# Health Information Compliance Alert

## Toolkit: Enhance Cybersecurity Skills With These Federal Tools

**Tip: Start small as you ramp up your implementation of new policies.**

If you're trying to reduce data risks or put together a cybersecurity training program, the feds recently designed a website that offers quick advice on a variety of topics - specifically for healthcare organizations.

**Lowdown:** Last December, the Department of Health and Human Services (HHS) set up a website for its 405(d) Aligning Health Care Industry Security Approaches Program. The online tools are a collaboration between industry experts and the feds, aka the HHS 405(d) Task Group, and aims to align healthcare organizations' compliance with regulations to better fight cyber threats en masse, an HHS release suggests.

"This website is the first of its kind! It's a unique space where the healthcare industry can access vetted cybersecurity practices specific to the [healthcare and public health] HPH sector on a federal government website," says **Erik Decker,** 405(d) Task Group Industry co-lead, in the HHS release. "I think it's a great resource for the HPH sector to turn to and will surely be a go-to site for organizations that want to better protect their patients and facilities from the latest cybersecurity threats."

**Understand the Nuts and Bolts of the 405(d) Website**

Among HIPAA's Security Rule provisions, the option to design your organization's compliance program can be simultaneously liberating and daunting. The 405(d) guidance touches on this perennially challenging task.

"The great thing about 405(d) is that it offers 10 best practices to improve security, and it breaks them down into recommendations based on organizational size," says **Jen Stone, MCIS, CISSP, CISA, QSA,** principal security analyst, with Security Metrics in Orem, Utah. "This means that even small practices with limited funding can get started with reasonable security controls."

With the 405(d) resources, practices can access tools to help with common issues that sometimes lead to data breach problems later on. "For example, implementing unique account IDs will allow a small organization to prevent terminated employees from accessing protected information after they leave. This type of account management is an area where we have seen significant breaches occur, but it's preventable using tools that are already paid for or have free versions," Stone explains.

Smaller providers don't always have the financial means nor the staff to dedicate toward cybersecurity and risk management; however, the 405(d) identifies the most common threats to these organizations and offers role-specific tips.

"Healthcare professionals, especially in smaller practices, often struggle because they take on many roles," Stone points out. "Cybersecurity best practices aren't complex, but not everyone knows where to find a quick summary of threats or the solutions to counter them. Fortunately, 405(d) offers both."

She adds, "A few of the most effective practices include multi-factor authentication, anti-malware, and timely patching."

**Important:** With more staff working from home, new challenges have popped up with access and security controls. Another area of critical importance is cybersecurity education - employees must understand the risks associated with remote work and how to recognize problems.

"Remote staff are becoming well versed in the technologies that keep us together while apart," Stone says. "The real trick is to make training meaningful so people will pay attention and retain it. Make sure the training you choose is focused on the type of work each staff member does so it will help them counter privacy and security challenges they will actually face."

**Resource:** Find the 405(d) website at https://405d.hhs.gov/public/navigation/home.