**Cyber Performance Goals (CPGs) Compared with What was Included in the HIPAA Proposed Security Rule**

**January 15, 2025**

| | Essential CPGs | Proposed Security Rule |
|---|---|---|
| **1.** | **Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet. | Part of Risk Management Standard<br>- Section 164.308(a)(5)(i)<br>- Page 145 |
| **2.** | **Email Security:** Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud. | Part of Security Awareness Training Standard<br>- Section 164.308(a)(11)(i)<br>- Page 170<br>Part of Configuration Management Standard<br>- Section 164.312(c)(1)<br>- Page 232<br>Part of Authentication Standard<br>- Section 164.312(f)(1)<br>- Page 242 |
| **3.** | **Multifactor Authentication:** Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet. | Part of Authentication Standard<br>- Section 164.312(f)(1)<br>- Page 242 |
| **4.** | **Basic Cybersecurity Training:** Ensure organizational users learn and perform more secure behaviors. | Part of Security Awareness Training Standard<br>- Section 164.308(a)(11)(i)<br>- Page 172 |

| | | |
|---|---|---|
| **5.** | **Strong Encryption:** Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion. | Part of Encryption and Decryption Standard<br>- Section 164.312(b)(1-3)<br>- Page 221 |
| **6.** | **Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers:** Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly. | Part of Workforce Security Standard<br>- Section 164.308(a)(9)(i)<br>- Page 157 |
| **7.** | **Basic Incident Planning and Preparedness:** Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents. | Part of Security Incident Procedures Standard<br>- Section 164.308(a)(12)(i-ii)<br>- Page 174 |
| **8.** | **Unique Credentials:** Use unique credentials inside organizations' networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks. | Part of Standard: Access Control Standard<br>- Section 164.312(a)(2)(i)<br>- Page 213 |
| **9.** | **Separate User and Privileged Accounts:** Establish secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised. | Part of Standard: Access Control Standard<br>- Section 164.312(a)(2)(ii)<br>- Page 216 |
| **10.** | **Vendor/Supplier Cybersecurity Requirements:** Identify, assess, and mitigate risks associated with third party products and services. | Part of Business Associate Contracts and Other Arrangements Standard<br>- Section 164.308(b)(1) and (2<br>- Page 182 |
| | **Enhanced CPGs** | **Proposed Security Rule** |
| **11.** | **Asset Inventory:** Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to potential risks and vulnerabilities. | Part of Technology Asset Inventory Standard<br>- Page 121<br>- Section 164.308(a)(1)(i) |
| **12.** | **Third Party Vulnerability Disclosure:** Establish processes to promptly discover and respond to known threats and vulnerabilities in assets provided by vendors and service providers. | Part of Vulnerability Management Standard<br>- Section 164.312(h)(1)<br>- Page 251<br>Part of Business associate contracts or other arrangements Standard<br>- Section 164.314(a)(2)<br>- Page 262 |

| | | |
|---|---|---|
| **13.** | **Third Party Incident Reporting:** Establish processes to promptly discover and respond to known security incidents or breaches across vendors and service providers. | Part of Security Incident Procedures Standard<br>- Section 164.308(a)(12)(i-ii)<br>- Page 174 |
| **14.** | **Cybersecurity Testing:** Establish processes to promptly discover and responsibly share vulnerabilities in assets discovered through penetration testing and attack simulations. | Part of Patch Management Standard<br>- Section 164.308(a)(4)(i)<br>- Page 140<br>Part of Vulnerability Management Standard<br>- Section 164.312(h)(1)<br>- Page 251 |
| **15.** | **Cybersecurity Mitigation:** Establish processes internally to act quickly on prioritized vulnerabilities discovered through penetration testing and attack simulations. | Part of Patch Management Standard<br>- Section 164.308(a)(4)(ii)<br>- Page 140 |
| **16.** | **Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTP):** Ensure organizational awareness of and ability to detect relevant threats and TTPs at endpoints. Ensure organizations are able to secure entry and exit points to its network with endpoint protection. | Part of Configuration Management Standard<br>- Section 164.312(c)(1)<br>- Page 232 |
| **17.** | **Network Segmentation:** Mission critical assets are separated into discrete network segments to minimize lateral movement by threat actors after initial compromise. | Part of Access Control Standard<br>- Section 164.312(a)(2)(vi)<br>- Page 219 |
| **18.** | **Centralized Log Collection:** Collection of necessary telemetry from security log data sources within an organization's network that maximizes visibility, cost effectiveness, and faster response to incidents. | Part of Audit Trail and System Log Controls Standard<br>- Section 164.312(d)(1)<br>- Page 235 |
| **19.** | **Centralized Incident Planning and Preparedness:** Ensure organizations consistently maintain, drill, and update cybersecurity incident response plans for relevant threat scenarios. | Part of Security Incident Procedures Standard<br>- Section 164.308(a)(12)(i-ii)<br>- Page 174 |
| **20.** | **Configuration Management:** Define secure device and system settings in a consistent manner and maintain them according to established baselines. | Part of Configuration Management Standard<br>- Section 164.312(c)(1)<br>- Page 232 |