imprivata®

Virtualized Desktops in Healthcare

Accelerating Adoption and Maximizing Value with Automated Access

By David Ting
Founder and CTO
Imprivata

The adoption of virtualized computing environments by healthcare organizations in the U.S. continues to grow. Many hospitals that already use server virtualization in their data centers are moving to the next phase and implementing virtualized desktop infrastructures (VDI) for their clinicians. This whitepaper is for hospital IT leaders who are considering, planning, or already making the transition to VDI.

As hospitals prepare for this transition, there are several key factors that management teams and IT leaders should consider to help ensure that their VDI initiatives are successful. The following are some of the important considerations covered in this paper:

- **Facilitating broad clinical adoption** – VDI deployments are successful only when doctors, nurses, and other clinicians embrace the technology. Virtual clinical desktops can make care delivery far more efficient, but only if clinicians can access these VDI desktops quickly and easily. Automated authentication and application single sign-on technologies remove one of the biggest roadblocks to clinical adoption: repetitive manual logins.
- **Enabling greater mobility for clinicians** – Clinicians are highly mobile and often move between hospital locations, clinics, offices, and elsewhere. Roaming desktops enable this mobility by 'following' clinicians as they move around. Access management solutions can optimize this mobility and increase clinical productivity by maintaining the state of physicians' desktops and applications as they move between locations.
- **Making smooth workflows a priority** – Healthcare workflows often involve multiple hand-offs and cross-department interactions. VDI initiatives must be designed to handle these interactions smoothly and effectively. By including automated access and single sign-on capabilities in your VDI deployment, you can ensure that care providers have quick and easy access to a patient's information as that patient moves through the various steps of a clinical workflow.
- **Reducing IT overhead by lowering costs with thin and zero clients** – IT teams should avoid lengthy deployment schedules, added integration work, and complicated maintenance by selecting components that have been certified to work together by virtualization vendors. Another factor to consider is cost savings and flexibility at the end points. Project teams need to be sure that all components of their VDI deployment can support their end point device strategy. This is especially important with the lower-cost thin and zero client devices that many hospitals are transitioning to.

- **Meeting new authentication needs** – as new user authentication requirements become part of the clinical workflow, such as those mandated by the DEA's Interim Final Ruling for electronic prescribing of controlled substances, thin and zero client selection must accommodate the use of special devices such as fingerprint readers. An equally important consideration is the selection of appropriate authentication management software on the thin/zero client that will allow the hosted EMR or ePrescribing application to properly use the device when it is hosted remotely.

Desktop Virtualization in Healthcare – Gaining Ground

Encouraged by successful virtualization projects in their data centers, many hospitals are now looking to use virtual technology to improve their clinical workflows. By virtualizing clinicians' desktops, hospital IT teams give doctors and nurses an easy way to boost their efficiency and productivity. Other operational benefits include improving workstation and desktop security, and achieving a consistent end user experience. For IT teams, virtualization lowers administrative burdens by providing centralized management and control of desktop environments.

With virtualized desktops, clinicians have faster and more flexible access to patient records and clinical applications that are critically important to healthcare delivery. Virtualized resources enable doctors, nurses, and other clinicians to spend less time dealing with technology and more time interacting with patients. The result is higher quality care delivered more efficiently.

Given these benefits, it is not surprising that virtualization technology in general, and VDI implementations in particular, are rapidly becoming the norm rather than the exception in U.S. hospitals.

This market traction was highlighted in the *Imprivata 2014 Desktop Virtualization Trends in Healthcare Report*: Imprivata's fourth-annual study about desktop virtualization adoption trends in healthcare. The report, based on a survey of 335 U.S. hospitals, showed that the adoption rate of VDI in healthcare has grown by nearly 150 percent in the last three years. This trend is expected to continue, with VDI adoption forecasted to reach 65 percent within the next two years, which represents a 27 percent growth rate from 2014.

These adoption statistics clearly show that the VDI trend has been accelerating over the past few years and that it will continue to do so for the foreseeable future. There are, however, potential issues and roadblocks that hospital IT leaders need to be aware of as they move forward with their organizations' VDI initiatives.

Virtualized resources enable doctors, nurses, and other clinicians to spend less time dealing with technology and more time interacting with patients.

Automated access solutions for VDI can significantly help increase users' productivity and drive faster and wider adoption among clinicians.

Managing the Transition to VDI

When introducing a new technology, there is always a risk that it will get in the way of user productivity rather than enhance it. This is especially true with measures designed to enhance security, as such measures are often viewed negatively, as roadblocks to productivity. With virtual desktop infrastructures, clinicians have little tolerance for the repetitive and time consuming manual logins they are required to perform to gain access through the multiple layers of IT infrastructure often required in VDI environments.

In deploying VDI, hospital IT teams have an opportunity to improve their user experience and clinical workflows while simultaneously providing greater information security. To gain these benefits, however, IT teams need to ensure that clinicians adopt the virtualized versions of their desktops, and embrace the changes they create in their workflows. As they embark on their VDI deployments, IT teams must ensure that their new access and security measures help, rather than hinder, their clinicians' productivity.

These changes, if not handled properly, can impede adoption of a hospital's desktop virtualization project by failing to offer any demonstrable advantages to clinical staff. Some doctors and nurses may view the VDI project as a simple hardware change, going from desktop PCs to thin clients. Automated access solutions for VDI can significantly help increase users' productivity and drive faster and wider adoption among clinicians.

User Access – The Potential Productivity Bottleneck

VDI implementations inevitably change the user experience, delivering a seamless workflow for desktop and application access as users connect from different devices. Virtualized desktops allow users to move throughout their work environment, with their virtual desktops "following" them as they go about their duties. By maintaining users' desktops as they move from one location to another, VDI makes it easier for them to do their jobs.

There are, however, certain challenges associated with virtualized desktop and application access that hospital IT teams need to address. The access point is where IT enforces security controls to ensure that only authorized individuals are able to access sensitive applications. Each additional login or security measure imposes another obstacle between the user and the completion of their tasks.

This is where IT teams confront the age-old trade-off between the need for strong security and smooth information access, and the need for productivity. Security must be maintained, but requiring repetitive, manual logins, logouts, and application restarts is not a winning strategy for clinicians.

Users typically need to take the following steps to get through the security layers within a VDI system in order to use an application:

1. Login to the endpoint, whether a laptop, a workstation, a desktop system, or a thin/zero client in a patient's room or a medical office.
2. Find and start the connection client for the virtualized environment.
3. Authenticate into that client.
4. Select the correct virtual desktop, and wait for confirmation that the desktop is connected.
5. Navigate to the right application.
6. Login to the application by supplying a user ID and password.
7. Logoff the application and the virtual desktop/device when leaving its location.

Roaming users who connect at many different workstations throughout the day must repeat this sequence of steps and logins many times, potentially using different IDs and passwords for each application. Even though the applications within a VDI environment persist as long as the session remains live, many applications can time out due to inactivity, necessitating another login and reconnection.

Each of these steps must occur while the user is trying to stay focused on doing their job. Consider the clinician in a healthcare environment moving from a patient room to a shared workstation and then to a PC in a medical office. Each time they move, they must execute these same steps. In such cases, technology is using up valuable time clinicians could otherwise spend focusing on their patients.

User frustration, unattended and unsecure workstations, weak, shared passwords, and large numbers of password-related calls to the IT helpdesk are the inevitable consequences of such password-heavy systems.

Virtualized desktops allow users to move throughout their work environment, with their virtual desktops "following" them as they go about their duties.

Maximizing the Power of VDI with Automated Access

By using an automated access solution, such as Imprivata OneSign® Virtual Desktop Access, the seven-step process, outlined above, can be streamlined into a few easy actions for users. Imprivata OneSign also offers important API-level automation that is not visible to the end user, but is vitally important, nonetheless:

1. **Authentication** – The user authenticates at different workstations during the day with the single touch of a fingerprint or ID card. OneSign automatically connects the appropriate virtual desktop with the right applications for each user.

Imprivata OneSign is an identity and access management platform that integrates user authentication, user access, password management, and access auditing in one secure, easy-to-manage appliance.

2. **VDI Desktop Access** – API level integration with the leading virtualization vendors provides policy driven automated connections to users' individual desktops and authorized applications after a successful user authentication at an endpoint device.
3. **Application Access** – Once authenticated into their desktop, as users launch applications, their user names and passwords are automatically filled in, providing direct access without the need to remember, or enter, multiple passwords.
4. **Security** – When finished at a workstation, a user can simply tap their badge or touch their fingerprint to a biometric scanner. This touch automatically logs the user off, so they can move on to their next location.

Imprivata Virtual Desktop Access for Streamlined and Secure Access

Imprivata OneSign is an identity and access management platform that integrates user authentication, user access, password management, and access auditing in one secure, easy-to-manage appliance. It simplifies access control with centrally managed authentication and access polices across an entire organization.

Imprivata Virtual Desktop Access leverages OneSign's authentication management and single sign-on capabilities, and integrates with VDI environments such as VMware Horizon View, Citrix XenApp, and Citrix XenDesktop—while extending security throughout clinical workflows. By streamlining and securing user access, Imprivata Virtual Desktop Access:

- Improves users' productivity with virtual desktops and clinical workflows by providing fast, easy, and automated authentication and access management.
- Embeds transparent security throughout the user authentication and access management processes
- Eliminates frustrating and time-consuming manual logins to virtual desktops and applications, letting clinicians spend more time focused on patients and delivering care.
- Minimizes the need to retrain users on authentication and application access in the new VDI environment. API level integration and policy driven automation make the entire process simple for users: users just tap their badges or swipe their fingerprints on a reader.

For clinicians, virtualized desktops combined with the Imprivata OneSign solution means less time wasted on repetitive, manual logins and logouts. It also means that clinical applications and patient information are just a badge-tap or fingerprint-swipe away.

Less time spent wrestling with technology. Less aggravation from password problems and other access issues. More flexible access and greater mobility. More time to focus on treating and interacting with patients. These are some of the ways Imprivata Virtual Desktop Access helps improve and ensure the success of hospitals' VDI initiatives.

How Imprivata Virtual Desktop Access Improves VDI Deployments

Healthcare providers have new and evolving compliance responsibilities in regulatory areas such as computerized physician order entry (CPOE) and Meaningful Use, as well as long-standing HIPAA privacy and security requirements. To comply with this body of regulatory requirements, doctors, nurses, and other clinicians need to digitally capture more information about their interactions with patients than ever before. They must also safeguard this information from unauthorized and inappropriate access.

From a workflow perspective, complying with these regulations means that during each patient interaction, clinicians must complete multiple steps to authenticate themselves and gain access to their systems and applications. Virtualized desktops introduce two additional steps to this process: launching the virtualization client and selecting the user's individual desktop.

This process, repeated multiple times during every shift as clinicians move about healthcare facilities, causes clinicians to waste time. The repetitive logins and logouts are also frustrating for clinicians because they disrupt their workflows and force them, even if only briefly, to focus on technology instead of on their patients.

Imprivata Virtual Desktop Access combined with Imprivata OneSign Authentication Management and Single Sign-On eliminates these repetitive, time-consuming manual steps. Unlike the seven-step process outlined above, the virtual desktop login process with Imprivata solutions is fast, easy, and largely automated.

Imprivata Virtual Desktop Access gives users fast, convenient access to VMware and Citrix published desktops and applications, giving them:

- **Fast, Secure Desktop Roaming:** To access an application via their virtual desktop without Imprivata OneSign, a clinician needs to: login to the end point device, launch and authenticate to the virtualization client, select their individual desktop, and launch and login to the application – and then logout of the application and their desktop. All of this needs to be done manually by keying in user names and passwords. Rather than going through this time-consuming process at each new location, Imprivata OneSign users can simply touch a fingerprint pad or tap their badge on a card reader to call up their desktop and their running applications. This process is so simple that many Imprivata OneSign users have come to refer to it as "Tap and Go". Individual's virtual desktops can also be personalized according to their job function and preferences.

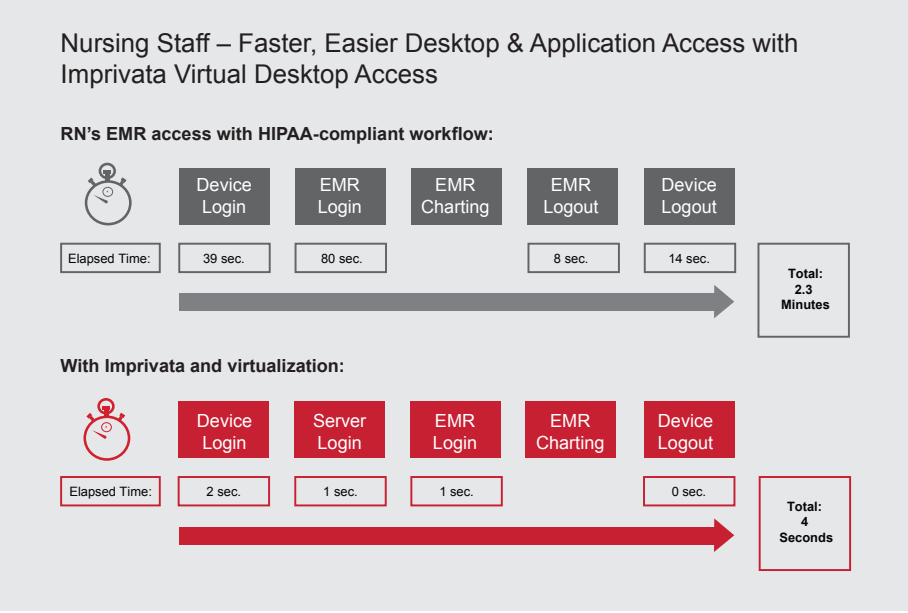
Imprivata Virtual Desktop Access combined with Imprivata OneSign Authentication Management and Single Sign-On eliminates these repetitive, time-consuming manual steps.

It's a fast and easy process, with no typing, and with nothing to remember—or, more importantly—nothing to forget.

- **Single Sign-On:** Enables rapid access to applications without the need to enter usernames and passwords. Launch an application and Imprivata OneSign automatically populates the clinician's username and password and logs them in. It's a fast and easy process, with no typing, and with nothing to remember—or, more importantly—nothing to forget.
- **Workflow Continuity:** In VDI deployments without the benefits of Imprivata OneSign's automated authentication and access management, clinical workflows get disrupted and care providers get frustrated. The disruptions are particularly egregious with critical applications, such as EMR systems, that are known to take a long time to load. With Imprivata OneSign, as users change locations, their desktops 'follow' them, maintaining their states, as appropriate. This eliminates the time-consuming requirement of connecting and disconnecting from various applications from each new location. When a user reconnects to their desktop from a new location, they are automatically reconnected to their previously established desktop session.

With automated access management and application single sign-on, doctors, nurses, and other clinicians can be more productive. That effect is magnified when clinicians are able to instantly access their own virtual desktops and sessions as they move around to different locations within their facility.

To quantify the clinical productivity gains delivered by VDI combined with Imprivata Virtual Desktop Access, Imprivata participated in a time-related study at a mid-sized community hospital. In the study, nursing staff members were observed and timed as they logged into and accessed the hospital's electronic medical records system, both with, and without, Imprivata Virtual Desktop Access.



The results were dramatic. With Imprivata Virtual Desktop Access, the nurses were saving over two minutes every time they logged into their EMR. For some of the nurses, their workflows involved dozens of logins every shift, so the time savings were significant. Other nurses' workflows required fewer logins, so they saved less time. The average time savings across the entire nursing staff was about 20 minutes per nurse, per shift.

With Imprivata Virtual Desktop Access, the nurses were saving over two minutes every time they logged into their EMR.

These results also align with survey results from the Imprivata 2014 Desktop Virtualization Trends in Healthcare Report in which respondents using a single sign-on solution in combination with VDI reported saving 19 minutes per clinician, per shift. These survey results validate the substantial productivity gains that automated access and VDI make possible for clinicians. Giving doctors and nurses fast and secure access to their virtual desktops, to their clinical applications, and to their patients' data saves them time – time that they can spend with patients.

Productivity Gains, Transparent Security, and Lower Hardware Costs

Too often, productivity and security are seen as trade-offs. By adding Imprivata Virtual Desktop Access to your virtual desktop environment, you have the opportunity to improve productivity and security, by transparently layering security throughout the VDI workflow—from session start to logoff.

Session Start: Applying Strong Authentication

The adoption of VDI is a good opportunity to eliminate the security risks associated with the inherent weaknesses of passwords. The fact is that when people have too many passwords to remember, they often forget them. So, they erode security by writing their passwords down, or setting them all to the same easy, obvious string.

The solution to this password problem is two-pronged. First, enable strong authentication beyond just a username and password, and provide single sign-on capabilities so users do not have to remember all their various passwords. Second, manage those credentials for users. With this strategy, knowing a password is not enough to gain access, and users won't need to write passwords down and stick them to their monitors.

When using Imprivata Virtual Desktop Access, it is easy for hospital IT teams to add strong authentication factors to their organizations' virtual desktop login and application sign-on routines. Imprivata OneSign enables a wide variety of authentication technologies, so IT teams can choose the method that works best for their users, their IT environments, and their organizations. For example, many notebooks have built in fingerprint devices - adding a biometric factor to the login on such devices ensures that an individual user is the only person who can successfully access their unique desktop.

Combining strong authentication with single sign-on offers convenience and productivity gains, as well as protection from phishing, password theft, and other unauthorized access.

Proximity cards are pervasive in healthcare delivery organizations, and can easily be added to authentication processes, enabling the hallmark Imprivata "Tap and Go" approach to authentication and application access. Workstations equipped with card readers allow users to quickly login with a quick tap of their ID badge, and perhaps an additional PIN entry. Imprivata OneSign also supports smartcards, one-time password tokens, and other methods.

Once users perform their initial authentication, repeated reconnections during their work shifts only require them to tap their proximity card, or swipe their fingerprint. There is need for them to enter additional data.

Combining strong authentication with single sign-on offers convenience and productivity gains, as well as protection from phishing, password theft, and other unauthorized access. Together with a complete audit trail of virtual desktop access, Imprivata OneSign helps to ensure that essential data and applications in a hospital's virtualized IT environment are well protected from misuse and unauthorized access.

Application Launch: Audit and Control

When deploying the VDI desktop, apply the principle of least privilege; only put those applications appropriate for each user, and their role, onto their desktop. This reduces the possibility of unauthorized access and eliminates clutter on users' desktops, which no longer needs to be filled with applications that are not appropriate to their roles.

Maintaining a secure audit log of application access gives hospital IT, compliance, and management teams constant visibility into who is accessing which applications, when, and from where. Combining strong access controls with constant audit and visibility is key to protecting applications and data from unauthorized access and misuse.

Transaction-level Authentication

Hospitals can require that users re-authenticate when they perform particularly sensitive transactions, such as writing prescriptions. Hospitals can avoid clinical workflow disruptions caused by re-authentication requirements by adding automated authentication and access management capabilities. That automation still gives the hospital the ability to challenge users to complete a re-authentication process—with all the security advantages that entails—without frustrating care providers with excessive disruption of their workflows. In addition, although requirements vary by state and are still evolving, many hospitals are preparing for the eventual introduction of Electronic Prescription of Controlled Substances (EPCS). Enabling stronger, transaction-level authentication helps hospitals to lay the technical groundwork required for EPCS by state and federal regulators.

Industry-leading Zero and Thin Client support
With their smaller footprints, thin and zero client devices let hospitals make better use of the space in their patient care areas. They also lower hospitals' power consumption costs, support costs, and IT management requirements. For these reasons, adoption of these devices by hospitals and other healthcare delivery organizations is growing rapidly.

Imprivata Virtual Desktop Access offers industry-leading support for zero and thin client devices, giving customers flexibility with their end-point device strategies. It is the only solution available today that enables true strong authentication and optimized policy driven workflow on zero client devices. In addition, Imprivata Virtual Desktop Access is the only solution available today that is embedded directly in the firmware of zero client devices from leading suppliers including Dell Wyse, HP, Igel, Teradici, N Computing, and others.

Imprivata Virtual Desktop Access offers industry-leading support for zero and thin client devices, giving customers flexibility with their end-point device strategies.

Partnerships for a Strong VDI Ecosystem
Imprivata has long-standing and productive technology partnerships with the two leading providers of virtualized computing environments: Citrix and VMware. With years of technical collaboration with those organizations, Imprivata has achieved API-level integration of authentication management and single sign-on functionality with VMware Horizon View, and with Citrix XenApp and XenDesktop. In addition, with VMware Horizon View, Imprivata OneSign is included in the reference architecture for VMware's AlwaysOn Point of Care solution for the healthcare industry, which is essentially a blueprint for a successful healthcare deployment. With Citrix, Imprivata OneSign has been certified as 'Citrix Ready', a designation that confirms that Imprivata OneSign works well 'out-of-the-box' with the Citrix virtualization solutions.

The strength and depth of Imprivata's partnerships promise safe and effective integration for hospital IT teams, with minimal deployment risks. And, in case issues do arise, Imprivata provides its customers with direct access to technical experts who are highly experienced with virtualization and automated access technologies in healthcare workflows.

Conclusion: Ensuring the Success of VDI Initiatives and Driving Measurable Benefits
Imprivata OneSign authentication and access management solutions are the perfect complements to a hospital's VDI deployment. By using advanced authentication and single sign-on capabilities, Imprivata OneSign solutions let care providers eliminate repetitive, manual logins from their workflows. Faster and easier access to the resources and information that clinicians need to do their jobs lets them save time – time they can spend focusing on patients instead of dealing with technology.

imprivata®

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata's single sign-on, authentication management and secure communications solutions enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care.

Over 2 million care providers in more than 1,000 healthcare organizations worldwide rely on Imprivata solutions. Imprivata is the category leader in the 2012 and 2013 Best in KLAS Software & Services Report for SSO, and SSO market share leader according to HIMSS Analytics.

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

Offices in:
Lexington, MA USA
Santa Cruz, CA USA
Uxbridge, UK
Paris, France
Nuremberg, Germany
Den Haag, Netherlands

These time savings translate into substantial benefits for patients, hospitals, and clinicians. Imprivata solutions enable care providers to spend more of their time focusing on patients, and less time dealing with technology. More time for patient interactions drives increases in clinical productivity and improvements in the efficiency of care delivery. These time savings and efficiency gains can positively impact a range of key performance indicators, including patient satisfaction scores, job satisfaction and retention rates among physicians and nurses, shortened patient stays, increases in the numbers of patients seen, and improvements to bed utilization rates.

In short, Imprivata's solutions, when implemented in conjunction with a Citrix- or VMware-based VDI initiative, can create real, 'hard dollar' benefits that directly impact a hospital's bottom line.

Virtual clinical desktops are powerful new tools for healthcare professionals. But to truly leverage all the potential power of roaming desktops in patient care, hospitals and care providers need authentication and access management technologies that can keep up. That's precisely what Imprivata brings to VDI projects.

Imprivata OneSign and VDI is a powerful combination that is already deployed and working at hundreds of hospitals nationwide. Your organization can do the same with its VDI initiative. Don't wait and watch your virtual desktop efforts being met with lukewarm adoption. Take a look at Imprivata's offerings and the success its customers have had with their VDI projects. There is no reason why your organization can't drive the same significant and positive results.

Contact Us

Imprivata OneSign solutions can help you ensure that your organization's transition to virtual clinical desktops is successful. Take the first step toward more efficient and secure care delivery, and contact us today at +1 781 674-2700, or visit us online at www.imprivata.com.