imprivata®

8 Tips For Increasing Cerner Millenium™ Adoption

Healthcare organizations with successful EMR adoptions have made sure to achieve physician and clinician acceptance before and during the transition to Cerner, and to minimize the effect of the new technology on workflow, even while securing access to patient data. This whitepaper highlights 8 tips that have been successful in increasing clinician adoption of Cerner Millenium.

INTRODUCTION: A QUICK OVERVIEW OF MEANINGFUL USE

Healthcare in the US is undergoing unprecedented change. The federal government has implemented the Health Information Technology for Economic and Clinical Health (HITECH) Act in hopes of transforming the efficiency and effectiveness of healthcare. Hospitals are scrambling to comply with Meaningful Use objectives within the HITECH Act to earn financial incentives.

The HITECH Act, part of the American Recovery and Reinvestment Act of 2009, puts $17 billion towards modernizing health information technology systems. The Meaningful Use objectives and associated incentives are intended to ensure that hospitals and physicians don't simply buy and install software and solutions, but that they integrate them in a significant way to improve the delivery of healthcare.

The Meaningful Use objectives are defined in three stages. Stage 1, taking place in 2011 through 2012, encourages the use of Electronic Medical Records for capturing and sharing data. Stage 2 (implementation by 2013) is about streamlining clinical processes, while Stage 3 (by 2015) focuses on improving healthcare outcomes. Each stage has financial incentives, penalties and deadlines from Medicare and Medicaid. As of this writing, hospitals face Medicare reductions if they cannot demonstrate Meaningful Use by 2015.

Also, EMR solution vendors must earn either a complete solution certification or "modular" certification for individual solutions for specific objectives. The modular certification is an important point, as many hospitals deploy multi-vendor environments with different component solutions for specific practices or parts of the healthcare environment.

This is a cursory description of a complex topic. For a more detailed description, see resources available at www.cms.gov/EHRIncentivePrograms. But there are several important points to note:

- ***Meaningful Use is a moving target:*** Exact objectives for each stage change in response to public comment. But hospitals that wait for finalization risk missing the full financial benefits of early compliance.
- ***Financial ramifications are steep:*** Hospital incentives include a $2 million potential base payment for early (mid-2012) adoption. And few hospitals are willing to risk reductions in Medicare reimbursements in 2015 if objectives are not met.
- ***It's both a sprint and a marathon:*** Hospitals must act quickly to achieve full financial incentives, yet be ready to make decisions that support future stages.

To meet immediate and long-term objectives, while continuing to comply with existing security and privacy regulations, hospitals need to create a strong and flexible foundation for integrating technology with patient care.

© 2011 Imprivata, Inc.

BARRIERS TO ACHIEVING MEANINGFUL USE

The technical barriers to Meaningful Use are primarily the responsibility of the various EMR vendors. With hospitals facing serious deadlines, vendors are working around the clock to update and certify their applications for Meaningful Use. This means that IT teams will be busy upgrading their applications with 'certified' versions. While difficult for IT teams, these software issues do not represent a significant barrier to broader compliance.

The real barriers to Meaningful Use compliance are outside of any individual software application—they are related to the effect that EMR technologies have on security/compliance, and on clinician workflows.

- The difficulty getting clinicians to adopt/use the EMR solution as part of their daily work—particularly physicians that are affiliated with, but not employed by, the hospital
- The effect of broader EMR adoption on security/compliance within the hospital

Clinician resistance

Any new technology represents a change over previous ways of doing things. For many people, change itself is a burden. For physicians and clinicians already pressed for time in a stressful environment, taking the time to learn and use new technology can be a hardship. Moreover, if that technology adds more work to their day rather than streamlining it, it's a trade-off many are unable to make.

To achieve widespread adoption, hospitals have to be sure that the EMR technology does not negatively affect physician and clinician workflows. If you ask around, you can find hospitals with functioning EMR solutions that physicians are not using, or physicians that insist on writing everything out on paper before it goes into the electronic record. Making the EMR solution both easy and attractive to use is essential for long-term success.

No matter how well the EMR software is designed, it exists within the broader ecosystem of applications that your clinicians use. A new application represents another login, another password to remember, and another application to bring up in each new location. Simply accessing new applications interferes with clinician workflow, introducing a barrier to adoption.

Maintaining HIPAA compliance

With the wider use of electronic records through the hospital, security and compliance teams need to ensure that HIPAA privacy and security requirements are met, defending patient data against risks due to:

- Unattended workstations with patient record data
- Passwords that are shared or written down, susceptible to compromise

© 2011 Imprivata, Inc.

As hospitals deploy EMR systems, they often take steps to lock down security, such as requiring physicians to 'log off' shared workstations, and using strong passwords and second authentication factors. If deployed with the EMR system, they are perceived as part of the total solution, and add more 'tasks' for the clinician to perform as part of the new environment. In effect, secure logins to multiple applications add to the workflow burden of EMR and feed clinician resistance to change.

To solve these problems, hospitals need to look beyond the EMR solution suites or modules to the complete IT environment to determine how to minimize the workflow impact of both the EMR adoption and the necessary security measures.

8 TIPS FOR ACCELERATING CERNER MILLENIUM ADOPTION

Many hospitals have made a successful transition to Cerner, with widespread adoption throughout the hospital. Hospitals with successful adoptions have taken care to achieve physician and clinician acceptance before and during the transition, and to minimize the effect of the new technology on workflow, even while securing access to patient data. This section highlights the strategies that have proven successful.

1. Study and minimize the workflow impact

Without understanding the existing clinician workflow, it is difficult to achieve smooth EMR adoption. Automating an inefficient workflow does not solve problems. Some hospitals deploy Cerner in concert with "lean" initiatives to streamline workflows and productivity.

- Workflows differ among practices: the workflow in neonatology, for example, differs from that in the emergency room. Hospital IT staff should work with clinicians in different departments and practices to understand what applications they use, where they use them, and how they move through the day.
- Be comprehensive: don't focus on a single task, such as medication administration, but how clinicians perform that task as part of the entire day, and as they move between locations.

By being sensitive to specific workflow needs, it is easier for IT groups to adjust solutions to minimize disruption, and to identify opportunities for rapid improvements in workflow for 'quick wins' in the EMR implementation.

2. Deploy in phases and find advocates

Many successful IT teams work with the different groups to roll out new technologies in phases, building successes and solving individual problems before moving on. A best practice is to find and work with advocates in each group. A physician who is convinced of the benefits will be more powerful in driving acceptance than any IT group can be. To make clinicians advocates of change, the technology must improve their workflow or deliver a visible benefit.

One strategy that may work is starting with the most difficult to please physicians first—start with the 20% that are likely to give you the most trouble, and take the time to get them running and successful. The remaining 80% will be easy.

© 2011 Imprivata, Inc.

3. Use physicians to train physicians

In addition to physician advocates, many hospitals have enlisted early-adopter physicians to train their colleagues on new technologies. In learning new technologies, physicians want to work with someone who understands their needs, particularly for technologies like EMR that affect the delivery of care. The location and timing of training are also potential barriers; physicians don't want to sit in a large classroom for hours. Offering training at the physician's convenience, in small groups, is another strategy for speeding adoption. By offering training from a fellow physician, on the physician's own terms, hospitals have greater success getting physicians up and running with new technologies.

4. Eliminate password problems with single sign-on

Deploying an EMR solution adds a new application (or multiple applications) that each clinician needs to log into each day, from every new location. This is in addition to logins they already have for e-mail and other clinical or administrative applications, as well as the actual workstations they use, if workstations are shared. If your hospital is taking the 'modular' approach to Meaningful Use compliance, using many different components for a complete solution, the login problem is even more acute.

In each new location, the clinician must remember and type the account and password for the workstation and for each application they access, which adds a barrier between the clinician and the patient data. Deploying a single sign-on solution immediately addresses the "not another login!" reaction and relieves clinicians of the existing burden of password management. At the same time, single sign-on solutions help IT groups track and manage application access, and provision applications to clinicians and other users.

With Imprivata OneSign, clinicians can sign into Cerner without typing and tabbing, by simply touching a finger or ID badge (proximity card) to a reader. Whenever a physician enters a new room, a single touch is sufficient to provide secure authenticated access to Cerner.

5. Simplify authentication and online signing with No Click Access™

IT organizations need to protect the login to the patient health records, whether it is part of a single sign-on solution or not. For full HIPAA security and privacy compliance, hospitals need to ensure that only authorized users gain access to patient data. Relying on passwords alone is fraught with risk – supplementing logins with physical measures (such as devices or biometrics) enhances security.

A variety of authentication technologies can streamline login to the desktop and its applications, particularly when integrated with single sign-on. Simple, No Click Access™ methods include:

- Passive proximity cards/badges that the clinician simply taps to a reader
- Fingerprint biometrics – touch a finger to a keypad

These options let clinicians access patient data without any typing. Again, it is important to match the method to the location. Fingerprint biometrics may work better in some areas, badges in others.

© 2011 Imprivata, Inc.

6. Simplify transaction-level strong authentication

Stage 1 Meaningful Use objectives include requirements that physicians re-authenticate with the application when executing electronic prescriptions or ordering medications using CPOE. Typically the physician must re-type their password for these protected transactions—once again distracting attention away from the patient. Using Imprivata OneSign, the physician can re-authenticate with a swipe of a fingerprint or tap of an ID badge—ensuring that the physician is the one placing the order or 'signing' the e-prescription while simplifying the process.

7. Automate logoffs from shared workstations—secure patient data

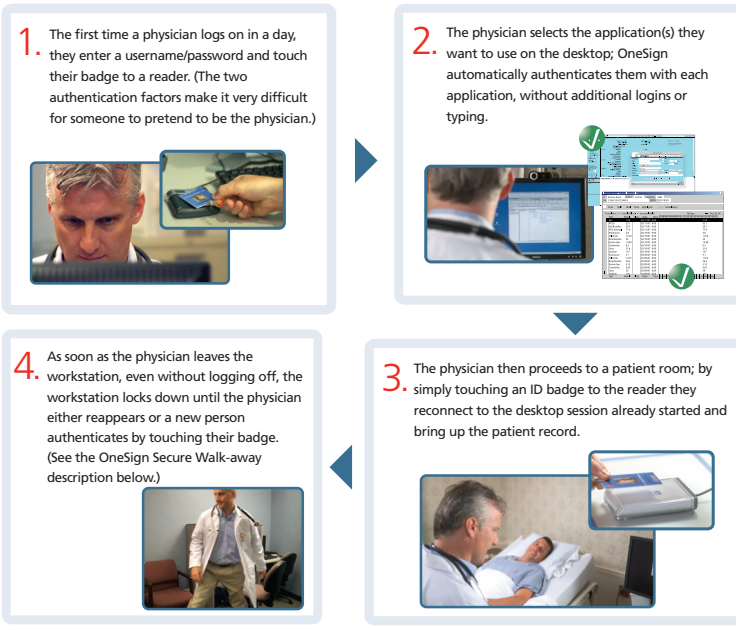
Hospitals meeting the Meaningful Use objectives will update patient records from a variety of locations, including patient rooms, shared workstations in hallways or nursing stations, and physician offices. In locations where the workstation is shared, an unattended workstation represents significant risk:

- A clinician at a shared workstation may inadvertently enter data into the wrong patient's record, endangering patient care
- An unauthorized individual may be able to gain access to patient data, violating HIPAA privacy measures

Requiring physicians and nurses to explicitly logoff each time they step away is impractical in the real-time healthcare environment. Instead, hospitals can deploy automated solutions that automatically lock down when the authorized user leaves, then restart at a single touch for simplified workflow combined with optimal security. View the "Protecting Unattended Clinician Desktops" Video.

8. Support clinician roaming with a virtual desktop

Adding a desktop virtualization environment to an Cerner rollout is another way to accelerate adoption by improving workflow. Using a virtual desktop in combination with single sign-on, clinicians can access their personalized workstation, in its current state, from different locations throughout the day.



For example, a physician can leave a record open in a patient room, walk to the office, and recall that same session with the record open with a single touch from the desktop. They can then complete the entry and close the patient record. This technology is attractive for time-pressed clinicians who roam throughout the day.

© 2011 Imprivata, Inc.

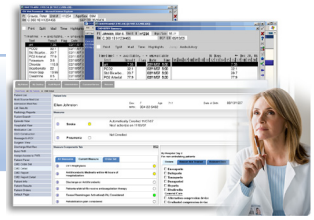
SOLUTION OVERVIEW: SIMPLIFYING AND SECURING CLINICIAN'S ACCESS TO PATIENT INFORMATION

Imprivata's healthcare solutions are specifically designed to streamline healthcare workflows allowing clinicians to spend less time with technology, more time on caring for patients.

Physicians have the freedom during patient rounds to easily access their patient's chart. Whether the data resides in legacy, virtual or web based applications. With a swipe of their badge and/or finger at any workstation on the floor at the nurses' station/patient room or in the physician lounge they are in their patient's chart.

OneSign® Single Sign-On
OneSign® Authentication Management
OneSign Virtual Desktop Access™
OneSign FBID

Physicians can easily navigate from a patient's chart to the PACs system to review an X-Ray without having to enter additional passwords.



OneSign® Single Sign-On

When reviewing a patient chart; a colleague interrupts with a question. The physician walks away from the workstation; as soon as they walk away the workstation locks; if they return within a defined period of time they are automatically logged back in.

OneSign® Single Sign-On
OneSign® Authentication Management
OneSign Secure Walk-Away®

Physicians can easily go from reviewing the patient chart to signing a new order with a swipe of their badge or finger – never having to remember any additional PIN or Passwords.

At discharge physicians can move from creating the discharge summary to signing off on the patients home meds via ePrescribing with a swipe of their badge or finger – never having to remember any additional PIN or Passwords.

OneSign® Single Sign-On
OneSign ProveID
OneSign FBID

When on-call, in their office, at home or on the road physicians have the same secure easy access to their patient charts as if they were in the hospital.

OneSign® Single Sign-On
OneSign® Authentication Management
OneSign Anywhere™

© 2011 Imprivata, Inc.

SUMMARY

By implementing some or all of the strategies above for improving Cerner adoption, hospitals can achieve the dual objectives of improving clinician acceptance and satisfaction with new technologies while enhancing compliance with HIPAA Security and Privacy regulations.

Authentication and access control measures such as single sign-on with strong authentication create a strong foundation for hospitals that need to both achieve immediate compliance with Stage 1 while forging a path towards the lesser-known Stage 3 objectives. A strong access and authorization infrastructure supports all technology initiatives, beyond Meaningful Use, and gives hospitals centralized control over and visibility into access to all of the applications that clinicians and employees use, even as the applications themselves change and increase in number.

IMPRIVATA ONESIGN®—SPEND MORE TIME WITH PATIENTS

Imprivata's healthcare products are specifically designed to streamline healthcare workflows allowing clinicians to spend less time with technology and more time with patients. The Imprivata OneSign solution suite helps hospitals meet Meaningful Use objectives by improving adoption and clinician acceptance with simplified, secure access to patient data and applications.

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 1,400 customers around the world.

© 2011 Imprivata, Inc.

Worldwide Headquarters
10 Maguire Road, Building 4
Lexington, MA 02421-3120 USA
Phone: 781 674 2700
toll-free: 1 877 ONESIGN
Fax: 781 674 2760

www.imprivata.com

© 2011 Imprivata, Inc.