COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 18, Number 8. August 31, 2018 Experts Warn CEs to Implement Safeguards for Data-Sharing APIs

By HCCA Staff

Application programming interfaces (APIs), increasingly used to connect unrelated software programs, will be exploited to hack health care organizations and others holding sensitive data, and covered entities (CEs) need to build strong technical defenses to manage these risks, experts advise.

Clyde Hewitt, vice president, security strategy for CynergisTek Inc., says that well-designed, implemented and managed APIs for health data should include authentication, authorization, encryption and signatures to ensure secure connections. "Managing the technical risks of securely exchanging credentials between systems is easier by comparison as interface standards—e.g., Security Assertion Markup Language, or SAML—exist," Hewitt tells *RPP*. "Other emerging standards exist and are listed on the government's HealthIT website," described later in this story.

The Healthcare Information and Management Systems Society warns that hackers will use common exploits such as man-in-the-middle attacks, session cookie tampering, and distributed denial of service attacks. APIs are used to allow data to flow between such unrelated systems as electronic medical records (EMRs) and third-party apps that collect and use health data.