

Report on Patient Privacy Volume 19, Number 11. November 07, 2019 Checklist for Using Health Industry Cybersecurity Practices

By Jane Anderson

Take a “cookbook” approach to using the four-volume HHS report “Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients,” urged Julie Chua, risk management lead in the HHS Office of the Chief Information Officer.

That means prioritizing the threats that are most important to you, breaking them down into components, and implementing the report’s recommendations on those components, Chua at a recent conference in Washington, D.C.

For example, she said, to manage phishing an organization might use the report’s sections on:

- basic email protection controls
- multi-factor authentication
- workforce education
- incident response plays
- digital signatures for authenticity
- advance and next general tooling

These sections come together in a “recipe” that creates an overall response to the threat posed by phishing, she said. Also, just as with any cookbook, Chua said, the “recipes” for combatting cyberthreats only provide the basic instructions. They do not teach you to cook, tell you which recipes to use, or limit your ability for substitutions, she noted.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)