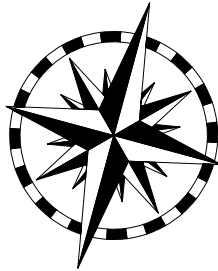


I



# TRUE NORTH ESSAY

---

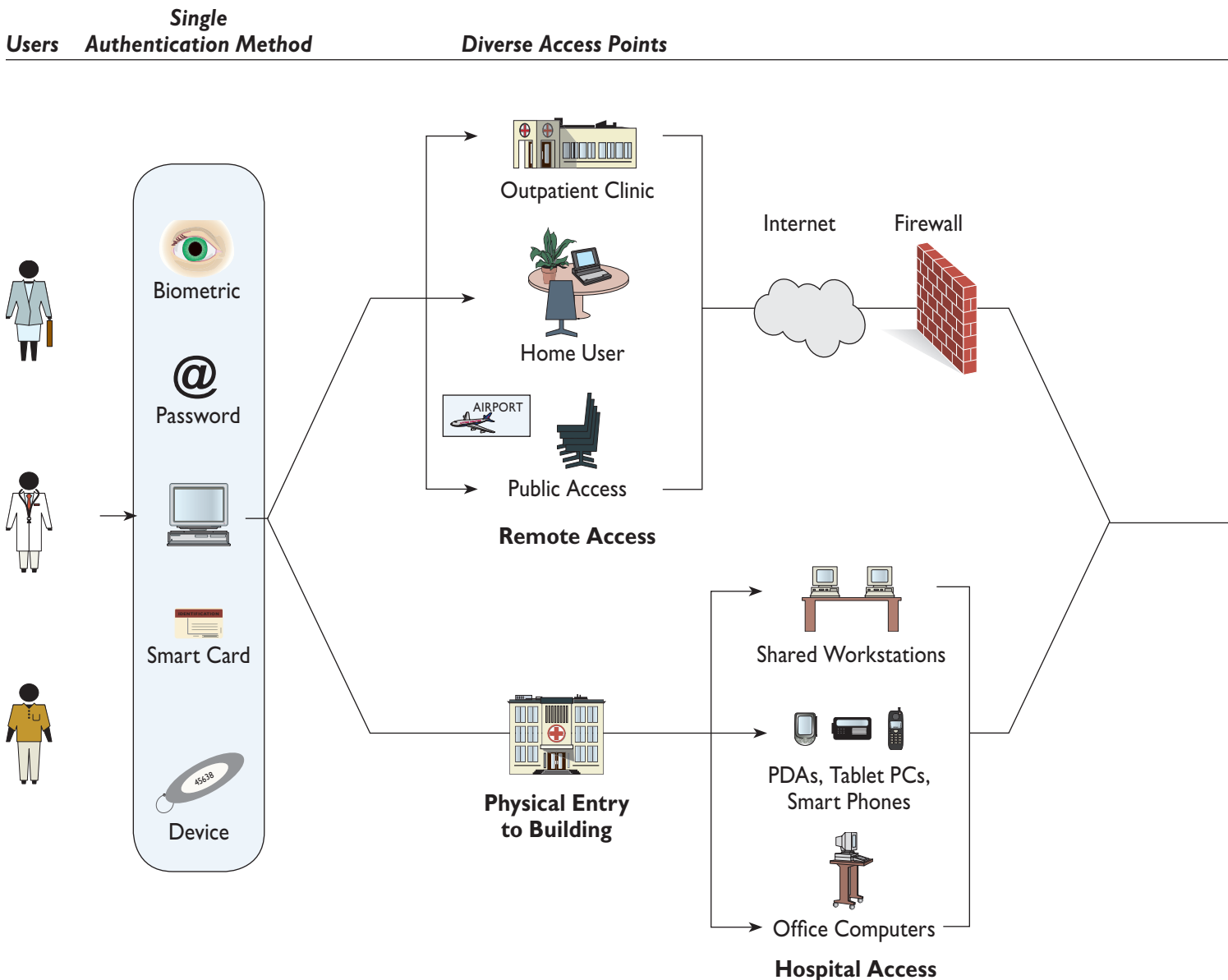
*Balancing Security and Convenience*

## ENVISIONING THE FUTURE STATE

### #1 True single sign-on (SSO)—the ability to access all resources with a single form of authentication—is the “Holy Grail” of today’s cluttered hospital IT systems

Clinicians face a mix of information systems that are often outdated, confusing, and difficult to navigate. Adding to the disorder, each system maintains its own proprietary user directory, patient data, and authentication scheme which do not interoperate, requiring separate logons. True single sign-on (SSO) alleviates these problems, providing seamless access to patient data across disparate systems—both inside and outside of the hospital—with a single form of authentication.

### The Holy Grail 2020: Secure and Transparent Access



Source: True North interviews and analysis.

**#2 In the ideal state, identity and access management (IAM) includes centralized authentication, authorization, and administration of users**

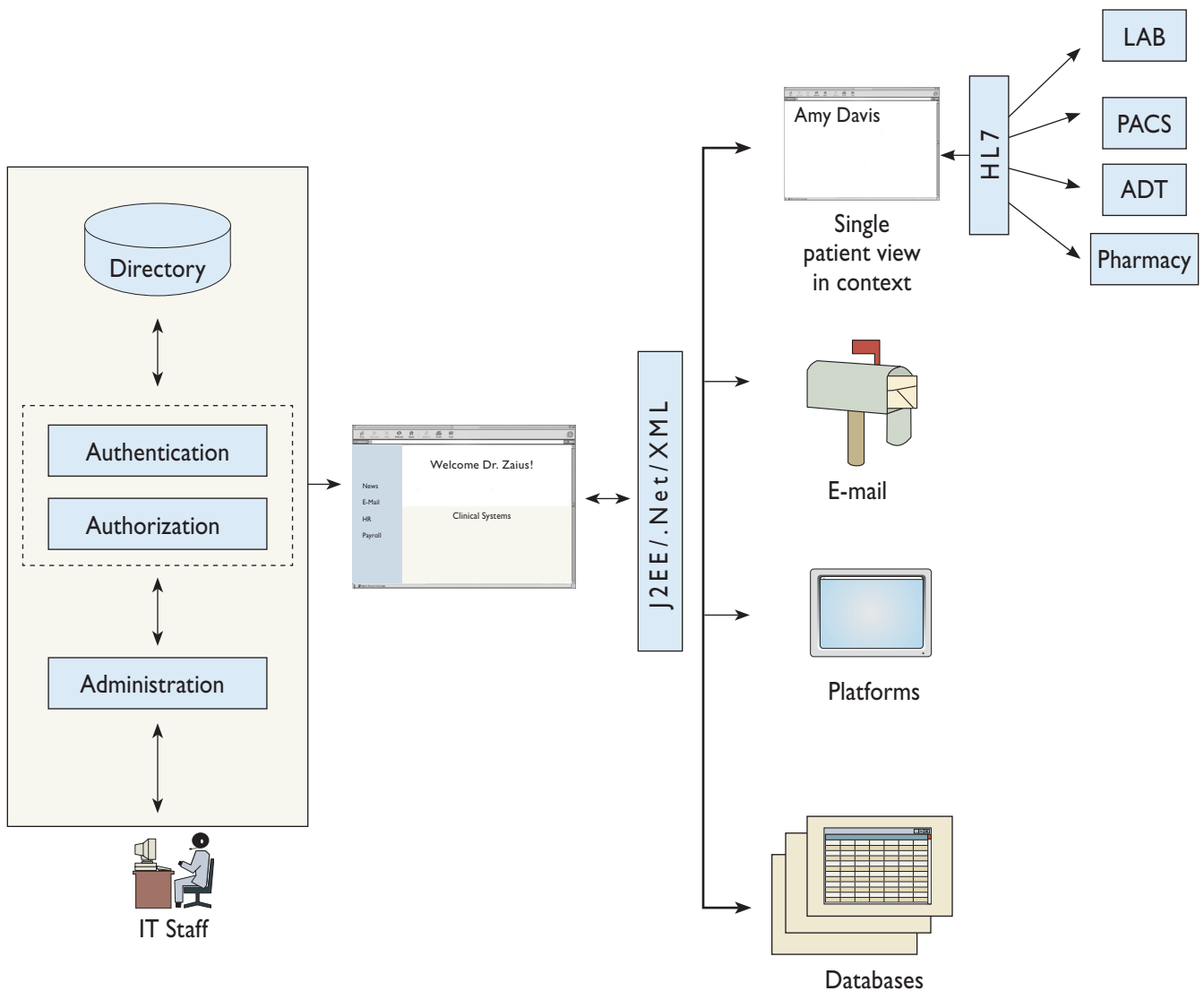
In the future, access is controlled from a central point. Users authenticate against a central directory and obtain authorization based on policies. IT staff have a single administration point to manage the directory, define policies, and provision and de-provision users. All applications use Web services, and a clinical portal displays patient data from disparate systems.

**Enabling Greater Clinician Effectiveness**

**Identity and Access Management**

**Portal/Presentation**

**All Electronic Resources**



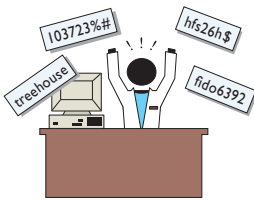
Source: True North interviews and analysis.

## STRUGGLING WITH TODAY'S ENVIRONMENT

### #3 Today, clinicians must work in complicated and cumbersome hospital IT environments

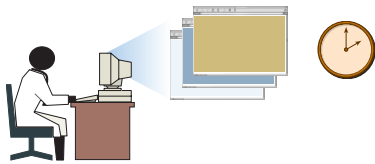
Multiple logons and passwords for different applications are barriers to efficient clinical workflow and clinician acceptance of IT. Multiple access points both in and out of the hospital present distinct authentication challenges. Remembering passwords and navigating systems are major sources of frustration for clinicians.

### **Barriers to clinical workflow...**



#### **Passwords Produce Clinician Frustration**

- Typical users access 7–8 different applications, many with their own passwords
- Passwords difficult to remember because of expiration frequency, strong password policies
- Different forms of authentication for different access points (e.g., ID token at home, password in the hospital)



#### **Accessing Data is Time-Consuming**

- Switching between users can take between 30–90 seconds
- Logging on to each application can take an additional 5–30 seconds
- Locating the same patient, who may have different identifier in different systems, can add 10–60 seconds to the process



### **...and their effects**



#### **Security Threats**

- Passwords are written down, lost, or left in plain view
- Users choose simple, easy-to-guess passwords
- Clinicians share accounts, violate access rights, and are not audited
- Users fail to logoff, exposing patient data

#### **Diminished Quality of Care**

- Clinicians might not use applications if they forget passwords or if logon is a hassle, compromising quality of care
- “Dirty log-offs” and system reboots mean loss of data and time



#### **Increased Help Desk Calls**

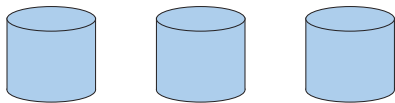
- Password resets account for 20%–40% of help desk calls, each call costing an estimated \$25–\$50
- Unlocking account after several failed login attempts further burdens help desk

Source: Novell, “HIMSS Audio Conference: Single Sign-On for Healthcare,” available at: <http://www.novell.com/industries/healthcare/sign.html>, accessed July 27, 2006; True North interviews and analysis.

**#4 Siloed IT infrastructure complicates IT department’s responsibilities to control security, manage user identities and access rights**

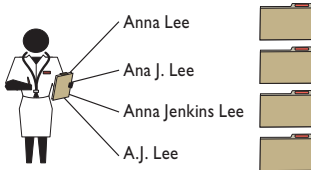
Hard-to-remember passwords lead to potential security breaches, HIPAA violations, and threats to patient data. With user identities and access rights isolated in different clinical databases and directories, there is no central administration of IAM components; provisioning, access control, authentication, and auditing must be performed at the application level.

***Burdens on IT staff...***



**Isolated Directories Without Central Administration**

- Each application maintains its own directory of users, credentials, access rights and password policies

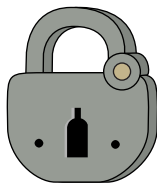


**No Automatic User Provisioning or Account Management**

- Directories contain many obsolete or duplicate accounts
- No established policies on password strength, access rights, or strong authentication



***...and their effects***



**Security Threats**

- No strong authentication deployment
- No role-based access control
- No user-based auditing



**Productivity Loss**

- New users wait days or weeks for appropriate resources and access rights
- IT manually sets up accounts and access rights in each of the back-end systems
- IT monitors security logs at the application level

Source: True North interviews and analysis.

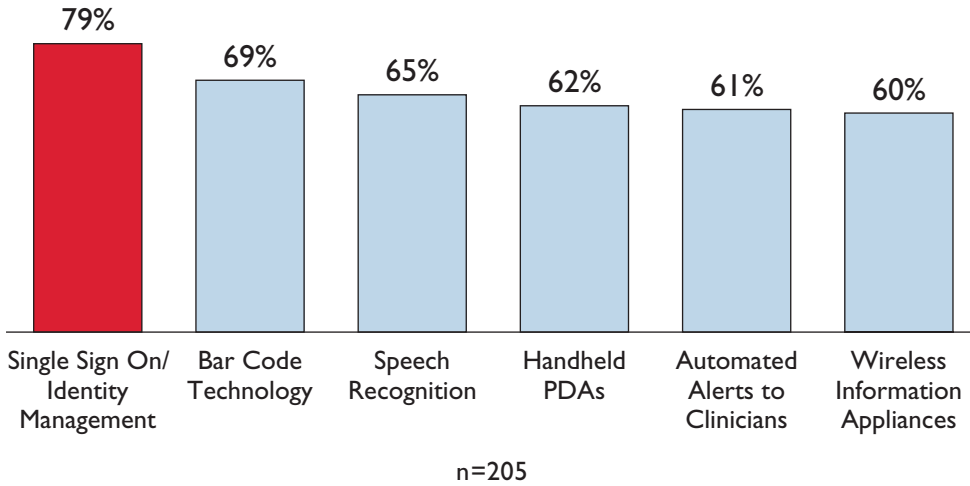
# 5 As a result, SSO increasingly seen as a “must have” investment in the era of the EMR

Hospital IT departments are under increased pressure to reduce the number of passwords and the amount of time spent searching for data. As the number of technologies in the hospital increases, these concerns will only become more pressing. Integration via standards or portals may be several years away, but SSO can provide a stopgap in the meantime.

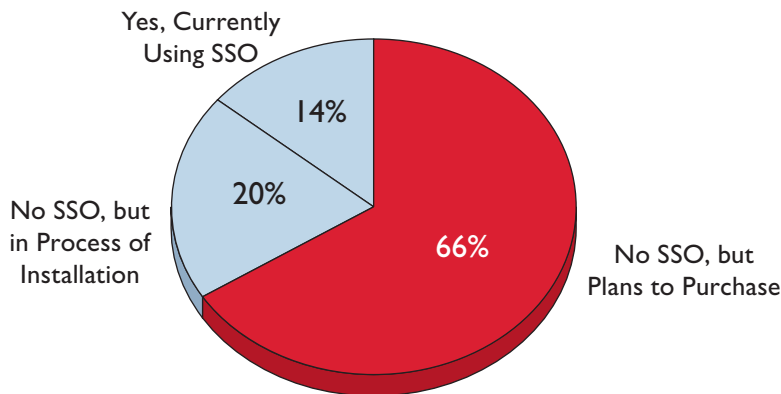
**A top-of-mind solution...**

Top Technologies to Buy Over the Next Two Years

Percentage CIOs in 2006



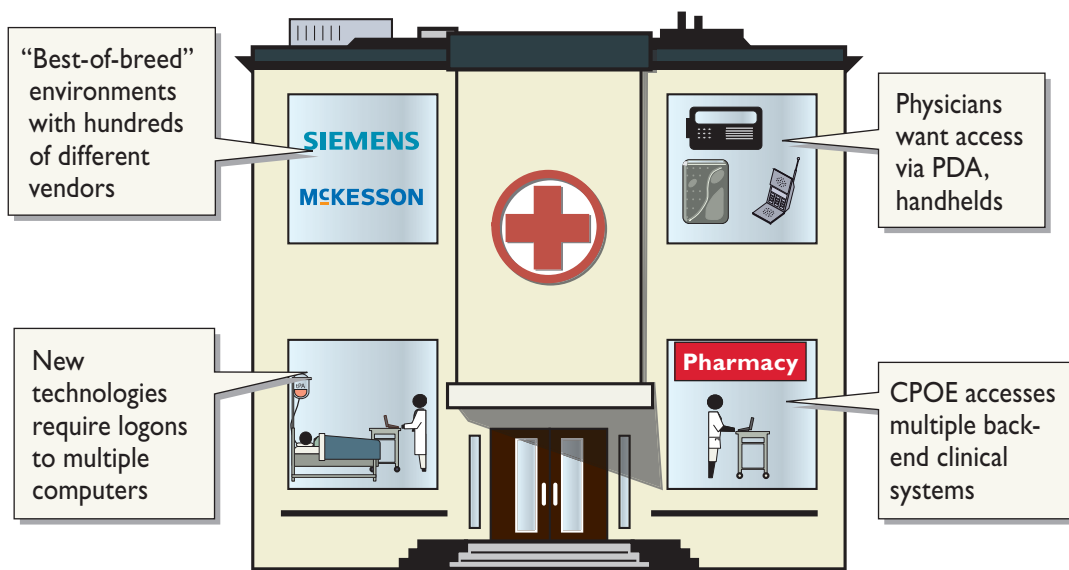
Current Stage of SSO Installation



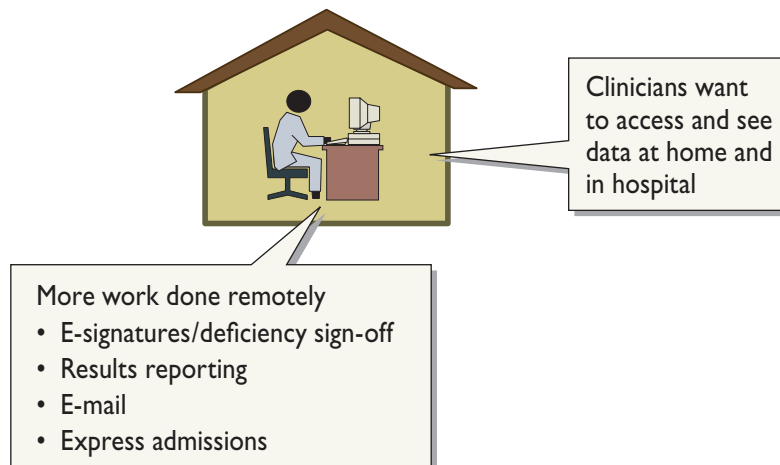
Source: 17th Annual HIMSS Leadership Survey, sponsored by ACS Healthcare Solutions, available at: <http://www.himss.org>.

**...to an ever-growing challenge**

**A Hotbed of New Technology**



**Allowing Remote User Access**



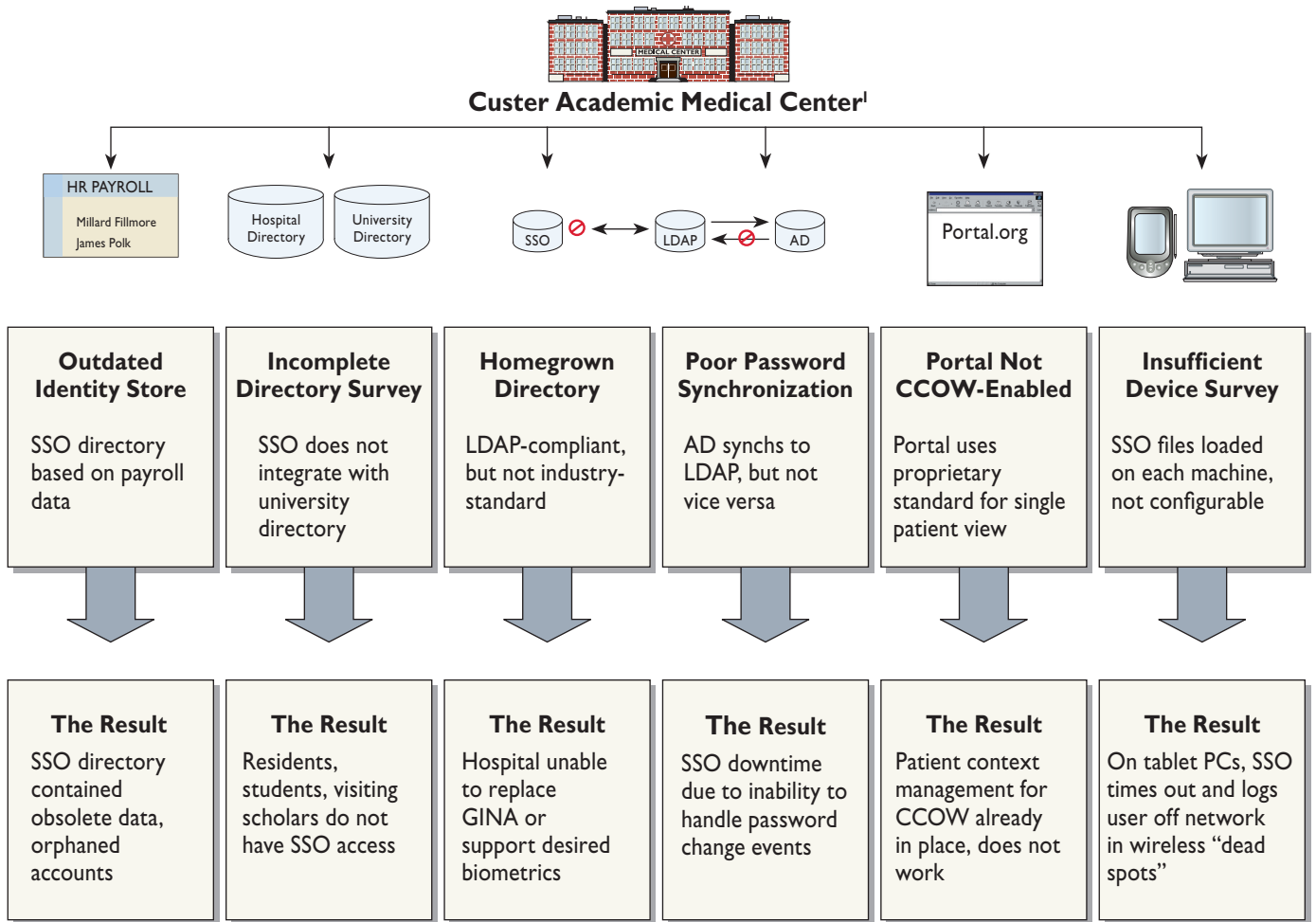
Source: True North interviews and analysis.



**#6 SSO is not necessarily plug-and-play and risks becoming “just another application” with its own password and management needs; ignoring other pieces of the identity and access management puzzle can have serious negative consequences**

Deploying SSO without thoroughly surveying your IAM environment and identifying IAM needs leads to real problems. Unaccounted users, devices, and applications result in access gaps and interference between overlapping technologies.

**Easy to Underestimate the Challenge**



**CASE-IN-BRIEF**

- Custer Academic Medical Center, an early adopter of E-SSO and Context Management
- Research-heavy institution with high turnover, diverse platforms, and non-clinical settings

¹ Pseudonym.

Source: True North interviews and analysis.

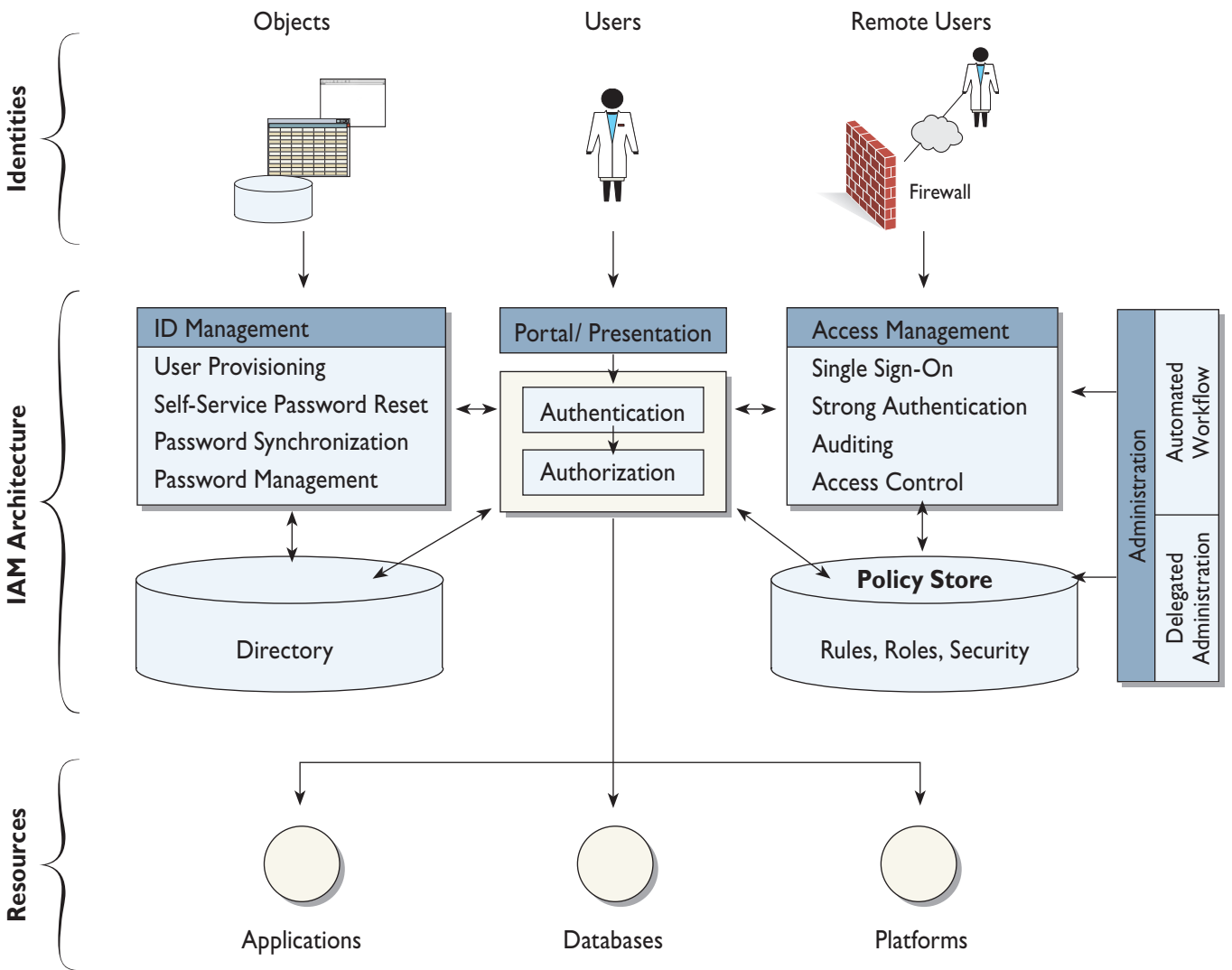


# SSO IN BROADER CONTEXT

## #7 SSO is just one piece of the IAM puzzle

While SSO can address many concerns at once, expecting SSO, in and of itself, to solve all of an organization's IAM needs will lead to disappointment. A successful IAM strategy depends on thorough planning and process management, and an appropriate mix of IAM-related technologies.

### SSO Is Only One Part of an IAM Strategy



### NO MAGIC BULLET

"Anything that is wrong with your security infrastructure—be it process or technology—is going to become visible and amplified with single sign-on."

Chief Technology Officer  
Southern Health System

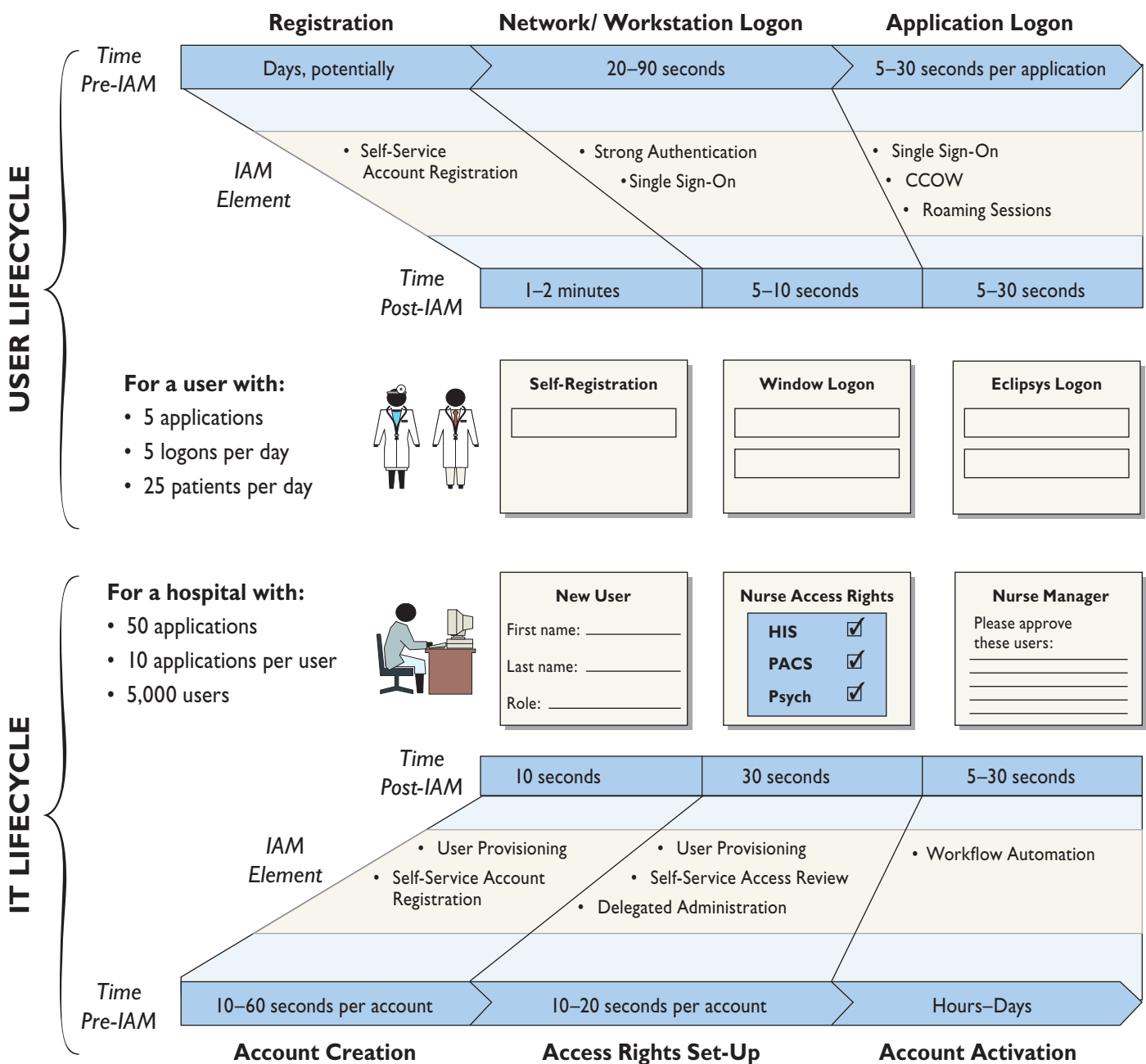
<sup>1</sup> Pseudonym.

Source: True North interviews and analysis.

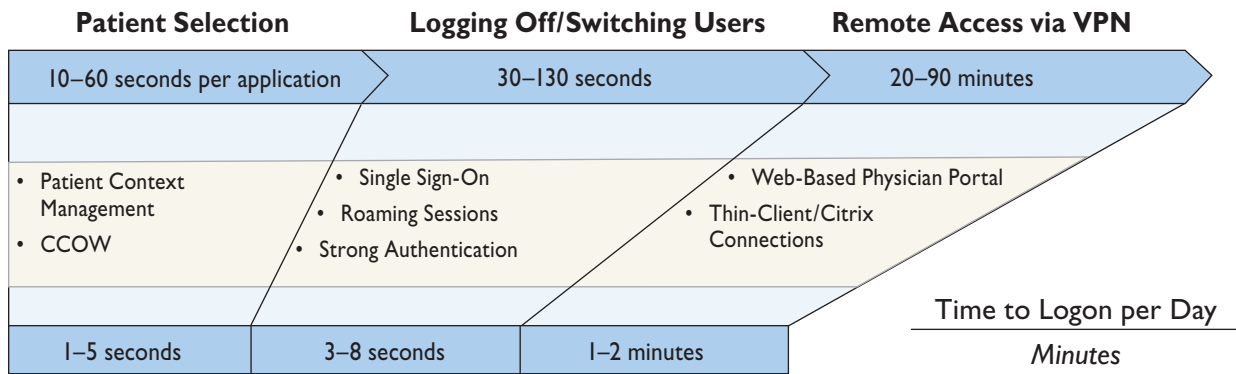
#8 Deployed carefully, however, an IAM strategy reaps significant time savings

IAM solutions can generate tangible benefits for both users and IT staff—beyond helping hospitals meet their security mandate. IAM components can automate almost every step a user takes to access information systems and every step IT takes to manage user accounts.

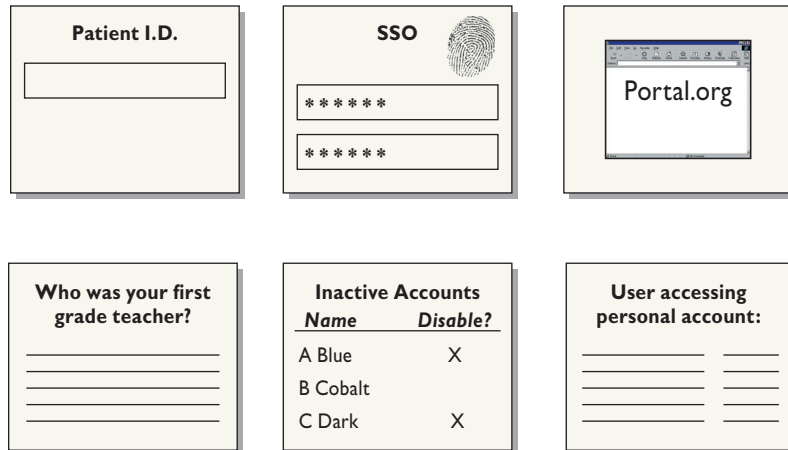
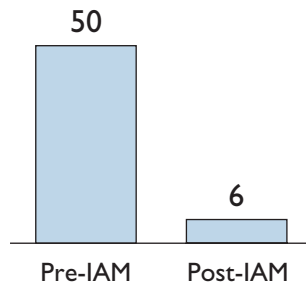
**Reducing Barriers to Initial Access**



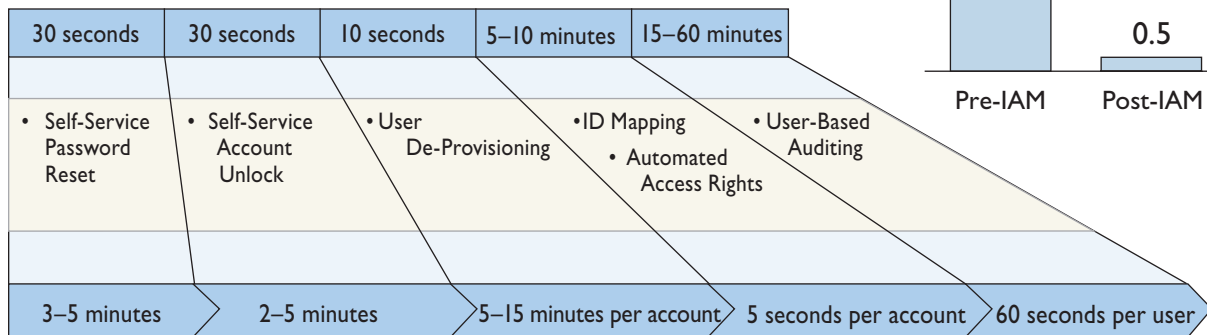
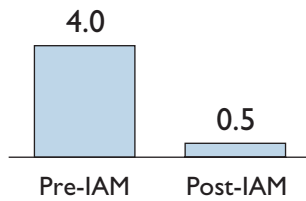
## Sustaining Ongoing Efficiency Gains



Time to Logon per Day  
Minutes



Time to Manage a Single User  
Hours



**Password Reset    Account Unlock    Account Disable    Account Clean-Up    Audit User Activity**

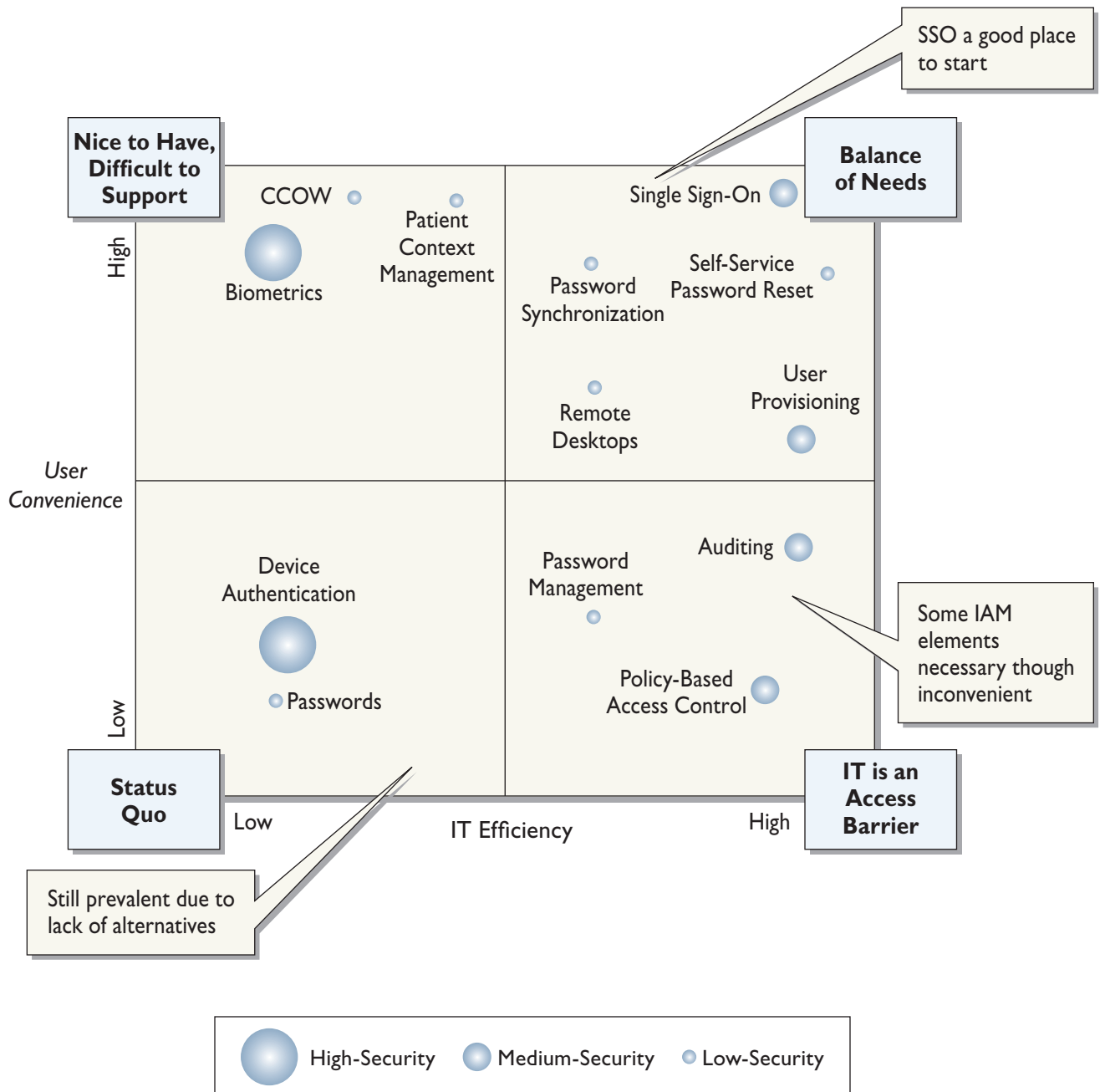
Source: Novell, "HIMSS Audio Conference: Single Sign-On for Healthcare," July 27, 2006, available at: <http://www.novell.com/industries/healthcare/sign.html>; True North interviews and analysis.



# 9 SSO can be a high-profile win for IT, achieving both security and convenience objectives, and a good first step in an overall IAM strategy

Typically user convenience, security compliance, and IT needs are at odds. If deployed correctly, SSO can occupy the sweet-spot, catering to all three, particularly when compared with other potentially valuable IAM products that cater primarily to only one of the three measures.

**Identifying the Big, Early Win**



Source: HIMSS Analytics, "Why You Need Single Sign-On," available at: [http://www.himssanalytics.org/PDFFiles/Single\\_SignOn\\_Webinar.pdf](http://www.himssanalytics.org/PDFFiles/Single_SignOn_Webinar.pdf), accessed July 17, 2006; True North interviews and analysis.

## PUTTING THE PIECES TOGETHER

### Selecting Elements for

Authentication—Verifying the User’s Identity			
IAM Component	Description	Effect on End Users	Effect on IT Staff
<b>Enterprise Single Sign-On (E-SSO)</b>	Technology that intercepts logon prompts and presents usernames and passwords.	+ Only one password + Faster access	+ Fewer help desk calls + Central administration point for identities, access rights – Careful planning required
<b>Web Single Sign-On</b>	Controls access to Web resources via proxy server, or plug-ins. Cookies track session and authentication state.	+ Portal centralized access – No access to non-Web resources	+ Central administration – Difficult to integrate external Web, internal non-Web resources
<b>Password Synchronization</b>	Technology that synchronizes passwords, propagates password changes across directories.	+ Only one password – Passwords entered manually	+ Fewer help desk calls + Cheaper than SSO – “Lowest denominator” password policies
<b>Reduced Sign-On</b>	Practice of pointing applications to existing directories by modifying application’s authentication code	+ Fewer passwords – Must still enter passwords	+ Fewer help desk calls – Significant scripting required
<b>Self-Service Password Reset</b>	Feature allowing users to reset their passwords by answering a series of security questions.	+ No wait for help desk reset	+ Fewer help desk calls
<b>Strong Authentication</b>	Authentication with more than one factor or with a highly secure factor like a biometric.	+ Faster access with proximity + Biometrics, devices eliminate passwords – Factor to remember or carry	+ Fewer help desk calls + Security – Device installation, cost – Reliability concerns
<b>Password Management</b>	Enforcing policies on password length, numeric or character requirements, and expiration rates.	– Passwords difficult to remember	+ Security

Authorization—Granting Users Correct Access			
IAM Component	Description	Effect on End Users	Effect on IT Staff
<b>Access Control</b>	Process of deciding user access based on roles, rules, and policies.	+ Personalized access – Additional access step	+ Security – Additional management
<b>Policies</b>	Organization’s established security practices. Definition of roles, rules, password strength, privacy, etc.	+ Personalized access – Limited access	+ Security – Central administration
<b>Auto Timeout</b>	Practice of automatically locking a workstation after a designated time.	+ Session locked, not closed – Need to re-authenticate	+ Security, privacy – More account unlock calls to help desk
<b>Auditing</b>	Tracking user activity for security and HIPAA compliance.	– Potential privacy loss – Limited access	+ Security – Manual auditing slow

## Identity and Access Management

Administration—Managing User Accounts			
IAM Component	Description	Effect on End Users	Effect on IT Staff
<b>Delegated Administration</b>	Practice of granting limited administrator privileges to others.	+ Speeded access to resources – Potential privacy loss – Limited access	+ Speeds provisioning process – Costly, complicated to deploy
<b>Automated Workflow</b>	Process of automatically sending access approval forms to the correct managers.	+ Speeded access to resources	+ Replaces manual approval distributions – Costly, complicated to deploy
<b>Automated User Provisioning</b>	Automated process of setting-up and disabling user accounts in all enterprise resources.	+ Speeded access to resources	+ Replaces manual provisioning – Costly, complicated to deploy
<b>Meta-Directory</b>	Directory that integrates identities across multiple directories	+ Speeded access to resources	+ Replaces manual provisioning
<b>Virtual Directory</b>	Directory that aggregates identities across an organization for viewing.	+ Speeded access to resources	+ Facilitates viewing of users – Does not integrate or provision identities

Other IAM-Related Components			
IAM Component	Description	Effect on End Users	Effect on IT Staff
<b>Patient Context Management</b>	Technology that synchronizes applications to same patient, user.	+ Passing user context reduces passwords + Fewer patient selections – Disruption to normal workflow	– Costly, difficult to deploy
<b>(CCOW) Clinical Context Object Workgroup</b>	Standard developed to allow communication across clinical applications, now part of HL7.	+ Fewer patient selections – CCOW bugs can disrupt workflow	– Vendor compliance difficult
<b>LDAP</b>	Industry standard for querying directory. LDAP-aware applications use LDAP, not proprietary directory.	+ LDAP-Aware applications reduce passwords	+ No need to manage disparate directories – Building LDAP authentication difficult
<b>Physician Portal</b>	Browser-based site offering a combination of Web applications, terminal-served applications, and links to external websites.	+ Universal access + Unified view of data – Performance depends on connection, browser, security	+ No difficult client installation – Portal development potentially difficult
<b>Service Oriented Architecture</b>	IT model where Web Services interoperate, share authentication information, or are LDAP aware.	+ Universal access + Only one password – Performance and functionality depends on Web application	+ Central deployment of applications + Minimizes IAM – Building Web Services difficult
<b>Roaming Sessions</b>	User session travels from desktop to desktop run off Citrix or Windows Terminal Services.	+ Applications launched once – Performance issues with data- heavy applications	+ Central management of desktops – Costly, requires Citrix farm – Applications must be Citrix-enabled
<b>Public Key Infrastructure (PKI)</b>	Allow secure data exchange and digital signatures over the internet by issuing users digital certificates.	+ Secure access – Downloading certificate can be confusing	+ No device to deploy – Costly, difficult to maintain

Source: M-Tech, "Identity Management Terminology," available at: <http://idsynch.com/docs/identity-management-terminology.html>, accessed July 17, 2006; True North interviews and analysis.

