Compliance Today - August 2024

Julie Hughes (jhughes@codyconsulting.com) is the Chief Compliance and Consultancy Officer at Cody Consulting Group in Tampa, FL.

Regulatory framework for healthcare cybersecurity requirements and standards

by Julie Hughes, JD, MS, CHC, CPC

Numerous high-profile cybersecurity events have impacted healthcare operations nationally and focused attention on cyber resiliency within the healthcare sector. These events reinforce the saliency of broader cybersecurity strategies announced by the Biden administration and the U.S. Department of Health and Human Services (HHS). As a result of these national and sector-specific initiatives, healthcare organizations should be prepared for increased accountability and new regulations related to cybersecurity practices and outcomes.

National cybersecurity strategy

In March 2023, the Biden administration published the *National Cybersecurity Strategy*, which focused on collaboration and concentrates on five pillars:[1]

- **Defend critical infrastructure**: This includes establishing new and enhanced cybersecurity regulatory frameworks.
- **Disrupt and dismantle threat actors**: This is done through improved intelligence sharing and prevention.
- **Shape market forces to drive security and resilience**: This can be accomplished by increasing accountability, liability, and incentives for entities that hold personal data.
- **Invest in a resilient future**: This includes innovation, research and development, and education.
- **Forge international partnerships to pursue shared goals**: This will maintain an open, free, and secure global internet ecosystem.

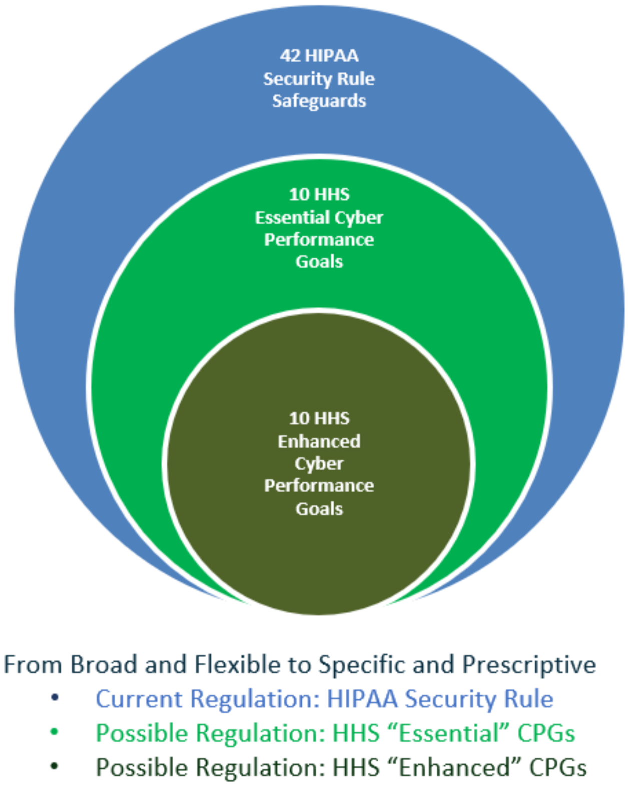
In line with the national strategy, in December 2023 HHS released *Healthcare Sector Cybersecurity*, which acknowledges, “Healthcare facilities are attractive targets for cyber criminals in light of their size, technological dependence, sensitive data, and unique vulnerability to disruptions.”[2] In its introduction to HHS’s strategy to protect the healthcare sector, it outlines four actions to take to improve cyber resiliency and protect patient data:

1. **Establish voluntary cybersecurity goals for the healthcare sector**: Publish voluntary Healthcare-specific and Public Health Cybersecurity Performance Goals (HPH CPGs) to help healthcare organizations plan and prioritize high-impact cybersecurity practices.
2. **Provide resources to incentivize and implement these cybersecurity practices**: Work with Congress to develop support and incentives for domestic hospitals to improve cybersecurity.

3. **Implement an HHS-wide strategy to support greater enforcement and accountability**. Greater enforcement and accountability will be achieved through incorporating new cybersecurity standards—informed by the HPH CPGs—into existing programs, including Medicare, Medicaid, and HIPAA.
4. **Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity**: the Administration for Strategic Preparedness and Response's coordination role as a "one-stop shop" for healthcare cybersecurity to improve coordination and partnership within and between government and industry constituents.

While much of HHS's approach continues to unfold, the release of the HPH CPGs completes the first pillar of action; it provides insight into the third pillar of action, specifically how cybersecurity standards may be incorporated into the existing regulatory framework to support protecting sensitive data.

Figure 1: Current and Emerging Regulation


42 HIPAA Security Rule Safeguards
10 HHS Essential Cyber Performance Goals
10 HHS Enhanced Cyber Performance Goals
From Broad and Flexible to Specific and Prescriptive
• Current Regulation: HIPAA Security Rule
• Possible Regulation: HHS "Essential" CPGs
• Possible Regulation: HHS "Enhanced" CPGs

This document is only available to members. Please log in or become a member.

Become a Member Login