Enabling Fast and Secure Clinician Workflows with One-Touch Desktop Roaming

WHITE PAPER

vmware® imprivata®

Table of Contents

Introduction

The Challenge Facing CMOs, CIOs and Clinicians

The move from paper-based medical records systems to electronic medical records (EMR) is rightly viewed as a step towards improving patient outcomes, increasing clinician productivity, and lowering costs. The transition, however, is often hampered by the challenge of providing secure access to patient information, particularly given the increased focus on regulatory compliance. From an IT perspective, the mandate is clear: access to patient information must be not only secure but also fast, convenient and reliable. Technologies that provide security but frustrate clinicians—either by slowing them down or adding steps to their everyday tasks—will slow adoption of EMR to a crawl.

Likewise, because clinicians are responsible for any changes to medical records made in their name, they will resist adoption unless safeguards are in place to ensure that every EMR change attributed to them was actually made by them. In the U.S., slow adoption can ultimately disqualify a hospital from receiving stimulus funding under the "meaningful use" guidelines of the HITECH act. Erecting obstacles for clinicians, even in the name of security, is inadvisable when the costs of recruiting and retaining clinical employees can run in the hundreds of thousands of dollars. This white paper explains how organizations can bridge the gap between clinician productivity and security, solving the "last mile" problem for clinicians by providing seamless, efficient, and secure access to electronic patient record data across multiple clients, where and when the clinician requests it.

Many organizations end up deploying a broad set of applications on every desktop, to meet the needs of any clinician or hospital staff member who might use it. The resulting environment—full of desktops with dozens of HIS applications from multiple vendors needed to access all kinds of data—is difficult, if not impossible, to secure. Clinicians must remember multiple passwords to access patient information that is spread across several applications. Moreover, the cost and complexity of maintaining many applications on numerous workstations has sparked a movement away from the traditional PC desktop to a thin client approach supported by a virtual desktop infrastructure (VDI).

Desktop virtualization offers several immediate advantages:

- Central management and administration of user desktop environments
- High availability for desktops and applications
- Significantly lower desktop operating costs
- Secure management of patient data on secure servers instead of vulnerable endpoints
- Easier access to patient data from many places (hospital, office, clinic, or at home) and from many devices (workstations, laptops, tablets, cart PCs, PDAs, etc.)

In a clinical setting, however, there are still several issues to be addressed even when deploying a virtual desktop infrastructure. Hospital workstations have been compared to hummingbird feeders, with clinicians moving in for a minute or two before moving on and allowing the next clinician to use the station. There are several security implications for such shared workstations. First, clinicians must be vigilant in ensuring they are entering data for their patients (and not the last clinician's patients) to minimize data entry errors. Similarly, to comply with privacy guidelines, open records cannot be left unattended. In addition, clinicians must remember multiple passwords to access individual applications made available via the virtual desktop—a task made more difficult by IT security practices that require different passwords with random character sequences for each system. None of this, of course, improves clinician productivity or patient outcomes.

From the perspective of a roaming physician, nurse, or other clinician in a hospital setting, location awareness is a key requirement for virtualized desktops. As clinicians move from floor to floor or from their office to a patient's room, their location is tied closely to the applications and patient data that are most relevant to the tasks at hand. A desktop in the office, for example, will likely have email software open and ready for use, while a desktop accessed in a patient's room would not. Similarly, a patient list for the fifth floor is no longer relevant when the clinician has moved to the third floor. Likewise, doctors in the operating room have different privileges than those they have on the exam floor. This need for location awareness extends to printers and other physical resources, as well. When a clinician prints from a virtual desktop, the document must be printed nearby; otherwise it represents both a productivity drain and a privacy risk.

Compliance and privacy, of course, are always fundamental concerns in a healthcare setting. From a workflow perspective, shared desktops must be automatically secured when clinicians move on to another area—especially if they are called away to handle an emergency situation and neglect to sign off. Government regulations increasingly require physicians to re-authenticate using something other than a password (such as a fingerprint scan) when prescribing medication, particularly for controlled substances. Further, ensuring patient data privacy has become mandatory, and enforcement of privacy regulations has been highly publicized across North America and Europe.

It is clear that enabling desktop roaming with virtualization in a clinical environment comes with a unique set of requirements and constraints. These include the ability to use multiple authentication mechanisms, manage passwords for access to clinical applications, integrate authentication seamlessly into workflows, provide session control to disconnect and reconnect intelligently as the clinician moves from one workstation to another, and use location awareness to increase efficiency and mitigate privacy risks. When these requirements are met, the benefits of desktop virtualization can be fully realized in clinical environments.

Enabling a Follow-Me Desktop for Roaming Clinicians

Imprivata OneSign simplifies and secures clinician access to desktops, networks, and applications. With Imprivata OneSign, doctors and nurses can navigate seamlessly across healthcare applications, accessing critical patient information in support of their workflows regardless of their location. By enabling fast, reliable access to EMR, Imprivata OneSign reduces clinician frustration and increases the likelihood of a successful transition to EMR technology.

One-Touch Clinician Roaming

Imprivata solutions are designed for healthcare workflows in which workstations are shared and clinicians move from workstation to workstation throughout the day. The desktop follows the clinician to any workstation and is immediately restored to its previous state, eliminating the need to restart each clinical application and streamlining access to patient data.

Automatic Desktop Lock

With OneSign Secure Walk-Away, clinicians are automatically logged off when they walk away from the workstation, and can easily re-authenticate when they return. This reduces cross-charting, data entry errors, and risks associated with exposing unattended records.

Transaction-Based Authentication

OneSign ProveID allows an application to leverage strong authentication services to positively identify a user at any point in the transactional workflow. For example, it can enforce the positive identification of a user prior to drug disbursement or when writing a prescription for a controlled substance.

Location Awareness

Just as importantly, Imprivata OneSign is fully location-aware, so when a clinician reconnects from a different workstation, the new location information is propagated to the virtual desktop and running applications. Patient lists, available applications, desktop and application appearance, default printer, and user privileges are configured dynamically based on the particular workstation they are using.

Deploy Transparent Security

Without security, easy access to patient data is a liability, not strength. Imprivata OneSign provides transparent security by integrating strong authentication, session management, application single sign-on, user provisioning, event reporting, and context management to clinical workflows. Strong authentication options include built-in support for biometrics, smart cards, active and passive proximity cards, and many National Health and government ID cards. Clinicians can log in at the start of their shifts with their proximity badge or fingerprint and a password, and then use convenient, secure one-touch logins for the remainder of their workday. Coupled with fast user switching, these capabilities streamline clinical workflows by balancing the clinicians' demands for convenience and usability with the organization's need for security and compliance.

A Clinical Workflow with Imprivata OneSign

Consider the typical clinician workflow illustrated in Figure 1. When the doctor taps her proximity card or swipes her finger to logon to the first workstation, Imprivata OneSign authenticates her. She launches any applications she may need for patient care, and Imprivata OneSign automatically signs her in to those applications. When she's finished, she simply taps her card again to lock the

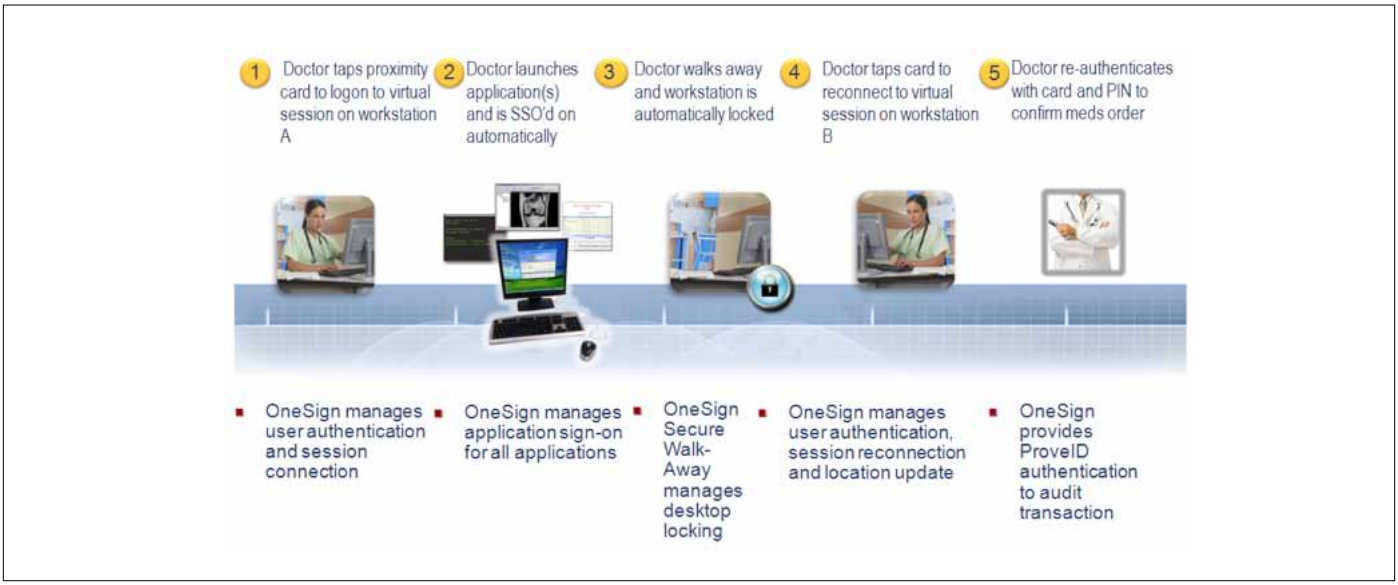

Figure 1: A typical clinician workflow with OneSign

workstation. If she forgets, Imprivata OneSign will automatically sign her out when she logs in elsewhere, or (with OneSign Secure Walk-Away) as soon as she leaves the workstation. After moving to another location, she taps her badge again to logon to another workstation. Imprivata OneSign immediately brings up her previous desktop, with all her applications active and in the same state she left them. It also detects her new location and updates her workstation configuration accordingly. Finally, when she orders medication, Imprivata OneSign re-authenticates her in compliance with hospital policy and regulatory mandates. Throughout the workflow, Imprivata technology enforces security while helping to improve patient outcomes by accelerating access to EMR applications and data, reducing errors, and eliminating redundant work.

VMware View and Imprivata OneSign: Complementary Technologies

Underpinning the ability to deliver a virtual desktop that can be accessed from a wide variety of client devices including thin clients, existing PCs or mobile clients is the VMware View™ virtual desktop infrastructure. VMware View is the industry's first purpose-built solution for delivering desktops as a managed service. By simplifying and automating desktop management, VMWare View can reduce the total cost of desktop ownership by 50 percent while providing end users with a consistent, high-performance desktop experience. Virtualization decouples desktop environments from the underlying PC hardware, and applications from the underlying operating system enabling desktop operating systems, applications, and data to be managed independently of each other in the datacenter. The ability to support a fully isolated virtual desktop complete with its own operating system for each user simplifies the deployment of enterprise applications that are often hindered by resource or naming conflicts when used in a multi-user environment. VMWare View uses PC over IP (PCoIP), a high-performance display protocol designed to provide a reliable, optimized desktop experience for the clinicians a wide variety of client devices with USB capabilities that match directly-connected PCs.

Imprivata OneSign complements VMware View by adding the capabilities needed to enable secure roaming for clinical workflows, including strong authentication, single sign-on, session management, and location-aware desktop personalization and customization.

Conclusion

Together, Imprivata OneSign and VMWare View solve the "last mile" problem for clinicians by providing seamless, efficient, and secure access to electronic patient record data across multiple clients, where and when the clinician requests it.

Complementing the reliable, cost-saving, and easy-to-manage virtual desktop infrastructure provided by VMware View, Imprivata solutions are specifically designed to improve patient outcomes by streamlining common healthcare workflows. Imprivata OneSign enables fast access to applications, EMR, and other data, while providing the security needed to protect patient

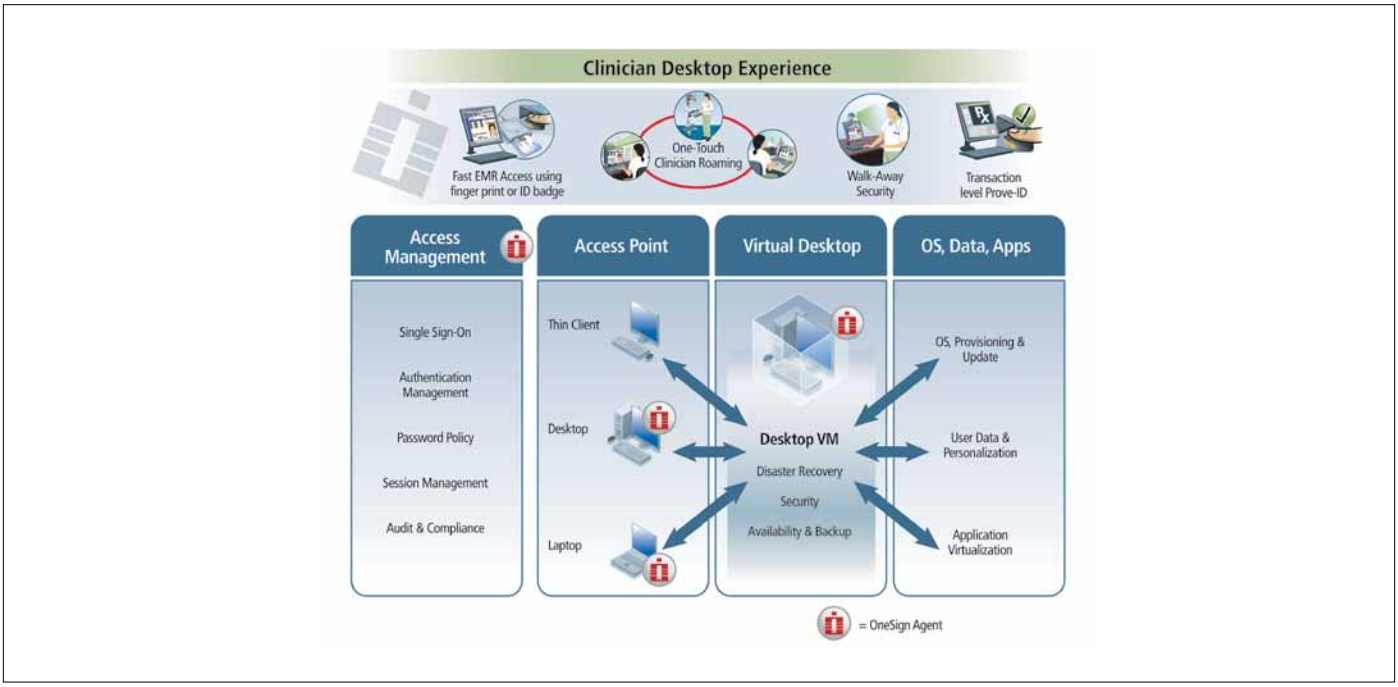

Figure 2: The integrated Imprivata OneSign and VMware View solution

data and simplify regulatory compliance. By capturing all access events, including who accessed what, when, and from where, Imprivata OneSign simplifies audit and compliance reporting.

Imprivata has been serving the healthcare sector for nearly a decade. In that time, Imprivata has developed strong relationships with more than 550 hospitals and built a user base of more than one million licensed healthcare users worldwide.

Rather than simplifying one group's workload at the expense of overburdening another group, Imprivata solutions are designed to support *all stakeholders* throughout the healthcare organization. Because the Imprivata OneSign platform is delivered in a secure, self-contained appliance that is non-invasive to existing IT infrastructures, involves no changes to user directories or applications, and requires no additional staffing or specialized management skills, *IT operations groups* benefit from rapid, easy deployment and lowered ongoing support costs. CMOs see significant improvements in vital healthcare workflows and a smoother transition to EMR-based systems. *CIOs and CTOs* are better able to enforce patient privacy policies and ensure compliance. Lastly (and perhaps most importantly) *physicians, nurses, and other clinicians* are empowered to deliver better patient outcomes through faster EMR access.

To learn more about Imprivata OneSign, visit www.imprivata.com, e-mail sales@imprivata.com or call 1-877-ONESIGN (1-781-674-2700).

To learn more about VMWare View, visit www.vmware.com/products/view

To learn more about VMware solutions for healthcare, visit: http://www.vmware.com/solutions/industry/healthcare/

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com