PUBLICATION

OCR's Latest HIPAA Guidance: Strategic Measures to Protect Your Systems and Data

Authors: Alisa L. Chestler, Layna S. Cook Rush
January 14, 2026

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently released its January 2026 Cybersecurity Newsletter, focusing on system hardening and security baselines as critical components of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance. The guidance reinforces OCR's continued expectation that HIPAA covered entities and business associates ("regulated entities") proactively reduce cybersecurity risks to electronic protected health information (ePHI) through ongoing technical and operational safeguards. OCR emphasizes that system hardening directly supports the HIPAA Security Rule's core requirement to ensure the confidentiality, integrity, and availability of ePHI. Privacy and security officers should also consider these recommendations as a baseline for risk management responsibilities and consider integrating the safeguards into internal auditing programs.

Patching Is a Required Risk Management Activity

OCR reiterates in the newsletter that unpatched vulnerabilities are a recurring root cause in HIPAA investigations. To ensure appropriate patching has occurred, regulated entities must:

- Maintain an up-to-date information technology (IT) asset inventory,
- Monitor vulnerability alerts from vendors and authoritative sources (e.g., National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA)),
- Conduct vulnerability scanning, and
- Implement a formal vulnerability management program.

By way of example, without a complete IT asset inventory, an organization cannot be assured that complete patching has occurred on all systems. OCR stresses that patching is continuous, not episodic. Newly discovered vulnerabilities – whether in operating systems, applications, firmware, or even prior patches – must be reassessed through the HIPAA risk analysis and mitigated to a "reasonable and appropriate" level.

Legacy Systems and Unpatchable Vulnerabilities Are Not Excuses

OCR acknowledges that patches may not always be available (e.g., zero-day vulnerabilities or unsupported legacy systems). However, regulated entities are still expected to implement compensating controls, such as disabling unnecessary services; network segmentation; access restrictions; and enhanced monitoring. The failure to patch must be paired with documented alternative safeguards.

Unnecessary Software and Default Accounts Create Hidden Risk

OCR highlights enforcement findings involving:

- Pre-installed or unused software (e.g., games, social media, messaging tools),
- Insecure services (e.g., Remote Desktop Protocol (RDP), File Transfer Protocol (FTP), Telnet), and
- Default or generic administrator/service accounts with weak or unchanged passwords.

Entities should not only remove unneeded software but also confirm that any associated user or service accounts are fully removed, which OCR noted is a frequently overlooked vulnerability.

Security Controls Must Be Enabled and Properly Configured

OCR underscores the importance of configuring both native and third-party security measures, specifically including the following expectations:

- Access controls and authentication (including multifactor authentication where appropriate),
- Encryption,
- Audit logging and monitoring, and
- Anti-malware, endpoint detection and response (EDR), and Security Information and Event Management (SIEM) tools.

Risk analysis should drive decisions about which controls are necessary and where third-party solutions are required. The documentation regarding the risk analysis should be robust enough to support changes and considerations for when tools or practices are not universally deployed.

Security Baselines Are Strongly Encouraged

OCR points to widely used frameworks such as NIST SP 800-53, Microsoft Security Baselines, or Department of Defense Security Technical Implementation Guides. While leveraging these resources can improve efficiency and consistency, OCR cautions that "checkbox" adoption is insufficient. Baselines must be reviewed, understood, and tailored to the entity's environment and documented through the HIPAA risk management process.

Testing and Evaluation Are Mandatory

Before deploying system changes to production, OCR advises testing in development or test environments to avoid unintended impacts on ePHI. Additionally, when environmental or operational changes affect security, the HIPAA Security Rule requires documented technical and non-technical evaluations to confirm continued compliance.

Practical Action Items for Regulated Entities

In light of OCR's guidance, regulated entities should consider:

- Reviewing and updating HIPAA risk analyses to explicitly address patching and system hardening for its systems and as a part of diligence for vendors;
- Auditing systems for unused software, services, legacy databases, and dormant or default accounts;
- Confirming/establishing patch management and vulnerability response timelines through articulated and clear policies and procedures with accountability;
- Assessing whether existing security baselines are documented, current, and tailored to the risk and organization's specific needs; and
- Ensuring evaluations and testing are performed and documented following system changes, i.e., a change management program that is adding to the documented security risk analysis on an ongoing basis.

Why This Matters

OCR's newsletter aligns with enforcement trends showing increasing scrutiny of basic cybersecurity hygiene failures, including unpatched systems, default credentials, and poor configuration management. These issues are frequently cited in OCR resolution agreements and corrective action plans and therefore have a corresponding impact on the growing data breach class-action litigation. System hardening is not merely a

technical best practice; it is a compliance obligation under the HIPAA Security Rule and a very clear risk management tool.

For further analysis tailored to your sector and compliance footprint, please contact the authors – Alisa L. Chestler, CIPP/US, QTE and Layna Cook Rush, CIPP/US, CIPP/C – or another member of Baker Donelson's HIPAA Team.