BMSS PRESENTS:

A Healthcare Compliance Update

DATE
Thursday,
May 21

BMSS
Advisors & CPAs

TIME
8:30 A.M. -
10:00 A.M. CDT

Debra Carpenter, PhD.

CIO Advisor
Blue Eagle Consulting

Jonathan Perz
Manager of
Information Security
Abacus Technologies

Rebecca Tipton, SHRM-SCP
HR Services Manager
BMSS Advisors & CPAs

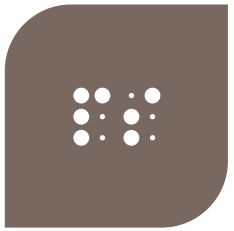
Stephen Von Hagel, CPA
Member
BMSS Advisors & CPAs

2026 CMS Regulatory Updates

- Electronic Prior Authorization (CMS-0057-F)
- Hospital Price Transparency
- Physician Fee Schedule (PFS)
- TEAM Model
- SAFER Guides Requirement

BMSS
Advisors & CPAs

Electronic Prior Authorization Rule



APPLIES TO MA, MEDICAID, CHIP, ACA PLANS

FHIR-BASED ELECTRONIC PRIOR AUTHORIZATION

FASTER DECISIONS: 72 HRS URGENT, 7 DAYS STANDARD

PUBLIC REPORTING OF PA METRICS

Hospital Price Transparency

- Effective Jan 1, 2026
- Median, 10th, 90th percentile rates required
- Include volume of claims
- Enforcement begins April 1, 2026

Physician Fee Schedule 2026

- Updates to reimbursement policies
- Telehealth policy evolution
- Increased documentation requirements
- Impact on physician practices and clinics

BMSS
Advisors & CPAs

TEAM Model

- Mandatory bundled payment model
- Effective Jan 1, 2026
- Hospitals accountable for full episode
- Focus on surgical procedures

SAFER Guides Requirement

EHR SAFETY SELF-ASSESSMENT REQUIRED

FOCUS ON GOVERNANCE AND SAFETY

CLINICAL DECISION SUPPORT AND DOWNTIME PLANNING

REQUIRED FOR PROMOTING INTEROPERABILITY

BMSS Advisors & CPAs

Healthcare HR Compliance Risks

- 24/7 operations create wage compliance issues as well as the potential for fatigue and increased safety issues
- Licenses, certifications, exclusions, and credentials must stay current.
- Employees may also be patients or be related to patients, leading to higher HIPAA compliance risks/ADA risks
- Increased risks for harassment liability due to high level of interaction with non-personnel

Cornerstones of HR Compliance

1 **Hire**

Screening, onboarding, and credentialing

2 **Wage and Hour**

Classifying, tracking time, paying correctly

3 **Leave and Accommodations**

FMLA, ADA, PWFA, jury duty, Voting/Election Officer, Crime Victim, Volunteer Emergency Responder, Adoption, workers' comp

4 **Safety**

OSHA, violence prevention, harassment/discrimination prevention

5 **Privacy**

HIPAA-aware HR processes

6 **Documentation**

Document, retain, audit

Healthy compliance = repeatable and consistent process + manager training + evidence.

Hire

- Job descriptions should reflect essential functions, physical requirements, and licensure needs.
- Credentialing needs ownership over initial processing, renewal dates, and escalation rules to prevent noncompliance in practice
- Screening and background checks should be consistent, job-related, and state-law aware.
- I-9 practices should be timely, centralized, and auditable.
- Onboarding should be consistent and ensure compliance is met, not only with ensuring compliant onboarding processes but also in informing the new employee of what compliance means to their role.

Cornerstone 2

Wage and Hour

- Classify roles carefully: hourly/non-exempt is the default risk-safe posture.
- Track all time worked: pre-shift huddles, charting, donning/doffing, training, and after-hours calls.
- Review automatic meal or break deductions; missed or interrupted breaks are common in clinical settings.
- On-call, travel between sites, and remote work can turn into compensable time.
- Ensure correct overtime rule is in place: 40 hours per week or 8 in 80.
- Ensure correct calculations of overtime pay.

Cornerstone 3

Leave and Accommodations

FMLA	Job-protected leave for eligible employees of covered employers for qualified reasons.
ADA	Interactive process and reasonable accommodation for disability.
PWFA	Pregnancy/Childbirth-related accommodations
PUMP Act	Break time and private space for expressing breast milk.
Workers' Comp	State-law injury claims, return-to-work, light duty.
State-Based Laws	Jury Duty Leave, Voting/Election Officer Leave, Crime Victim Leave, Volunteer Emergency Responder Leave, and Adoption

BMSS Advisors & CPAs

Cornerstone 4

Safety

- Higher amount of OSHA compliance needs: bloodborne pathogen exposure, SHARPS, hazardous chemical handling

- Additionally, workplace violence is more of a threat in many healthcare environments due to increased stress, ranging from threats and verbal abuse to assault.

- Harassment
  - Risks from co-workers/supervisors, vendors, patients, and visitors.
  - Need reporting options for non-standard business hours

Cornerstone 5

Privacy

- Know what is in the HR file, employee medical file, and any patient records — and keep them separate.
- Use minimum necessary access; role changes in HER system should trigger access reviews.
- Educate staff on conflict of interest and access policies; document training/acknowledgement.

Documentation

HR's own version of charting…

The golden rule: **If it is not documented, it did not happen** (If it is documented badly, it did happen — badly)

Follow the 3 C's:

- **Current**
  - Timely, so details remain fresh
- **Clear**
  - Who, what, when, where
  - Are there follow-up actions?
- **Consistent**
  - Similar issues should be documented similarly

Compliance myths that need a second opinion

“Salaried” means no overtime.

Diagnosis: false. Duties + salary basis + current thresholds + state law.

Employees must say “FMLA” or “ADA” to trigger HR.

Diagnosis: false. Managers need to recognize clues.

A complaint about a patient is not an HR issue.

Diagnosis: maybe. It can be safety, harassment, retaliation, or privacy.

At-will employment means an employer can terminate employees without consequence

Diagnosis: false. Employment-at-will means you are not breaching a contract if you terminate an employee without documented due cause. Policies, documentation, and disciplinary action processes prevent liabilities.

BMSS
Advisors & CPAs

Abacus TECHNOLOGIES

HIPAA Cybersecurity Rule Changes

2026 Healthcare Compliance Update

Jonathan Perz
Manager of Information Security

Status checked: May 21, 2026

CURRENT STATUS

Where the HIPAA Security Rule update stands

Abacus TECHNOLOGIES

Dec. 27, 2024

HHS/OCR issued the proposed rule to strengthen cybersecurity protections for ePHI.

Jan. 6, 2025

The NPRM was published in the Federal Register.

Mar. 7, 2025

The public comment period closed.

As of May 21, 2026, the rule is still proposed. The current Security Rule remains in effect until a final rule is published.

- Official planning materials have targeted final action for May 2026, but that is not a guaranteed publication date.
- The safe business posture: prepare now without claiming the proposed rule is already final. The course is clear.

Sources: HHS OCR NPRM page; Federal Register proposed rule, Jan. 6, 2025; RegInfo.gov RIN 0945-AA22.

CORE DIRECTION

What changes if finalized as proposed?

The proposal raises the floor for healthcare cybersecurity.

- **“Addressable”** safeguards largely become **required** — less room to defer controls as optional.
- Requirements apply to all ePHI and systems that affect confidentiality, integrity, or availability.
- Security controls must be implemented, deployed, documented, reviewed, and tested.
- Business associate oversight must become active governance, not passive contract language.

Sources: Federal Register proposed rule; HHS OCR fact sheet.

THE STARTING POINT AND ONGOING RECORD

Security Risk Analysis Drives HIPAA Compliance

Abacus TECHNOLOGIES

A credible HIPAA security program starts with a written, accurate, and thorough assessment of risks and vulnerabilities to ePHI.

It defines scope

What systems, vendors, users, locations, workflows, and data flows affect ePHI?

It identifies risk

What threats and vulnerabilities could affect confidentiality, integrity, or availability of ePHI?

It drives action

Which ePHI safeguards are needed, what is prioritized, and what must be documented?

The Security Risk Analysis is not a one-time report. It is the living record that identifies risk, drives remediation, and supports compliance decisions.

Sources: Federal Register proposed rule at 45 CFR 164.308(a)(2); HHS OCR January 2026 Cybersecurity Newsletter.

PROPOSED RULE EMPHASIS

What a defensible risk analysis must cover

Abacus TECHNOLOGIES

1. ePHI Location & Network Map

Where ePHI is created, received, maintained, transmitted, stored, backed up, and accessed and how it flows through your network.

2. Asset Inventory

Hardware, software, cloud services, electronic media, and systems that affect ePHI.

3. Vendors

Business associates and service providers that affect ePHI or operations.

4. Threats

Reasonably anticipated events that could compromise ePHI confidentiality, integrity, or availability.

5. Vulnerabilities

Weaknesses, missing safeguards, misconfigurations, unpatched systems, and process gaps.

6. Likelihood / Impact

Risk level for each threat-vulnerability pairing, with a documented rationale.

The proposed rule is specific on these risk analysis areas.

Source: Federal Register proposed rule, proposed 45 CFR 164.308(a)(1)–(2).

CONTROLS ARE DOWNSTREAM

What the risk analysis drives

The proposed technical expectations are not random. They flow from known healthcare risks and must be tied back to the organization's risk analysis.

MFA

Logical access to ePHI should be protected with multi-factor authentication.

Encryption

ePHI at rest and in transit should be encrypted using effective methods.

Logging & review

Access and system activity must be monitored, reviewed, and retained.

Vulnerability scans

Routine scans and remediation tracking become harder to treat as optional.

Penetration testing

Annual testing is emphasized to validate control effectiveness.

Backup & recovery

Recovery expectations must be documented, tested, and tied to operational needs.

Leadership question: Can we show why each safeguard is in place, what gap remains, who owns it, and when it will be fixed?

Sources: Federal Register proposed rule; HHS OCR NPRM fact sheet.

Vendor oversight becomes harder to ignore

The proposed rule pushes covered entities to verify that business associates are not just promising security, but operating it.

- Business associate risk should be included in the covered entity's risk analysis.
- Business associate agreements and written arrangements may need updates after a final rule.
- Security expectations should include MFA, encryption, logging, backup, incident notice, and recovery support.
- Annual written verification and evidence requests should become normal governance, not emergency paperwork.

Why it matters

HIPAA enforcement can include corrective action plans and civil monetary penalties reaching up to $2.19M for the highest violation tier.

Federal Register, January 28, 2026, "Annual Civil Monetary Penalties Inflation Adjustment," 91 FR 3665

WHAT TO DO NOW

Practical readiness plan

1. Assess

Perform a HIPAA Security Rule gap assessment and Security Risk Analysis focused on ePHI scope.

2. Prioritize

Rank gaps by likelihood, impact, patient care disruption, legal exposure, and ease of remediation.

3. Remediate

Close obvious control gaps: MFA, encryption, patching, backups, email security, endpoint protection.

4. Prove

Keep evidence of decisions, testing, reviews, exceptions, and fixes.

Recommended Next Step:
Perform a HIPAA Security Rule gap assessment against the proposed requirements and create a 90- to 180-day remediation plan.

Sources: HHS OCR Security Rule guidance; HHS OCR January 2026 Cybersecurity Newsletter.

Questions?

Debra Carpenter, PhD, CHCIO, CHISL
CIO Advisor
Blue Eagle Consulting
debra@blueeagle-consulting.com
208.305.9181

Rebecca Tipton
HR Services Manager
BMSS Advisors & CPAs
rtipton@bmss.com
256.964.9788

Jonathan Perz
Manager of Information Security
Abacus Technologies
jperz@abacustechnologies.com
205.443.5922

If you have a question that you'd like to ask, please use the Q&A Button at the bottom of your screen.

CPE certificates will be issued approximately two weeks after the presentation.

BMSS
Advisors & CPAs