Report on Patient Privacy Volume 24, Number 2. February 08, 2024 HHS Unveils Voluntary Cybersecurity Goals To Harden Systems; Many Will Seem Familiar

By Jane Anderson

New voluntary health-care-specific, cybersecurity performance goals released by HHS Administration for Strategic Preparedness and Response (ASPR) call on health care organizations to take both basic and more advanced steps to harden their cybersecurity stance against cybercriminals, ultimately protecting patient health information and safety.

The overall document[1] —released less than two months after HHS said it would establish voluntary cybersecurity goals for the health care sector that it said eventually could become mandatory[2] —urges organizations to start by meeting "essential goals" designed to help health care entities address common vulnerabilities. Goals include implementing email security measures and employing basic cybersecurity training.

A second set of "enhanced goals" can help organizations with more advanced security postures "mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors," according to the ASPR document.

"These goals are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety," the report said.

Ultimately, though, these goals could become mandatory for hospitals through Medicare and Medicaid, HHS said in its December concept paper. That paper outlined four "pillars for action": (1) publish voluntary health care and public health sector cybersecurity performance goals; (2) work with Congress to provide resources to incentivize and implement cybersecurity practices across the health care and public health sector; (3) implement an HHS-wide strategy to support greater enforcement and accountability by incorporating the goals into existing regulations and programs; and (4) expand and mature the one-stop shop within HHS for health sector cybersecurity.