blackwell
Cybersecurity Made for Healthcare

Blackwell Advisory

HHS Cybersecurity Performance Goals Guidance

Executive Insights for IT and Security Strategies in Healthcare

Jason Lee, CISSP
Co-Founder & Chief Information Officer

JASON.LEE@BLACKWELLSECURITY.COM

blackwell
Cybersecurity Made for Healthcare

Mastering HHS Cybersecurity Performance Goals: An Indispensable Guide for Healthcare Leaders

The Department of Health and Human Services (HHS) has recently introduced new voluntary performance goals to enhance cybersecurity within the healthcare sector. These guidelines encompass essential and enhanced goals, emphasizing minimum foundational practices and advanced strategies to bolster cybersecurity resilience.

As a security leader, your role is pivotal in ensuring the successful implementation of these cybersecurity performance goals. You are the key decision-maker in the realm of healthcare cybersecurity, and your understanding and implementation of the HHS guidance are crucial to safeguarding sensitive patient data and maintaining the integrity of healthcare systems.

By adhering to these performance goals, healthcare organizations can fortify their defenses against evolving cyber threats, mitigate risks, and establish a robust cybersecurity framework. The HHS cybersecurity performance goals are not just a set of guidelines, but a pathway to enhancing your organization's cyber resilience and protecting against potential security breaches. Stay tuned to discover how aligning with these goals can transform your cybersecurity practices.

Overview of HHS Cybersecurity Performance Goals

The Department of Health and Human Services (HHS) has established Cybersecurity Performance Goals (CPGs) to safeguard healthcare organizations against cyber threats and enhance overall security measures within the healthcare sector. These goals are categorized into essential and enhanced targets, each serving a distinct purpose in fortifying cybersecurity practices. Below is a visual breakdown of each:

Graphic by [Blackwell Security, Inc](#).

HHS Essential Cybersecurity Performance Goals

The essential goals outlined by HHS focus on establishing foundational cybersecurity practices in healthcare organizations. These goals serve as the fundamental building blocks to ensure the security and integrity of sensitive healthcare data. By adhering to these essential targets, healthcare institutions can implement robust security measures to mitigate risks and protect patient information effectively.

Here is a breakdown of each goal within the **Essential** CPGs:

1. **Mitigate Known Vulnerabilities**: Keep software and systems updated. This straightforward step significantly lowers the risk of attackers exploiting old vulnerabilities, particularly in internet-facing systems.
2. **Email Security**: Activate spam filtering and instruct users to avoid opening suspicious emails or attachments. This fundamental practice can thwart many email-based threats, including phishing and fraud.
3. **Multifactor Authentication**: Implement an additional verification step, such as SMS codes, wherever possible. This basic measure greatly enhances the security of internet-accessible accounts and assets.
4. **Basic Cybersecurity Training**: Teach all organizational members to use strong, unique passwords and to recognize suspicious online activities. This minimal training effort can foster more secure behaviors across the board.
5. **Strong Encryption**: Use standard encryption methods to secure sensitive data in transit, such as employing HTTPS for web interactions. This basic step is crucial for protecting data confidentiality and integrity.
6. **Revoke Credentials**: Immediately remove access rights for individuals leaving the organization. This simple procedure helps prevent unauthorized access to organizational resources.
7. **Basic Incident Planning and Preparedness**: Have a simple response plan ready for cyber incidents, including essential contacts like IT support. Quick, organized reactions can minimize the impact of cybersecurity incidents.
8. **Unique Credentials**: Ensure that every user has their own login credentials, discouraging sharing accounts. This practice aids in monitoring unusual activities and enhances security.
9. **Separate User and Privileged Accounts**: Maintain separate accounts for regular and administrative tasks. This easy-to-implement control measure can protect privileged access from being compromised through general user accounts.

10. **Vendor/Supplier Cybersecurity Requirements**: Select vendors with demonstrable security commitments, even if it's through basic standards or certifications. This approach mitigates risks associated with third-party products and services.

Note: Redefining ***'Basic'*** in CPGs: Recognize that fundamental cyber hygiene practices, though foundational, are powerful tools in preventing a wide array of security incidents, as shown by Blackwell's narrative. Beginning with these critical, yet often underestimated, security measures are vital for averting potential threats. This approach lays a solid foundation for enhanced protection under the Enhanced CPGs and encourages progression within sophisticated maturity frameworks like NIST CSF 2.0.

HHS Enhanced Cybersecurity Performance Goals

In contrast, the enhanced cybersecurity performance goals set by HHS aim to elevate cybersecurity measures in healthcare institutions beyond the basic requirements. These advanced goals are designed to further strengthen security protocols, enhance threat detection capabilities, and bolster incident response mechanisms. By achieving the enhanced goals, healthcare organizations can proactively combat sophisticated cyber threats and safeguard critical healthcare systems.

Here is a breakdown of each goal within the **Enhanced** CPGs:

1. **Asset Inventory**: Develop a thorough inventory management process to identify and track all assets, including those that are unmanaged or part of the shadow IT. This allows for quicker detection and response to vulnerabilities and threats affecting organizational assets.
2. **Third-Party Vulnerability Disclosure**: Implement a structured approach for the timely identification and remediation of vulnerabilities within third-party products and services, enhancing the security resilience against external threats.
3. **Third-Party Incident Reporting**: Establish a robust mechanism for the swift reporting and management of security incidents involving third-party vendors, ensuring that breaches are contained and resolved effectively to minimize their impact.

4. **Cybersecurity Testing**: Conduct regular penetration tests and attack simulations to identify and address vulnerabilities proactively. Share findings responsibly to foster a culture of continuous security improvement and awareness.
5. **Cybersecurity Mitigation**: Create internal protocols to quickly act upon vulnerabilities revealed through security assessments, prioritizing remediation efforts based on the severity and potential impact of each vulnerability.
6. **Detect and Respond to Relevant Threats and TTPs**: Ensure the organization can recognize and counteract evolving cyber threats. Implement endpoint protection solutions and strategies for securing network entry and exit points against unauthorized access.
7. **Network Segmentation**: Strategically divide the network into segregated zones to restrict unauthorized access and reduce the scope of potential lateral movement by attackers within the network, safeguarding critical assets more effectively.
8. **Centralized Log Collection**: Aggregate log data from across the network into a centralized repository to enhance visibility into security events, facilitating more efficient and effective incident analysis and response.
9. **Centralized Incident Planning and Preparedness**: Standardize incident response planning across the organization, regularly updating and practicing response procedures to ensure readiness for addressing emerging cybersecurity challenges.
10. **Configuration Management**: Establish and maintain standard configurations for all devices and systems, aligning with best practices and security benchmarks to mitigate risks associated with misconfigurations and vulnerabilities.

Potential Amendments to the HIPAA Security Rule by HHS

There is speculation regarding potential amendments to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule by HHS to align with evolving cybersecurity requirements in the healthcare sector. The proposed amendments aim to enhance data protection measures, address emerging cyber threats, and strengthen regulatory frameworks to ensure compliance with evolving cybersecurity standards.

Financial Incentives and Penalties for Adhering to or Violating CPGs

Blackwell mentions the potential penalties within a blog post here. There has been proposed funding within the 2025 U.S. Federal Budget to allow for health systems to fund their cybersecurity programs in adhering to the CPGs. This funding has yet to make its way to the President's office at the time of this guidance by Blackwell Security. In addition to potential funding, penalties for non-compliance with these goals may be introduced. The American Hospital Association (AHA) has voiced concerns about imposing penalties and advocates for a balanced approach that incentivizes compliance while supporting organizations in enhancing their cybersecurity posture.

Funding in the Federal 2025 Budget for HHS Cybersecurity Guidelines

The federal 2025 budget includes allocations to support implementing and enforcing the HHS Cybersecurity Performance Goals. These funds are dedicated to enhancing cybersecurity initiatives in the healthcare sector, facilitating the adoption of best practices, and promoting collaboration between government agencies and healthcare organizations to strengthen the overall security posture.

For more information on HHS Cybersecurity Performance Goals, refer to HPH Cybersecurity Performance Goals and stay informed about the evolving landscape of cybersecurity in healthcare.

Relationship between 405(d) and HHS Cybersecurity Guidelines

The HHS Cybersecurity Performance Goals align with the guidelines outlined in section 405(d) to collectively enhance cybersecurity practices in the healthcare sector. By integrating the principles of 405(d) with the CPGs, healthcare organizations can establish a cohesive framework for implementing robust cybersecurity measures, fostering a culture of security awareness, and strengthening defenses against cyber threats.

Relationship between NIST CSF and HHS Cybersecurity Guidelines

The HHS CPGs and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) are both critical resources designed to improve cybersecurity practices within organizations. However, they serve somewhat different purposes and are tailored to different audiences, leading to distinct approaches and focuses. The HHS Cybersecurity Program Guide (CPG) offers tailored, tactical approaches for quick wins in safeguarding patient data and building quick resilience, making it an essential tool for healthcare entities looking to address cybersecurity threats efficiently. While the HHS CPG provides the specificity needed for immediate action in the healthcare context, achieving maturity in the NIST Cybersecurity Framework 2.0 (CSF 2.0) remains a valuable strategic goal for comprehensive risk management and cybersecurity governance.

For healthcare organizations looking for immediate, tactical approaches to protect patient data and build resilience, the HHS Cybersecurity Program Guide offers targeted guidance and quick wins. These initial steps are crucial for safeguarding against imminent threats and establishing a foundation for cybersecurity.

Available HHS Cybersecurity Training Resources

HHS provides comprehensive training resources to assist healthcare professionals in enhancing their cybersecurity knowledge and skills. These resources offer valuable insights into the latest cybersecurity practices, threat mitigation strategies, and best practices for securing healthcare data. Healthcare professionals can access these training modules to stay informed about evolving cybersecurity trends and enhance their cybersecurity acumen.

Conclusion

Aligning with the HHS Cybersecurity Performance Goals is paramount for healthcare organizations to enhance their data security measures. These goals, encompassing essential and enhanced practices, serve as a framework for mitigating cyber threats and safeguarding sensitive information within the healthcare sector. By adhering to these guidelines, Chief Information Officers, Chief Information Security Officers, and Chief Security Officers can proactively strengthen their cybersecurity posture and ensure the confidentiality and integrity of patient data. Embracing these performance goals not only fosters compliance with industry standards but also bolsters overall resilience against evolving cyber risks. Stay vigilant, stay secure.

Author Biography

Jason Lee has nearly two decades of expertise in managed services, cybersecurity, and technical infrastructure. His tenure at Deloitte, NTT, and Secure-24 showcased his expertise in leading global security initiatives and aligning technology with business goals to foster the development of secure digital transformation across many industries. Having functioned as a global CISO, he champions cybersecurity and operational excellence, driving innovation to improve healthcare outcomes while ensuring compliance with regulations like PCI, HIPAA, and HITRUST. Jason's forward-thinking approach aims to empower healthcare providers to safeguard patient data, envisioning a future where technology infrastructure fortifies against threats and fosters secure patient care