imprivata®

BECKER'S HOSPITAL REVIEW

Why healthcare CIOs and CISOs need an integrated identity and access strategy — 5 lessons

Digital identity is the key to security for today's healthcare networks. A digital identity ecosystem must be flexible, not only to deal with an ever-changing environment of users, locations, devices and applications, but also the changing roles and access required by every healthcare employee as they move through different shifts, organizations, and stages of their careers.

During a recent webinar hosted by Becker's Hospital Review and sponsored by Imprivata, Wes Wright, chief technology officer at Imprivata, talked with Chris Paravate, chief information officer at Northeast Georgia Health System (NGHS), about the digital identity program at NGHS, as well as the challenges and results.

Five key learnings:

1. **Rapid implementation of IT solutions has led to fragmented security and identity management.** "We've spent the last decade implementing technology systems that are now essential in day-to-day operations," Mr. Paravate said. "However, this hybrid system has created a fractured process around identity management and role provisioning."

2. **Significant resources are required to manage this fragmented system.** Mr. Paravate said he has six full-time individuals handling provisioning exceptions; while six sounds like a lot, Mr. Wright stated he knows an organization with six times as many staff members doing the same work. "The existing framework is, frankly, outpacing us," Mr. Paravate said. "We are focused on redesigning our architecture."

3. **Organizations need a flexible digital identity framework that addresses all key areas in healthcare.** Imprivata has created such a framework based on 32 different capabilities. "It's a blueprint for strategic planning around digital identity," Mr. Wright acknowledged.

   Mr. Paravate explained the importance of flexibility in such a framework. "We have all of these big applications in our environment like ERP or EMR systems," he said. "However, other applications will increasingly come and go because they enable the use of those systems. We need to create an ecosystem where all those things can coexist."

4. **Digital identity must be fluid, meeting the changing needs of staff throughout the day.** Mr. Paravate shared an example of how fluid digital identity must be in practice. "Let's say I've got nurses who share a department smartphone," he said. "When they pick up that phone, they tap their badge, which automatically assigns them to a role. They can receive alerts and are dynamically placed in a phone directory." When they put the phone back, the system removes them from that role.

   "This identity framework creates a control plane for individuals to plug into and out of the system," he explained. "We have to recognize that these things are fluid, so we have to be fluid in the way that we're managing identity through those roles."

5. **An effective digital identity system must make security easy and relevant.** To facilitate adoption, it's critical that all teams understand how security will further departmental objectives. "The role of the CIO is to remove the hassle, burden and overhead of security so that clinicians, for example, can be in the moment," Mr. Paravate said.

   Mr. Wright noted that clinicians are going to do what they need to do to serve their patients. "We need to give them the right tools to make doing the right thing from a security standpoint easier than not doing the right thing," he said. "Once we do that, the whole organization will be just as security conscious as we are."

Watch webcast