COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 11. November 07, 2019 Health Industry Eager to Use Step-by-Step Cyber Security Practices in HHS Report

By Jane Anderson

Officials from the National Institute of Standards and Technology (NIST) and the HHS Office for Civil Rights (OCR) say they are seeing some success in spreading the do-it-yourself-style cybersecurity messages contained in a major report released late last December.

The four-volume HHS report "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients"[1] contains a wealth of information on how health care organizations of all types and sizes can voluntarily protect themselves – so much information, in fact, that users may become overwhelmed. But the report's architects tried to break it down into more digestible pieces, and that may have worked.

"We have been reaching out to a lot of the health sector conferences and events; however, we have also been lucky that people are asking for us to come to their meetings," said Julie Chua, risk management lead in the HHS Office of the Chief Information Officer.

"We have been engaging with them, and we know that this is something that they are in need of and they are actually using," Chua told attendees at the OCR-NIST HIPAA security conference held in Washington, D.C., in October.

With respect to HIPAA compliance, OCR will not look at whether an organization has implemented these recommendations, said Nicholas Heesters, OCR health information privacy specialist. "We are not going to go into an investigation compliance review specifically looking for HICP practices," Heesters told attendees at the meeting.