: WHAT'S CHANGING AND WHY IT MATTERS

- **Electronic Prior Authorization:** CMS is requiring automated, FHIR API-based workflows with strict turnaround timelines and mandatory public reporting of approval and denial rates. Technology streamlines the process, but documentation and medical necessity support remain essential.
- **Hospital Price Transparency:** As of April 1, 2025, hospitals must publish detailed negotiated rate data in machine-readable format. Inaccurate data carries financial penalties and reputable risk, requiring tight alignment across finance, contracting, compliance, and IT.
- **Physician Fee Schedule (PFS):** Telehealth flexibilities should not be assumed permanent. The greatest operational risk is inconsistent workflows and documentation across providers and departments, not misunderstanding the rule itself.
- **TEAM Model (Transforming Episode Accountability Model):** Effective January 1, 2025, selected hospitals are accountable for the full cost and quality of surgical episodes, including post-acute care and readmissions. Success requires strong care coordination and clinical-operational-financial alignment.
- **SAFER Guides:** Hospitals in the Promoting Interoperability Program must complete ONC SAFER Guide self-assessments. Treat this as a genuine improvement exercise, as CMS is expected to require supporting documentation and evidence of remediation going forward.

BMSS Advisors & CPAs

WORKFORCE COMPLIANCE: HR ESSENTIALS FOR HEALTHCARE

- **Hiring:** Job descriptions must define essential functions, physical requirements, and licensure needs. Credentialing must have a dedicated owner with clear renewal tracking, as lapses can result in denied billing before anyone realizes there is a problem.
- **Wage and Hour:** FLSA classification requires both a salary and duties test. All compensable time must be tracked for non-exempt employees, including huddles, charting, training, and on-call time. Automatic break deductions require an interruption process to avoid violations.
- **Leave and Accommodations:** FMLA, ADA, the Pregnant Workers Fairness Act, and the PUMP Act each carry distinct obligations. HR must proactivley recognize when these protections apply, not wait for an employee to invoke them by name.
- **Safety and Privacy:** OSHA compliance, violence prevention, and harassment policies are non-negotiable, and liability extends to patient immediate-access reviews.
- **Documentation: Follow the three C's:** Current, clear, and consistent. Similar issues must be documented similarly to reduce discrimination exposure and demonstrate a fair, defensible process.

CYBERSECURITY: THE HIPAA SECURITY RULE OVERHAUL

- **What is Changing:** The proposed rule, the most significant HIPAA cybersecurity overhaul since 2013, elevates many formerly "addressable" safeguards to require status. Any system touching ePHI must be assessed, documented, tested, and reviewed periodically.
- **Security Risk Analysis:** The foundation of any defensible HIPAA program. It must be a living record covering ePHI location, asset inventory, vendor risks, threat identification, and documented likelihood and impact ratings for every risk pairing.
- **Required Controls:** MFA on all logins, encryption of ePHI at rest and in transit, access logging, routine vulnerability scans, annual penetration testing, documented and tested backup, and recovery procedures.
- **Vendor Oversight:** Business associate agreements will likely need updating once the final rule is published. Covered entities must verify that vendors are actively operating security controls, not just contractually promising them. A 72-hour incident notification requirement is proposed for ePHI-related cybersecurity.

BMSS
Advisors & CPAs

BOTTOM LINE

Healthcare organizations in 2026 are facing simultaneous compliance pressure across CMS policy, workforce law, and cybersecurity, and the cost of falling behind is growing. The organizations best positioned to succeed are those that treat compliance as an operational strategy, standardize their workflows and documentation, and let their regulatory requirements drive technology decisions rather than the other way around. The time to act is now, before the next deadline forces a scramble.

https://www.bmss.com/newsletter-signup/

STAY INFORMED

Sign up for our newsletter and contact us at www.bmss.com and (833) CPA-BMSS

BMSS Advisors & CPAs