



# 3 Steps to Faster EMR Adoption with Desktop Virtualization and SSO

Virtual Desktops Deliver Tangible Benefits in Hospitals

WHITE PAPER

**Table of Contents**

STEP 1:  
DEPLOY DESKTOP VIRTUALIZATION ON THE HOSPITAL FLOOR ..... 3

STEP 2:  
ACCELERATE EMR ADOPTION WITH DESKTOP VIRTUALIZATION  
AND NO CLICK ACCESS™ TO VIRTUAL DESKTOPS ..... 3

STEP 3:  
NEVER LEAVE PATIENT DATA UNATTENDED—SECURE THE UNATTENDED  
DESKTOP ..... 5

CASE STUDY:  
MEMORIAL HOSPITAL AND ONE-TOUCH DESKTOP ROAMING ..... 6

SUMMARY ..... 6

ABOUT IMPRIVATA ..... 7

The Meaningful Use objectives in the HITECH Act are creating new urgency for hospitals to implement [Electronic Health Records \(EHRs\)](#) and Computerized Physician Order Entry (CPOE). As hospitals deploy new applications, they must take steps to protect both the clinician experience and patient data, while controlling costs. Without physician adoption, Meaningful Use objectives cannot be met. This whitepaper highlights three steps hospitals can take to accelerate EMR adoption and achieve Meaningful Use using VMware View and Imprivata OneSign:

1. Deploy desktop virtualization throughout the hospital floor using VMware View™
2. Deploy single sign-on to the hospitals virtualized environment—providing No Click Access™ to virtual desktops
3. Secure unattended patient data on workstations using OneSign Secure Walk-Away®

### STEP 1: DEPLOY DESKTOP VIRTUALIZATION ON THE HOSPITAL FLOOR

Despite the obvious benefits that EMRs can deliver, any new technology faces serious hurdles in healthcare organizations:

Clinicians must be willing to embrace and use the new technology. It must make their jobs easier and more efficient, rather than harder

- Technology should ultimately drive down the cost of delivering high quality care by saving clinicians and the IT department time
- IT teams must be able to demonstrate HIPAA compliance and maintain the security of patient data when it is stored electronically on workstations, in patient rooms or in public areas

Desktop virtualization solutions like VMware View can solve any of these challenges. Using desktop virtualization, hospitals can provide thin clients that access a 'virtual' PC actually running on a server in a data center.

Desktop virtualization has many benefits that are particularly powerful in the healthcare environment:

- For physicians, nurses, and other clinicians, desktop virtualization can improve productivity and satisfaction by providing a personalized desktop experience. Rather than having a desktop session resident on a specific physical computer, it can follow them throughout their day as they move between rooms and workstations. And because the desktop itself is hosted in the virtualization environment in the data center, physicians can use mobile devices like iPads or iPhones to access applications.
- For IT staff, using desktop virtualization reduces the tasks of maintaining and supporting PCs throughout the hospital. IT can install, maintain, back up and manage all software and data

within the data center. The actual devices in patient rooms and nursing workstations can be thin, browser-based clients that are less expensive to deploy and maintain. With centralized control of applications and data in a virtual environment, IT can deliver better service levels (availability and performance) to clinicians.

- From the security and compliance perspective, the patient data itself remains in the data center, rather than being distributed throughout the hospital. Data is kept securely in a centralized datacenter simplifying HIPAA compliance.

Virtualization alone is not enough. To achieve Meaningful Use objectives and have clinicians adopt new technology, hospitals need to protect the clinician workflow as well as the patient data.

How do you make desktop virtualization solutions more attractive for clinicians? You focus on what the clinician needs to be effective, productive, and responsive to patient needs.

### STEP 2: ACCELERATE EMR ADOPTION WITH DESKTOP VIRTUALIZATION AND NO CLICK ACCESS™ TO VIRTUAL DESKTOPS

The one consistent "lesson learned" from hospitals deploying EHR is that you must have physician acceptance of the technology. The best software in the world won't solve problems if it isn't accepted and used, and 'shelfware' isn't enough to meet Meaningful Use guidelines.

How do you make desktop virtualization more attractive for clinicians? You focus on what the clinician needs to be effective, productive, and responsive to patient needs.

The first and most important step is making it easy for clinicians to access their applications quickly and securely. This requires solving the 'authentication' problem: how do clinicians log in not only to the virtual desktop, but also to all of the applications on that virtual desktop? Because physicians and nurses are constantly changing locations and re-connecting with their virtual desktops, solving this problem is a high priority if you want widespread adoption.

Imprivata OneSign has worked in partnership with VMware to solve this problem by adding single sign-on and strong authentication to the VMware virtual environment.

Imprivata and VMware have collaborated to fully integrate Imprivata OneSign with VMware View™. [OneSign Virtual Desktop Access™](#) ensures that hospitals can implement a virtual desktop environment using VMware View, and gain flexible strong authentication, single sign-on, and comprehensive audit and reporting for application access and roaming desktops.

### Strong authentication options

Imprivata OneSign supports many flexible authentication options, including:

- Passive proximity cards
- Active proximity cards
- Smart cards
- [Fingerprint biometrics](#)
- One-time password tokens

Often, different methods are appropriate for different environments and groups of clinicians within the hospital. For example, a hospital might use fingerprint readers in areas during medication order signing, but use ID badges in areas where gloves are required. Using Imprivata OneSign, hospitals can design the access policies they need. OneSign will then automatically enforce and audit those access policies.

### CPOE

Meaningful Use guidelines require electronic prescription capabilities. Physicians that are writing an e-prescription or order medications may need to re-authenticate, to ensure that the licensed physician is the person actually making the order.

Using Imprivata OneSign, hospitals can integrate these re-authentication processes with their one-touch authentication. For example, a physician writing an e-prescription simply touches a badge to a reader to electronically 'sign' the order.

The login process is also essential to security and compliance. While it must be fast and convenient for authorized users, it should be impossible for those who are not authorized to get to applications. Hospitals must secure logins with something beyond simple passwords, reduce or eliminate 'shared' logins, and enforce password and authentication policies automatically.

Using OneSign with VMware View, a hospital can define flexible application and desktop access policies, using authentication technologies such as fingerprint readers or proximity card readers that make the most sense for their environment. A common situation is like the following:

1. The first time a physician logs on in a day, they enter a username/password and touch their badge to a reader.
2. The physician selects the application(s) they want to use on the desktop; OneSign automatically authenticates them with each application, without additional logins or typing.
3. The physician then proceeds to a patient room; by simply touching an ID badge to the reader they reconnect to the desktop session already started and bring up the patient record.
4. As soon as the physician leaves the workstation, even without logging off, the workstation locks down until the physician either reappears or a new person authenticates by touching their badge. (See the [OneSign Secure Walk-Away](#)® description below.)

The tight integration of OneSign with the VMware environment means that the connection between the single touch authentication and the virtual desktop is seamless. Physicians find immediate benefit in the time and frustration saved by not having to constantly type in user names and passwords for every application. Watch ["Improving Clinician Workflows with One-Touch Roaming"](#) Video.

### Using OneSign with VMware View

1. The first time a physician logs on in a day, they enter a username/password and touch their badge to a reader. (The two authentication factors make it very difficult for someone to pretend to be the physician.)



2. The physician selects the application(s) they want to use on the desktop; OneSign automatically authenticates them with each application, without additional logins or typing.



4. As soon as the physician leaves the workstation, even without logging off, the workstation locks down until the physician either reappears or a new person authenticates by touching their badge. (See the [OneSign Secure Walk-away](#) description below.)



3. The physician then proceeds to a patient room; by simply touching an ID badge to the reader they reconnect to the desktop session already started and bring up the patient record.



### STEP 3: NEVER LEAVE PATIENT DATA UNATTENDED— SECURE THE UNATTENDED DESKTOP

Hospitals are unpredictable places. It's unrealistic to expect clinicians to always log off of their workstations and, when a patient is in crisis, there's no time to think of logging off. In some cases, clinicians may just leave a room for a few moments to retrieve something or confer with a colleague. In those moments, the patient record is unattended and vulnerable to anyone passing by.

Leaving patient data unattended can have serious consequences, including:

- Medical Errors—corrupted patient records and compromised patient safety—when a clinician at a shared workstation does not realize that someone else's session is open and enters data into the wrong patient record
- HIPAA non-compliance—when a clinician leaves an open patient record in a hospital room with visitors or others present

Hospitals have searched for ways to lock down unattended workstations. There are many “partial” technological solutions, from creating a simple ‘hot key’ for logging off to automatically locking down after a specific period of inactivity. But most of these solutions, even implemented together, are ineffective, causing clinician frustration.

Advances in facial recognition technology provide hospitals a new option for a completely automated workstation lockdown. Imprivata OneSign Secure Walk-Away uses facial recognition software to create facial patterns that temporarily identify the clinician who has authenticated at the workstation.

When the clinician steps away, the workstation locks. When someone steps in front of the workstation again, OneSign Secure Walk-Away examines the facial pattern. If it matches the person currently authorized at the workstation, OneSign unlocks the workstation. If someone different is standing at the keyboard, then the new person will need to authenticate on the workstation and bring up their own virtual desktop. This creative use of facial recognition technology won the Security Innovation of the Year award from the British Computer Society's UK IT Industry Awards.

There are several important factors to note:

- OneSign Secure Walk-Away does not actually authenticate the user - it merely confirms that the person reappearing in front of the workstation is the same one who just authenticated at the workstation. As a result, it does not store facial data permanently, can handle daily changes in appearance, and does not require any special process for provisioning users.
- The workstation lockdown is completely automated. The clinician does not need to take any special steps to log off, or re-authenticate after having stepped away.
- It works if the clinician is wearing a cap or mask.

The following table compares different methods for locking down unattended workstations.

Methods for Securing Unattended Desktops

METHOD	ADVANTAGES	DISADVANTAGES
<b>Hot key logoff</b>	<ul style="list-style-type: none"> <li>• Quick, easy</li> </ul>	<ul style="list-style-type: none"> <li>• Clinician must remember to press the hotkey upon leaving</li> </ul>
<b>Unattended timeout</b>	<ul style="list-style-type: none"> <li>• Automated, does not require clinician action</li> <li>• Clinician can return before timeout period takes effect.</li> </ul>	<ul style="list-style-type: none"> <li>• Clinician must remember to press the hotkey upon leaving</li> <li>• Workstation is accessible before timeout</li> <li>• An unauthorized user can interrupt the timeout by pressing a key</li> </ul>
<b>Active proximity badges (with batteries)</b>	<ul style="list-style-type: none"> <li>• Automated, does not require clinician action</li> </ul>	<ul style="list-style-type: none"> <li>• Provisioning and maintaining the badges adds cost</li> <li>• Radio interference is possible in some situations</li> </ul>
<b>Passive proximity badges</b>	<ul style="list-style-type: none"> <li>• Logout with a single touch of the card to a reader</li> </ul>	<ul style="list-style-type: none"> <li>• Clinician must remember to logout</li> </ul>
<b>Facial recognition (OneSign Secure Walk-Away)</b>	<ul style="list-style-type: none"> <li>• Completely automated</li> <li>• Workstation is unlocked immediately when clinician returns - without user intervention</li> <li>• Workstation protected as soon as the clinician walks away, without a timeout</li> </ul>	

### CASE STUDY: MEMORIAL HOSPITAL AND ONE-TOUCH DESKTOP ROAMING

Memorial Healthcare in Owosso, Michigan is a compelling example of a hospital that is using one-touch roaming desktops and walk-away security to enhance patient-centered care while meeting privacy and security objectives.

Memorial Healthcare has been voted one of top 100 “Most Wired Hospitals” by Hospital and Health Networks. As a Planetree hospital, it embraces a patient-centered model of care. Says Frank Fear, VP of Information Services for the hospital, “We want to be a national model for excellence in personalized healthcare. We consider this objective with every new initiative.”

Memorial Healthcare has used Imprivata OneSign for single sign-on and strong authentication since 2006. In 2010, the hospital started implementing a patient-centric obstetrics unit, with Computerized Physician Order Entry (CPOE) and Electronic Physician Documentation applications, an entertainment & information system for patients, and secure one-touch roaming for clinicians.

As part of the new roll-out, Memorial Healthcare is using VMware View virtual desktops with Imprivata OneSign Virtual Desktop Access™, for No Click Access to roaming desktops. Virtual desktops follow each user during the course of their shifts, and are removed from memory when the shift is over.

The new environment includes:

- Strong, multi-factor authentication: The first time a clinician logs in during their shift, they use a password in addition to tapping their existing ID badge, which is a passive proximity card. From then on, clinicians simply tap the reader with their card for No Click Authentication.
- Secure unattended desktops: OneSign Secure Walk-Away® uses facial recognition technology to automatically lock down the workstation when the authorized user is not present, without requiring an explicit logout.

#### Cameras in patient rooms

If cameras are not already part of the patient care environment, hospitals may be concerned about putting cameras in patient rooms.

OneSign Secure Walk-Away uses cameras that are either built-in or added to the workstation. OneSign Secure Walk-Away does not create or store any images. Instead, it uses facial recognition software to create in essence a ‘facial fingerprint’ that it stores in memory only for the duration of the authorized session.

---

*“Using Imprivata OneSign and VMware View, our clinicians can access patient records quickly and securely with the tap of a card, so they can focus on delivering highly personalized patient care. And with OneSign Secure Walk-Away always watching over the shared workstations, we don’t have to worry about patient data being left unattended on shared workstations.”*

– Frank Fear, VP of Information Services,  
Memorial Healthcare

---

### SUMMARY

As healthcare organizations struggle to meet Meaningful Use objectives and leverage technology in the healthcare environment, they face several hurdles including: the cost and implementation effort for new EHR and CPOE applications, clinician adoption, and ongoing HIPAA compliance and patient privacy. Desktop virtualization technologies, combined with integrated single sign-on and strong authentication, can address many of these challenges. Three steps hospitals can take to accelerate EMR adoption and achieve meaningful use include:

1. Deploy desktop virtualization throughout the hospital floor
2. Deploy single sign-on to the hospitals virtualized environment—providing No click Access to virtual desktops
3. Secure unattended patient data on workstations using OneSign Secure Walk-Away

The virtual desktop environment reduces implementation and management costs, by using thin-client workstations. A convenient, one-touch desktop with single sign-on reduces authentication problems and speeds adoption and acceptance. With authentication policies automatically enforced and unattended workstations monitored, hospitals can demonstrate HIPAA compliance and feel confident in the security and privacy of electronic health information.

### ABOUT IMPRIVATA

With more than one million healthcare users, Imprivata is the #1 independent provider of [single sign-on](#) and [access management](#) solutions for healthcare, government, finance and other regulated industries. By strengthening [user authentication](#), streamlining application access and simplifying compliance reporting across multiple computing environments, customers realize improved workflows, increased security and compliance with government regulations.

Imprivata has received numerous product awards and top review ratings from leading industry publications and analysts, including a Strong Positive rating in [Gartner's 2010 ESSO MarketScope](#), the #1 ranking in the KLAS SSO Performance report and the #1 rating in 2010 Best in KLAS and Category Leaders report.

Headquartered in Lexington, Mass., Imprivata partners with over 200 resellers, and serves the access security needs of more than 1,100 customers around the world.

