i imprivata®

Northeast Georgia Health System transforms communications with mobile-first strategy powered by Imprivata

Digital identity solutions break down mobile technology adoption barriers, simplify access security, and unleash mobile productivity

Northeast Georgia Health System, Inc.™

Challenge

- Transform into a mobile-first organization
- Unify and modernize communications and collaboration
- Optimize user experience, safeguard PHI, and simplify operations

Solution

- Imprivata digital identity solutions provide frictionless security for shared and BYOD endpoints
- Cloud-based management tools make it easy to track, support, and maintain shared assets

Results

- Identity-based approach streamlines communications, automatically sending calls and messages to the right device
- Seamless workflows save time, improving user satisfaction and patient care
- Shared mobile devices contain CAPEX
- Comprehensive digital identity solution portfolio removes mobile technology adoption barriers, accelerates time-to-value, and mitigates risk

> "We have used Imprivata for identity governance and SSO for our traditional endpoints and applications for years. Imprivata Mobile Access and Control lets us easily extend those familiar workflows to shared mobile devices."
>
> – Chris Paravate, Chief Information Officer
>   Northeast Georgia Health System

Organization Snapshot

A not-for-profit community health system dedicated to improving the health and quality of life of the people of Northeast Georgia, with five hospital campuses, 850+ beds, and 11,000+ employees including 1,300+ medical staff members.

Overview

Northeast Georgia Health System (NGHS) uses Imprivata digital identity solutions to optimize mobile productivity, streamline workflows, and safeguard protected health information (PHI). The solutions empower the healthcare system to take full advantage of all the benefits of mobile technology, including shared mobile devices, without sacrificing security, visibility, or control.

Clinicians use shared mobile devices or their personal mobile devices to access Epic mobile apps and Vocera unified communications (UC) tools – effortlessly and securely. With the identity-based approach, voice calls and messages are automatically directed to the right device based on a person's name or current role.

Challenge: Unify and modernize communications

Like many healthcare delivery organizations, NGHS was constrained by a disjointed collection of legacy communications solutions – conventional voice systems, legacy cordless phones, pagers, proprietary messaging tools, etc. – that were inherently inefficient and ineffective. These outdated solutions impeded clinical productivity, squandered valuable time, and impaired critical communications.

"Hospitals are notoriously dynamic environments. Clinicians are always moving around and changing roles," explains Chris Paravate, Chief Information Officer at NGHS. "Historically, we had no way to assign a human identity to an endpoint, so our user community had no way to know how to contact any particular person at any particular time. You had to dial the switchboard to find a specialist on call. And charge nurses were writing extension numbers on index cards at the beginning of each shift so they would know how to reach the right people."
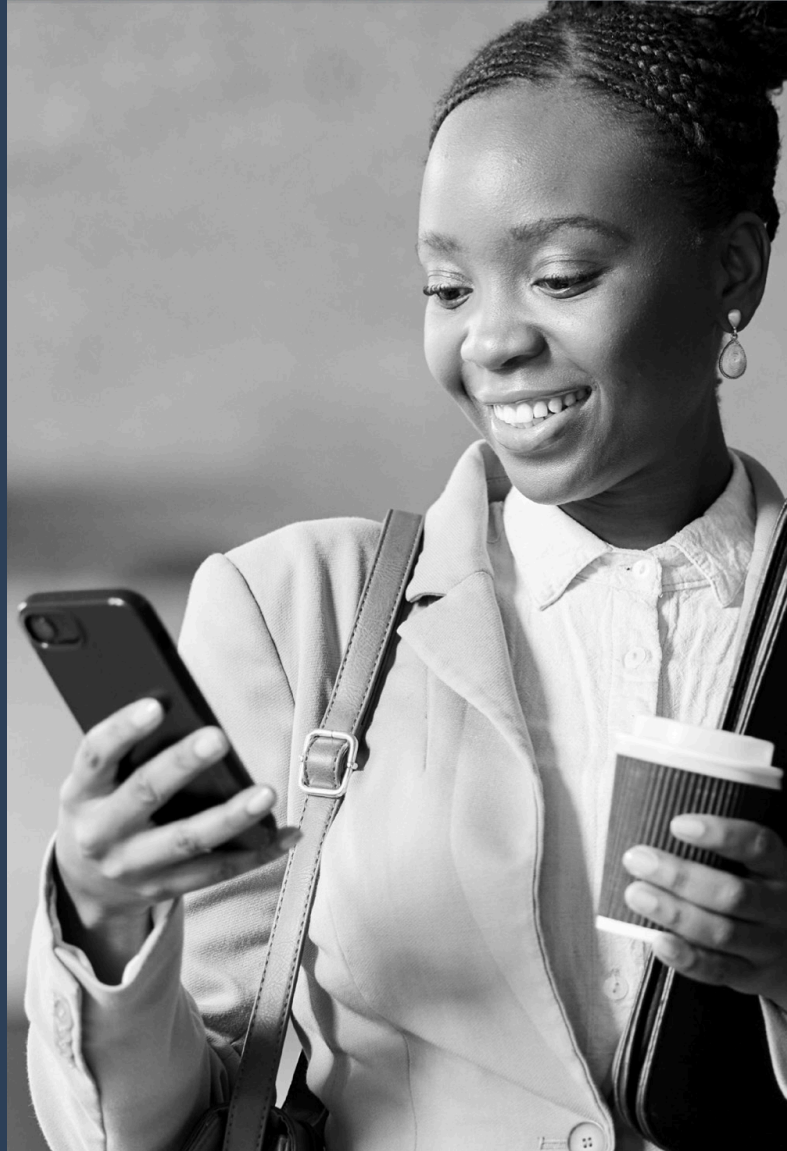
Solution: An identity-based, mobile-first approach

Increasingly concerned about patient care and clinician productivity, Paravate initiated a mobile-first strategy to consolidate and modernize the health system's aging communications environment and streamline workflows. The modernization initiative eliminates disjointed systems and practices, introduces identity-based communications, and adds support for smartphones, tablets, and mobile apps. The new system leverages a number of Imprivata digital identity solutions including Imprivata Identity Governance and Administration for secure role-based user provisioning and application credentialing, Imprivata Enterprise Access Management (formerly OneSign) for seamless single sign-on (SSO), and Imprivata Mobile Access and Control (formerly GroundControl) for managing, securing, and optimizing shared mobile devices.

"We have used Imprivata for identity governance and SSO for our traditional endpoints and applications for years," notes Paravate. "Imprivata Mobile Access and Control lets us easily extend those familiar workflows to shared mobile devices." Imprivata Mobile Access and Control uses digital identity to quickly assign shared devices to trusted individuals. The solution facilitates the secure and seamless exchange of devices between users, protecting data privacy as devices change hands, while providing a personalized device experience for each user.

Results: Superior user experiences and unmatched mobile productivity

The mobile-first initiative helps NGHS automate communications flows, improve collaboration and mobile productivity, and increase user satisfaction. With the new identity-based model, messages and calls are automatically directed to the right device based on role or name. The approach saves time and effort, improving patient care and user satisfaction.

Users are free to use their own mobile devices, or they can take advantage of system-supplied endpoints. Paravate deployed nearly 3,600 shared mobile devices to keep capital equipment expenses in check. Every day, about 5,700 users across the health system utilize a shared mobile device.

"Imprivata helps us break down adoption barriers and make the most of our mobile technology investments," explains Paravate. "Checking out a shared device couldn't be simpler. You just tap your badge, pull a phone, log in, and you're good to go. And with the identity-driven approach, staff members can get in touch with the right person, quickly and easily, which is extremely important in an emergency situation."

– Chris Paravate, Chief Information Officer, Northeast Georgia Health System

Imprivata Mobile Access and Control helped NGHS accelerate the adoption of mobile technology and unlock the full potential of shared mobile devices. Users check out a shared device from a smart USB hub with a simple badge tap for ultimate speed and convenience. Imprivata Mobile Access and Control automatically configures the device to deliver a personalized experience, customized for the user. Clinicians receive a tailored set of applications based on their role and identity. Shared devices are automatically wiped and de-personalized between uses to prevent data leakage, ensure compliance, and mitigate risk.

Asset management reports and status notifications make it easy for Paravate and his team to track shared-device health and usage data, as well as reduce inventory loss. A cloud-based device management service gives the IT operations team deep visibility and tight control over the entire device fleet, from any location at any time, simplifying device support and software maintenance. The Imprivata solution integrates with NGHS's VMware Workspace ONE platform, helping NGHS protect previous investments and extend existing mobile device management practices to shared devices.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

MAC-CS-northeast-georgia-health-system-0124