# OCR Highlights System Hardening as Key to Protecting ePHI in 2026

## EBIA Weekly (January 15, 2026)

*January 2026 OCR Cybersecurity Newsletter: System Hardening and Protecting ePHI*

*Available at:*
***https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-january-2026/index.html***

HHS's Office for Civil Rights (OCR) has released a newsletter that highlights the critical role of system hardening to reduce the risks that HIPAA covered entities and business associates face from cyber threats targeting electronic protected health information (ePHI). System hardening refers to making electronic information systems (i.e., laptops, desktops, servers, mobile devices, virtual machines, routers, and firewalls) safer to reduce the risk of attackers breaking in. By eliminating unnecessary software and services, patching vulnerabilities, and implementing secure configurations, organizations can reduce their "attack surface," thereby reducing the weaknesses and vulnerabilities that an attacker can exploit. OCR emphasizes that hardening is not a single action but an ongoing discipline requiring regular review, documentation, and updates as threats evolve. The newsletter outlines how HIPAA covered entities, business associates, and their workforce can strengthen their defenses through system hardening:

- *Patching Known Vulnerabilities.* Regularly updating operating systems, applications, and security tools is critical. The newsletter notes that often, vulnerabilities can be mitigated by applying patches. OCR recommends establishing a formal patch management process to address vulnerabilities promptly and reduce the risk of exploitation by cybercriminals. OCR stresses the importance of a comprehensive risk analysis to identify all locations where ePHI is created, received, maintained, or transmitted. Maintaining a current inventory of all IT assets is essential for tracking vulnerabilities and ensuring timely updates.
- *Removing or Disabling Unneeded Software and Services.* A key system hardening principle is minimizing unnecessary applications, features, or services, since pre-installed or unused software can contain vulnerabilities or insecure default settings that expand the attack surface. Such software could include, for example, games, messaging apps, social media, or utilities, whether included from the device manufacturer or added by a reseller or other vendor. It may be unnecessary because it duplicates the organization's preferred software solutions or provides an unnecessary or unwanted function or service. OCR warns that unused or weakly secured services—such as remote access or file transfer protocols—should be disabled to prevent attackers from exploiting them. OCR stresses the importance of removing default accounts, changing initial passwords immediately, and ensuring that old service accounts are eliminated when software is uninstalled. Before making these changes, OCR recommends testing them in a nonproduction environment and conducting required HIPAA evaluations to confirm they do not negatively impact ePHI security.
- *Enabling and Configuring Security Measures.* System hardening also requires enabling and properly configuring built in security controls—such as access and audit controls, encryption, and strong authentication including multi-factor authentication. Organizations may implement third-party tools like anti-malware, endpoint detection and response, or security information and event management solutions. Establishing standardized security baselines helps ensure consistent, secure configurations across all systems handling ePHI and must be integrated into an organization's risk analysis and risk management processes.

**EBIA Comment:** The newsletter reinforces that configuration and maintenance of system security settings are compliance obligations under the HIPAA security rule, not merely best practices. As cyber threats to ePHI continue to rise, OCR is recommending updated risk analyses, documented security baselines, and ongoing monitoring and remediation. The newsletter includes resources for further assistance (see our article). Covered entities and business associates should use this guidance to harden their systems and reduce potential vulnerability. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XX.C ("HIPAA Compliance Audits by OCR"), XXI.C ("Regulations and Compliance Dates"), XXIII.A ("Introduction to HIPAA's Privacy and Security Requirements"), and XXIX.E ("Developing Your Security Program").

Contributing Editors: EBIA Staff.