MEDTECH INSIGHT
CITELINE COMMERCIAL

14 Feb 2024 | **News**

HHS Releases 'Essential' And 'Enhanced' Cybersecurity Performance Goals

by Hannah Daniel

HHS publishes a new website and releases its essential and enhanced voluntary cybersecurity performance goals.

As promised, the Department of Health and Human Services has released its *voluntary cybersecurity performance goals* (CPGs), split into "essential" and "enhanced" goals. A related *website* from HHS.gov, posted 24 January, offers resources intended to connect the healthcare and public health (HPH) sector with the department.

While the CPGs are currently voluntary, the HHS is working to establish enforcement informed by the goals around cybersecurity standards for healthcare delivery organizations (HDOs), HHS Deputy Secretary Andrea Palm said in a *release*.

The CPGs were created to "directly address common attack vectors against U.S. domestic hospitals as identified in the *2023 Hospital Cyber Resiliency Landscape Analysis*," the release reads.

Essential goals are the bare minimum for healthcare cybersecurity and set a "floor of safeguards" to protect HDOs from cybersecurity attacks.

The essential goals are:

- Mitigating known vulnerabilities;
- Reducing risk from email threats;
- Introducing multifactor authentication;

2024 HIPAA Update Will Include Cybersecurity Requirements

By Hannah Daniel

14 Dec 2023 A new report explains how the Department of Health and Human Services

plans to incentivize good cybersecurity practices for healthcare organizations. Read the full article here

- Conducting basic cybersecurity trainings;
- Encrypting sensitive data;
- Revoking credentials of departing employees in a timely manner;
- Creating unique credentials to detect anomalous activity within systems;
- Separating accounts based on security levels; and
- Extending cybersecurity requirements to third-party partners.

These are considered basic, good cybersecurity practices across industries. (Also see "*FDA And CISA Device Cybersecurity Agreement Needs To Be Updated, GAO Says*" - Medtech Insight, 4 Jan, 2024.)

The HHS's enhanced set of goals is resource-dependent and intended to help organizations "mature" their cybersecurity and reach the "next level of defense" against threats.

These include:

- Inventorying assets to identify known and unknown assets and detect vulnerabilities more quickly;
- Establishing processes for identifying, detecting and reporting vulnerabilities in third-party partnerships;
- Cybersecurity testing, such as penetration testing;
- Detecting and responding to threats and common techniques used by threat actors;
- Segmenting networks to prevent threat actors from accessing multiple assets;

What is penetration testing?

"Penetration testing often includes hiring a third party to test a system's vulnerabilities by trying to exploit the system as much as possible. After the tests are finished, the vulnerabilities are reported back to the organization for fixing." (Also see "*Vulnerabilities Up 59%: The State Of Healthcare Cybersecurity In 2023*" - Medtech Insight, 10 Aug, 2023.)

- Creating centralized log collection and incident planning and responses; and
- Defining a baseline of secure device and system settings.

The report's appendices outline these goals in greater detail, including desired outcomes and implementation resources.

The HHS's CPG website also has a comprehensive, *guided tour* of its CPGs in a different format that acts as a checklist for organizations.