Building and sustaining a secure virtual care strategy with Imprivata digital identity solutions

Healthcare delivery organizations (HDOs) have rapidly implemented telehealth strategies and remote care options in response to COVID-19. They are developing policies and protocols to incorporate virtual care into their long-term strategies. At the same time, HDOs are also re-thinking the inpatient experience to improve safety for patients, clinicians, staff, and visitors.

Imprivata solutions have helped HDOs across the globe mitigate risk and manage response to the COVID-19 pandemic, as well as the successful implementation of virtual care strategies, by:

- Reducing the risk of spreading infectious disease through contactless workflows
- Enabling a seamless experience for new and remote clinical workflows
- Supporting low-touch, remote implementation and managed services
- Improving security and maintaining compliance by adapting digital identity strategies and solutions

This paper outlines how Imprivata technologies and professional services offerings have been implemented by our HDO customers to support COVID-19 response, as well as to help shape virtual care initiatives that will deliver lasting benefits for patients, clinicians, and support staff.

The emergence of virtual care in COVID-19 response

The COVID-19 pandemic has rapidly accelerated adoption of telehealth and telemedicine to support remote clinician/patient encounters. The initial impetus for telehealth adoption in the setting of the COVID-19 pandemic was for infection control purposes to reduce risk and adhere to social distancing requirements. But there are many additional, longer-term benefits as well. Telehealth is often more convenient for patients, and it can reduce patient re-admissions, emergency department visits, and healthcare insurance costs to employers, among other benefits.

Remote care is likely here to stay, and technology plays a critical role in facilitating the successful long-term adoption of virtual care. However, the scope must be broadened from just patient encounters via video conference to a holistic remote care strategy that integrates all facets of care delivery, both inside and outside the hospital walls.

For example, many HDOs are conducting inpatient rounding via video consults to minimize the risk of clinical staff coming into contact with patients or over-utilizing personal protective equipment (PPE) to make their routine rounds. Similarly, patients are using video conferencing and other tools for virtual visits with their families and loved ones, while maintaining adherence to strict visitation policies.

Outside of the hospital, virtual care requires interaction among care teams who can be widely distributed geographically. This requires more efficient and effective communication and collaboration. Converting in-person clinical workflows to remote often requires an adaptation of technology solutions, processes, and applicable policies.

Imprivata supports these initiatives by delivering purpose-built solutions that enable these new and innovative workflows in a way that is safe, efficient, and secure for all users – including the IT teams being asked to implement them.

Increasing safety by enabling contactless workflows to reduce the risk of spreading disease

Imprivata solutions increase safety for patients, providers, non-clinical staff, and others in a number of different ways, including monitoring for exposure to infectious disease and supporting virtual rounding and patient visitation.

Monitoring for potential exposure to infectious diseases

Healthcare organizations are leveraging Imprivata solutions to monitor for the possible exposure to (and subsequent spreading of) infectious disease in real-time. **Yale New Haven Health** (New Haven, Conn.) uses Imprivata OneSign® login data to identify users who have been in areas of the hospital with a potential risk of infection.

Imprivata OneSign provides the granularity to narrow down which specific users have accessed workstations in different departments, helping Yale identify users who are potentially at risk (for example, those users who accessed a workstation in a specific location of the hospital where a patient with an identified infectious disease may be).

This is accomplished by analyzing the information that Imprivata OneSign collects when users tap their proximity badge to access a workstation. Imprivata OneSign creates a centralized audit record of the user's name, the workstation they accessed, the time and date they accessed the workstation, and how long they used it. By matching this data to the location of the workstation, Yale can determine which specific users were in areas with a high risk of infection, and they can take any necessary actions.

Yale NewHaven Health

Take a closer look

Organizations are also using Imprivata OneSign to streamline access to symptom-free attestation workflows. Many organizations require their clinical staff to demonstrate that they are symptom-free in order to start their shift. Using a survey application, organizations ask questions related to the CDC's COVID-19 symptoms guideline. Imprivata OneSign can be integrated with these applications to enable fast, simple badge-tap access to the survey application. Requiring clinical staff to authenticate to complete the survey also increases compliance and allows organizations to identify, in real-time, any answers indicating that a user could be positive for COVID-19.

Supporting virtual rounding and patient visits

As part of the effort to reduce the risk of spreading infectious disease, many organizations have adopted virtual patient visits as well as virtual in-patient rounding and consults. Imprivata solutions support these initiatives by enabling the rapid, secure deployment and management of iPads and iPhones as well as providing patients and clinicians with fast, secure access to mobile and other devices.

The University of Rochester Medical Center (Rochester, N.Y.), like most organizations, put restrictions in place for hospital visitation in an effort to reduce the risk of spreading infectious disease. To facilitate this change, URMC provides iPads to patients so they can communicate with would-be visitors. These iPads are shared among patients, so URMC needs a way to quickly provision and configure the devices, wipe them clean of personal data between users, and reset the devices back to a "ready state" for the next patient to use. Imprivata Mobile helps URMC manage these devices by digitally sanitizing the devices, reconfiguring the proper tools and applications for patients, and securing them for the next patient's use, all while they are charging.

Take a closer look

Organizations are using similar workflows to support virtual in-patient rounding. This includes using iPads to conduct in-patient consults via video. Cutting down on contact with COVID-19 patients is critical to reducing exposure and flattening the curve. Hospitals are now using iPads to facilitate on-site telehealth sessions, where appropriate, to handle certain interactions with patients kept in isolation. By providing patients with iPads during their stay, clinicians can conduct video check-ins. Imprivata Mobile allows organizations to automatically manage the configuration, and digital sanitization of shared iOS device to ensure patient privacy and HIPAA compliance.

Imprivata solutions are also used to enable virtual consults between in-patient clinical staff and remote physicians. **Cambridge Health Alliance** (Cambridge, Mass.) deployed Microsoft Surface Pro tablets in the ICU that will be shared amongst clinicians to enable virtual consultations with remote physicians and other support staff. To streamline this workflow, Cambridge Health Alliance uses Imprivata OneSign to support fast, secure badge-tap access to the Surface Pro devices and applications. This reduces the need for users to touch the tablet screens to log in, which helps mitigate the risk of contracting infections.

CHA Cambridge Health Alliance

Take a closer look

Enabling secure, efficient clinical workflows outside the hospital walls

The success and sustainability of virtual care depends on the ability to adapt workflows in a secure and efficient way for all users. This requires more efficient and effective communication and collaboration. It also necessitates replicating clinical workflows for a remote setting.

Imprivata solutions help support this transition to remote and distributed care by replicating the same fast, consistent clinical workflow experience that care teams currently experience when they are in the hospital. This includes enabling secure and efficient remote network access, delivering simplified access to clinical workflows via the cloud, and supporting remote enrollment for electronic prescribing for controlled substances (EPCS).

Children's Hospital of the King's Daughters (Norfolk, Va.), like many organizations, experienced a rapid increase in its remote workforce in response to COVID-19. This required the hospital's IT team to quickly deliver remote network access for a greater number of users to allow them to continue to do their jobs effectively. This access still needs to be secure, particularly as hackers are taking advantage of the COVID-19 pandemic through targeted phishing attacks and similar scams. Children's Hospital of the King's Daughters and other organizations are delivering secure remote access with Imprivata Confirm ID®, the enterprise multifactor authentication platform for healthcare.

CHKD Children's Hospital of The King's Daughters

Take a closer look

Imprivata Confirm ID improves security for virtual and remote workflows by enforcing two-factor authentication for access to cloud applications. Using Imprivata ID, Imprivata's convenient phone-based token app, providers and non-clinical staff can quickly but securely access applications anytime, anywhere. This includes both clinical and non-clinical applications such as video conferencing, finance and billing, HR, and others. And, when integrated with Imprivata OneSign Web SSO, access to these applications is simplified further, all while maintaining security.

vmware

Take a closer look

Organizations are also using Imprivata to simplify and streamline clinical workflows in a remote setting. Imprivata integrates with VMware Horizon Cloud Service to deliver single sign-on, EPCS, and other clinical workflows via virtual desktops delivered from the cloud. To better enable work from home as well as from temporary facilities, organizations need an elastic capability to deliver virtual desktops to their remote and distributed users. Through delivery of virtual desktops from the cloud, organizations achieve this capability and can provide desktops at the scale they need for their user base. This gives users fast, secure access to their applications and workflows, allowing them to adapt care to a remote environment.

Remote EPCS is particularly important for enabling end-to-end virtual care – and promoting safety – because it eliminates paper prescriptions and therefore does not require the in-person interaction between patients and providers necessary to pick up a physical prescription.

Imprivata supports anytime, anywhere EPCS by allowing providers to quickly and easily complete the two-factor authentication requirement for EPCS using the same Imprivata ID mobile application used for remote network and application access. With a simple swipe from the lock screen, providers can sign EPCS orders from anywhere. Imprivata also offers Hands Free Authentication and fingerprint biometrics to further improve workflow efficiency and minimize physical interaction with authentication devices.

Imprivata also delivers automated remote identity proofing and provider enrollment for EPCS. The Imprivata Confim ID enrollment utility enables credentialing staff to quickly identity proof providers and enroll their credentials via web conferencing. For organizations requiring individual ID proofing, Imprivata partners with DigiCert, a federally approved Certification Authority, to allow providers to complete the identity proofing process in compliance with DEA requirements.

Supporting IT with remote deployment, enrollment and administration services

Healthcare IT teams have played a crucial role in the industry's response to the COVID-19 pandemic and are now developing strategies and implementation plans to support virtual care. IT is being asked to support these initiatives with limited resources and uncertainty surrounding budgets. Imprivata is helping IT organizations plan for and adapt to these new requirements by delivering solutions to automate workflows and processes that save time and free up IT resources to focus on higher-value activities and projects. Imprivata Professional Services has also fully adapted to be able to implement Imprivata solutions, enroll users, and provide ongoing administration with no on-site requirements.

Imprivata Identity Governance® enables automated user provisioning for appropriate application access. An increase in remote workforce and adoption of virtual care requires users to have different access rights – care team members may shift and expand roles and users may need remote access to applications they didn't previously require. This access must be secure and audited, which is particularly important in a rapidly evolving virtual care environment.

Manual processes for managing this access are cumbersome, time-consuming, and prone to error. Imprivata Identity Governance automates this process while keeping a comprehensive audit trail, allowing organizations to provide faster user access to free up IT resources without compromising security and compliance.

Virtua Health (Marlton, NJ), for instance, leverages Imprivata Identity Governance to supports its ramp up of remote workers, particularly those in non-clinical administrative roles. Specifically, these users need access to Skype – which required provisioning – to communicate and collaborate. Using Imprivata Identity Governance, the Virtua IT team was able to provision access to Skype for about 400 additional users in less than one hour. This process allowed users to immediately start using Skype to complete their remote work while maintaining an audit record of users with access to that application.

Virtua Health

Take a closer look

Imprivata Identity Governance can also be configured to quickly provision access for critical applications that normally would require a manual approval workflow, without losing audit trail. This allows for users to be on-boarded quickly and given access to applications they need to do their jobs on day one. In a remote setting, manual workflows could delay this access and create significant inefficiencies to the virtual care process. Imprivata Identity Governance automates this access, without compromising security or auditing.

And provisioning requirements are not limited to users. HDOs are quickly adopting mobile devices to support virtual workflows, including patient visitation and in-patient consultations, as previously discussed. Devices used in these and other workflows are often corporate-owned and shared amongst staff and/or patients. This places a burden on IT to ensure that these devices are delivered in the proper state to support video conferencing needs, from the initial device provisioning to the re-imaging and resetting of devices between each use.

Imprivata Mobile supports the rollout of shared mobile devices by delivering automated device provisioning, secure device assignment, and fast, secure access for users, helping customers unlock the full potential of shared mobile devices by ensuring a fast, efficient workflow while improving security and auditability. Importantly, Imprivata delivers zero-effort, automated iOS device provisioning to reduce IT burden and device management efforts with rapid scalability. The cloud-based platform gives IT staff remote, extended reach into every location, for device repairs, resets, and updates. This allows IT to quickly enable these devices and workflows in an efficient, low-touch way.

Imprivata Professional Services is also helping to support IT through comprehensive, remote implementation and go-live support, as well as managed services offerings. Leveraging a proprietary implementation methodology, Imprivata helps organizations at all stages of their technology adoption lifecycle. This includes project readiness, education, optimization, and maintenance.

Renown® HEALTH

Take a closer look

Imprivata Professional Services helped **Renown Health** (Reno, Nev.) implement and enroll its providers for EPCS without requiring any in-person or on-site activity. Renown leveraged a new offering from Imprivata through which members of the Imprivata Professional Services team serve as Enrollment Supervisors. The team completed the identity proofing and credential enrollment with Renown's providers remotely, allowing them to quickly enable providers for EPCS with minimal internal resource requirements. This same remote enrollment service is being used by other organizations across the U.S. to enable EPCS to comply with state and federal mandates while adapting to a remote environment.

Imprivata Professional Services is also supporting resource-strapped IT teams through comprehensive managed services offerings. Due to the significant changes being made by many organizations, IT teams have had to rapidly adjust in order to support a remote workforce and virtual workflows. But existing clinical workflows must still be supported, along with all other critical business needs. Imprivata Managed Services helps organizations administer Imprivata solutions remotely, ensuring continued support for existing clinical workflows while freeing up organization IT resources to focus on other critical tasks.

Securing a virtual care environment starts with a comprehensive digital identity strategy

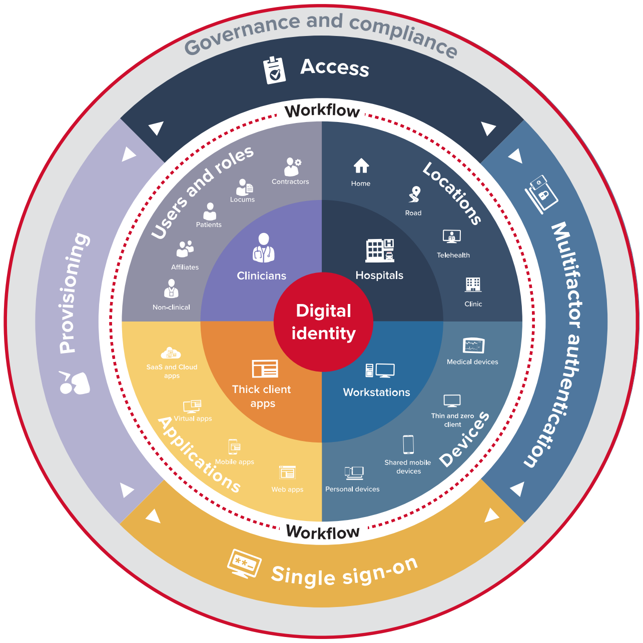
The shift to telehealth was necessary in response to the COVID-19 pandemic and has significantly disrupted what is already a hypercomplex IT environment for HDOs and the care delivery ecosystem.

For example, many organizations experienced an immediate need to ramp up and rotate clinical staff between different roles, departments, and facilities. At the same time, more and more users are being required to work remotely, so they need secure access to their applications and data. The devices from which users need access is changing. Use of mobile devices – both personal and corporate-owned – has increased, and hospital-owned iPads and tablets have been put into use to support telehealth as well as virtual patient visits.

And the number and variety of applications needed for healthcare workers responding to this crisis have also grown in number and complexity. Of course, workers need rapid access in order to do their jobs, but safety, security, and compliance with privacy regulations all remain a significant concern. Beyond the usual EHRs and other common applications, many organizations are developing and deploying new applications to support COVID response, as well as virtual care, all of which need proper access management. And there are certain applications and workflows, such as EPCS, that require a re-thinking of existing processes.

To successfully integrate and scale these and other initiatives as part of a longer-term virtual care strategy, organizations need to implement the same security and compliance foundation they've applied to their in-patient, on-premises infrastructure.

In this new ecosystem, organizations must establish trusted digital identities across a complex network of people, technology, and information.



In this new ecosystem, organizations must establish trusted digital identities across a complex network of people, technology, and information. With focus on trusted digital identity, organizations can implement identity and access management (IAM) solutions to optimize processes and technologies to solve critical workflow, security, and compliance challenges. They can give users secure access to the applications, devices, and information they need, anywhere and anytime they need it.

In healthcare, however, there are unique considerations and challenges that impact IAM deployment and management. For instance, the digital identities (users, devices, applications) that must be managed by an effective IAM program are very different in healthcare than they are in other industries. Healthcare is a highly regulated industry with unique and specific regulatory requirements that must be addressed by IAM. Perhaps most importantly, clinical workflows are unique and complicated, and technology can introduce barriers to care which in turn can impact user experience and workflow efficiency.

Imprivata IAM solutions are purpose-built to meet the unique, demanding, and constantly changing security, compliance, and workflow challenges of the modern healthcare enterprise. Imprivata helps organizations strike the necessary, but often elusive balance between security and clinical workflow efficiency, including in a virtual care environment.

Only Imprivata delivers end-to-end provisioning, seamless multifactor authentication, role-based access, ubiquitous single sign-on, and integrated governance and compliance to secure and manage trusted digital identities across the increasingly complex healthcare ecosystem. Imprivata supports on-premises, cloud, and mobile clinical and business applications, integrations with shared mobile devices and interconnected medical devices, the broadest range of innovative and convenient authentication options, and end-to-end compliance for EPCS and other healthcare regulations.

This ensures all users have secure and seamless access to the applications and information they need, anytime and anywhere they need it, from any device and location. Imprivata IAM solutions help organizations strike the necessary balance between security and clinical workflow efficiency, allowing providers to leverage technology to deliver quality patient care.

About Imprivata

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands