COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 11. November 11, 2021 OCR Offers Legacy System Security Checklist

By Jane Anderson

Many health care organizations rely on legacy systems that contain electronic protected health information (PHI), and these systems can be more difficult to secure, because components may have been supplanted by newer technology and manufacturers may have discontinued support.

These legacy systems may not be ideal from a security standpoint, but there are many reasons health care entities continue to use them, the HHS Office for Civil Rights (OCR) acknowledged.[1] For example, OCR said:

- The organization may not be able to replace the legacy system—which may include medical devices, electronic health records and other systems offering critical services—without sacrificing availability of data, disrupting critical services or compromising data integrity.
- The organization may be "reluctant to tinker with technology that appears to be working, or to deploy a new and unfamiliar system that may reduce efficiency or lead to increased user errors."
- The organization may be reluctant "to replace a system that is well-tailored to its business model, or with which it has a high degree of competence.
- "The organization's other systems depend on the legacy system or are incompatible with newer systems.
- "The organization is unable to dedicate the time, funds, or human resources needed to retire and replace the legacy system."