



...Essential Security

Proactively Controlling Access to Patient Data

The challenge: In a typical healthcare organization, hundreds to thousands of medical and support staff need to access patient data to do their job. How do you effectively enforce access controls to hospital information systems without hampering medical care efficiency and effectiveness?





The Shift to Electronic Medical Records Increases the Challenge of Keeping Information Private

In light of President Obama's drive to make electronic health records a cornerstone of national health care reform, healthcare organizations are going to be further challenged to ensure patient privacy.

Changes to Health Insurance Portability and Accountability Act (HIPAA) were recently enacted as part of the new American Recovery and Reinvestment Act to support this shift to electronic medical records. The American Recovery and Reinvestment Act of 2009 provides over \$22 billion to develop, implement, and promote new health information infrastructure, including nationwide electronic health records by 2014. To address the privacy and data security challenges presented by electronic health records, the new law also mandates significant changes in the health data privacy and security regulations issued under HIPAA as part of the Health Information Technology for Economic and Clinical Health Act (HITECH).

While these changes don't go into effect until February 2010, most security professionals are starting to look now for ways to improve their access controls to sensitive IT infrastructure, services, data, and applications.

What's more, the Department of Health and Human Services is getting much tougher about HIPAA non-compliance. The Department recently imposed fines on both Providence Health and CVS Caremark Corporation, putting even more teeth into the 12 year old regulation and causing hospitals to take HIPAA compliance more seriously.

Another example of how regulations are driving hospital data privacy requirements is two new California laws that impose harsher penalties for hospital workers who inappropriately access patient data. The law was driven by multiple cases where high-profile patients' records were breached including files for Farrah Fawcett, Maria Shriver and Britney Spears at UCLA Medical Center. In fact, as many as 165 doctors and other workers had improperly accessed the medical records of numerous celebrities over a 13 year period.

Earlier in 2009, a Los Angeles hospital fired 15 workers for accessing the medical records of octuplet mother Nadia Suleman without permission. In this case, the hospital was monitoring the systems and was able to determine who had medical reason to access the files, and therefore discovered the breach. However, the hospital fell short in that they were unable to proactively restrict access to appropriate medical personnel.

“The snooping incidents highlight the lack of adequate data-security controls at hospitals and other healthcare organizations,” said Deborah Peel, who heads the Patient Privacy Rights Foundation in Austin, TX. “Thousands of workers may be able to access patient data, even if they don’t need to do so.”

The Unique Aspects of Healthcare Related to Access Control

The healthcare business features serving thousands of patients, receiving a myriad of procedures, provided by thousands of workers, with differing needs to access and update information.

To do their job, nurses, doctors, technicians, and administrators must access a variety of applications, running on diverse servers, from a variety of desktops and wireless devices. And they need to access applications and update records from a variety of locations: start at bedside...move to clinic...back to doctor’s office...or move between patient appointment rooms. Logging onto both the desktop and then the application is time consuming. Leaving the patient in the room with the desktop application “open” is a security risk. The challenge is to grant the various healthcare workers secure, rapid access to the applications and data they need as they move about the organization serving patients, often in stressful situations.



Best Practices for Securing Patient Records

So how do you best secure patient records without impeding levels of care? You don't do it by reporting on who accessed records after the fact. You must implement proactive, robust access controls. These proactive controls include:

- **Authentication:** verify that the person is who they say they are... and control how you want the person to authenticate based on who they are, where they are, and what systems they need to access.
- **Authorization:** control what systems, applications and data they can access and how/when.
- **Audit:** record all user access events and consolidate that information across diverse servers and applications.

Sounds good, but considering that you have desktops, connecting to servers, running a variety of applications and databases... the ability to control thousands of users accessing data is a huge challenge.

Another big challenge: How do you secure data without making it cumbersome to access? Doctors and nurses do not have the time to repeatedly enter desktop and application passwords as they move between appointments and clinics. Difficult processes will likely alienate doctors and nurses, who are key to the success of an organization.

Making hospital information systems and databases easy to access, yet secure, requires a flexible, enterprise solution. There are several best practices you should consider. Let's think of them in terms of multiple access control layers.

Layer One: Control access to the core hospital information systems and applications.

Here is where you associate users with their "entitlements" or "privileges".

- First you centrally define user roles (users with similar security requirements), and determine which systems they are authorized to access and how they can access these systems (access profiles/rules).
- Next you associate your actual hospital workers with these roles and access profiles.
- Finally, you define and associate what type of authentication is needed for the particular user role or system being accessed.
- Key tip: Leverage smart cards, or virtual smart cards to reduce sign-on requirements. This will greatly improve ease of use and productivity, while greatly increasing the security of your desktops. Using smart cards, users do not need to enter passwords for the desktop access and then another password to access the application. The initial password and security credentials in a smart card are all that is required. The user simply puts in the smart card to start a session and when they remove it, the session is closed automatically. It makes it easy to securely share desktops.

Layer Two: Control access down to the data level

- Ideally, you should be able to enforce and authorize access (read, write, execute, copy delete) to specific files.
- Access privileges should be associated with the roles defined in Layer One.
- You also need the ability to control and monitor file access in real time.

Layer Three: Control access to the operating systems that drive the servers.

- Privileged users who administer the operating systems and databases often have the most “open ended” access to underlying data and therefore, can do the most damage. How well are you controlling the users who control your systems?



- If you allow privileged users to sign on directly as “root” or “sysdba” you cannot track exactly which person accessed the system and what they did.
- Again, user privileges can be granted by role.
- You need to apply a unique blend of technologies to control and track privileged users.
- Plus implement a password vault for the cases when you must utilize the root account password.

Layer Four: Consolidate user activity logs and access events from across servers and applications and create meaningful reports.

Reporting is key to achieving compliance, simplifying your internal audits, and implementing continuous improvements in access control policies.

Look for a comprehensive enterprise access management solution versus best-of-breed point solutions to reduce implementation costs, integration efforts, and associated on-going support costs.

The Real Value of Access Controls Management

- **Reduce the Cost of Administration:** By creating logical groups of host machines and assigning users to roles with similar security requirements, administrators no longer need to setup individual users access controls. That means adding new users or removing users who have left is very efficient. As well, some access management solutions also enable your IT staff to centrally manage passwords, SSH keys, and PKI credentials to further reduce operating costs while improving security.
- **Simplify Accessing Systems and Maximize Medical Staff Productivity:** The ability to leverage smart cards or other similar technology can reduce the amount of time doctors and nurses spend signing-on to the patient information system as they move about the hospital and clinics. They can focus on healthcare and not the underlying systems.

- **Pass HIPAA Audits and Reduce Exposure to Penalties:** The ability to proactively and centrally control access to desktops, applications and servers is key to maintaining security over patient records. Consolidated, robust audit logs and reports provide timely meaningful information to auditors and regulators alike. You are much more likely to pass HIPAA audits with a lot less effort.
- **Reduce Impact of Security Breaches:** Even though your reputation is based on your level of healthcare and not your IT systems, a security breach is not the kind of publicity you want.

FoxT Enterprise Access Management Solutions for Healthcare

FoxT provides centralized access control management to simplify securing the data and systems that drive your healthcare organization. The FoxT solution suite enables you to centrally manage authorization, authentication, and auditing across diverse server platforms, applications and desktops. Here is a case study from one of our healthcare customers, Danderyd Hospital in Sweden.

Danderyd Hospital, Sweden – A Case Study

Simplified, Secure Access Management

One of the security challenges Danderyd Hospital faced was that thousands of their healthcare staff had access to the patient administration system. A majority of the medical staff used shared PCs on the wards and could be called away from their workstation at any time. As well, the workers who shared PCs often had different system security privileges and patient data access rights. FoxT Access Control for Desktops solution solved these problems for Danderyd by providing strong, two-factor authentication to the PCs in the form of a smart card, which contains public key credentials that verify the identity of the user.



Without their cards, the medical staff cannot log onto their computers, and if a smart card is removed during a session, FoxT Access Control for Desktops automatically locks the PC, preventing unauthorized access. A new user can, however, easily and quickly continue to work on the same PC if his or her smart card has the proper privileges.

Patient Data Protection

Danderyd Hospital also uses two other FoxT solutions: FoxT Access Control for Servers for securing the database servers, application servers, and the network, and FoxT Access Control for Applications, which provides a reduced secure sign-on to the Melior patient records system. These solutions function as seamless components with FoxT Access Control for Desktops, implementing an integrated security strategy that keeps Danderyd's patient records secure and assures that the hospital passes its yearly platform audit.

The Melior patient record system uses a Sybase database on the servers. Danderyd opted to use FoxT Access Control for Applications to integrate the smart card authentication system with the Sybase security system, providing a common reduced sign-on to the desktop and to the application. Users do not have to enter multiple passwords to both the desktop and application: the initial card password and the security credentials in their card are all that is required. As well, the traffic between the PC and the application is automatically encrypted to further improve security.

Reducing the Cost of Administration

FoxT Access Control for Servers, Desktops and Applications solutions reduce the cost of administration at the hospital by providing logical groups of host machines, applications, and users with well defined security requirements.

Administrators no longer have to set up individual user access controls; access entitlements can be activated as a single action for all users

with similar needs. Similarly, users can be granted access specifically to the applications and hosts necessary for them to be effective in their jobs in the hospital - in one operation.

Streamlined access management both aids Danderyd in implementing and enforcing their security strategy and helps them prove their ongoing compliance to all the appropriate healthcare and personal privacy regulations.

Copyright © 2009 FoxT. All rights reserved.

The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.

