5 WAYS AN SSO SOLUTION CAN ASSIST WITH COMPLIANCE

WHITE PAPER

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

CONTENT

1. CHALLENGES OF MEETING COMPLIANCE NNEEDS

Compliance is a complex issue in many industries and organizations know all too well that there are major fines and potential punishments for not meeting the laws and regulations. Some major compliance regulations in the United States including *The* ***Health Insurance Portability and Accountability Act*** (HIPPA), *The Control Objectives for Information and Related Technology* (COBIT) and *Sarbanes Oxley Act* (SOX) require businesses to ensure certain standards within their organizations, including protection of data and full disclosure.

Several important HIPAA requirements include workstation security, access controls, audit controls, and person or entity authentication. HIPAA protects the use and disclose of patient data and ensures that healthcare organizations have the correct security measures in place. COBIT, which is published by the IT Governance Institute also provides "a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit control and security practitioners." In addition, SOX is a set of auditing accountability standards for all publicly traded companies in the United States.

2. ADDRESSING THE ORGANIZATIONS NEEDS

When looking at compliance needs there are several areas which organizations focus on and often have trouble complying with.

Some of the issues that organizations face in meeting compliance needs are:

- How to ensure that passwords aren't easily stolen.
- How to generate easy audit trails
- Ensuring that compliance needs are met within the budget of the organization
- Being able to easily track what each employee did on the company's network
- How to protect confidential company and customer data
- How to implement a solution which won't disrupt the organizations processes

Attempting to meet all of these requirements can be daunting, and implementing several solutions to help can become expensive. This whitepaper outlines 5 different ways implementing only a single sign on (SSO) solution can help your organization easily meet compliance needs. Organizations should look for these features in an SSO solution in order to receive the best results for their money.

3. 5 WAYS AN SSO SOLUTION CAN ASSIST WITH COMPLIANCE

1. EASILY ELIMINATING SHARED ACCOUNTS

Often in many organizations, especially in hospitals and in healthcare settings, employees have a shared account with other employees at the company. This means that they all login with the same credentials to access the systems and applications they need to perform their jobs. Many organizations are doing away with shared accounts though as a result of not being able to tell which employee did what while they were logged in. For compliance reasons, they need to be able to document what each employee is doing on the company's network. To meet HIPAA compliance they also need to be able to document who the user is and their role in the organization. This forbids any shared accounts or concurrent logons.[1] In addition, SOX compliance requires there to be 'segregation of duties'.

Simply eliminating shared accounts though can cause issues since employees will then have to remember several new sets of credentials for each system or application. A single sign on solution can mitigate this issue, and make the change from shared accounts to single accounts easier on the company and the employees. With an SSO solution, employees will still only be required to remember a single set of credentials, which is unique for each employee. This allows the organization to eliminate the shared account for compliance needs without drastically disrupting business procedures.

2. STRONG AUTHENTICATION

Ensuring that the data from your company and for your customers and patients is protected is another important part of compliance. Many data protection laws require organizations to have strong access controls in place. The 'Person or Entity Authentication' section of the HIPAA standard requires that organizations provide strong authentication in order to ensure that the person logging in is who they claim to be. The Sarbanes Oxley Act also requires publicly traded companies to ensure the security of their critical data, and states that "security and control around the application and data are critical."

A single sign on solution allows companies to implement strong authentication with 'two factor authentication. This ensures security by requiring the users to enter both a PIN code and a smart card in order to access the system or application. This means that they need something that they own, which is their smart card, and something that is known, which is the PIN code. Organizations can also add enhanced functionality for more security such as requiring the application to automatically be closed as soon as the smart card is removed. This is a feature which organizations should look for in an SSO solution in order to ensure the security of their sensitive data.

3. EASY AUDIT TRAILS

HIPAA requires a complete audit trail of all users at an organization. In addition SOX also requires all information about user's actions including document/data access, password changes, logins and logouts, and any changes made to be recorded.

1 SANS Institute InfoSec Reading Room

Organizations should implement an SSO solution where all end-user activities are logged in the central SSO database, as well as a copy of every user name and password is encrypted and stored in the central database. It should also report exactly which user accounts have access to what applications along with the dates and times access actually occurred. This allows organizations to go back later and easily have the information for audits. Additionally, according to SOX, audit records must be kept for seven years and must be secure as so not to be tampered with. The SSO solution should confirm that all confidential information is exchanged via secure methodologies.

4. SECURITY OF PASSWORDS

Ensuring that only the correct people have access to critical systems and data is a major part of complying with SOX and HIPAA. Often systems become non-secure when employees need to remember several passwords and resort to writing them down. This opens the possibility for those who are not authorized to gain access and for a security breach to occur.

To mitigate this issue, single sign on allows employees to eliminate their several sets of credentials and only need to remember a single user name and password. This in turn eliminates the need to write down their passwords in order to remember them. The solution can also be integrated with password reset software, to allow for password changes to be made periodically for applications that require it for additional security. When an application requests the entry of a new password after a period of time, the SSO software itself can generate and store a new password, without the employee having to do anything. Or, if desired, the SSO software can also prompt the end-user to create a new password manually.

5. PROPERLY DELEGATE AND REVOKE ACCESS

Often when an employee is sick or on vacation, another employee temporarily takes over their duties. In order to do this they are sometimes given their credentials which makes the network non-secure since they can then continue to login whenever they like unless the absent employee remembers to change their password upon return. If they do take the steps to securely delegate access, it is often forgotten to be revoked.

With an SSO solution, an employee can be given temporary user access rights for a set period of time, without being given the users credentials. After that specific period of time ends, the access is automatically revoked.

In addition, part of the HIPPA compliance states that upon termination, the company must have processes in place to revoke access to systems and applications. Revoking access for employees sound simple, but this task is often overlooked and employees are left active.

An SSO solution can also integrate with an account provisioning solution which allows system admins to easily disabled employees with one click. This ensures that the ex-employee no longer has access to the organizations systems and applications.

Example of an SSO Implementation Situation

Consider a healthcare organization which has 500 employees who use at least 10 different systems and applications each. In addition, the company deals with confidential customer data, which only certain employees should have access to.

Problem: Many of the employees have trouble remembering their credentials to all the systems and applications so they write them down. Several employees also share one set of credentials to some of the systems, which makes it impossible to track who is taking what actions. The organization wants to eliminate the shared accounts but does not to give the employees additional credentials to remember. In addition, the employees are in and out of rooms all day and often accidently leave themselves logged in.

Solution: An SSO solution is implemented in conjunction with two factor authentication. Employees now only have to remember their PIN code and swipe their pass along the card reader in order to gain access to all their systems and applications. Then once they remove their cards and go to another room they are automatically signed out. This allows users who have opened applications to easily move to another workstation and continue their work, which in turn allows them to be more efficient.

Result: The organization can now clearly see which employees are doing what on the network. In addition, the employees no longer have to write down their credentials. Overall, the organization has greatly increased the security of their network.

4. CONCLUSION

Ensuring that your organization meets audit needs, within your budget can be a difficult task. With the correct SSO solution, organizations can greatly improve their security while at the same time meeting compliance needs and staying within their budget. With an SSO solution organizations will also be able to eliminate some of the many hours that there IT staff spend on ensuring the security of systems, and allow them to focus on other important tasks.

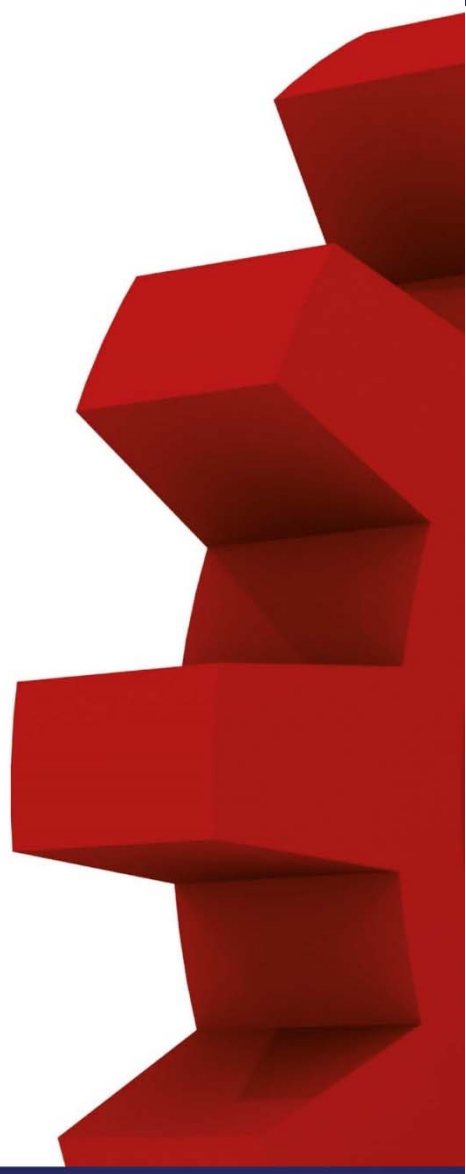
In addition to helping with compliance, SSO can also offer additional benefits to your organization. It allows employees to work more efficiently since they do not have to login with several different sets of credentials for each system and application. It also provides these benefits for those employees who are working remotely and are working outside the organizations network.

Providing Audit Trails of Employee Actions	Eliminate shared accounts as well as securely store all actions taken by employees on the network
Ensure Passwords aren't stolen	SSO provides the ability to remember a single set of credentials, so employees no longer write them down
Strong Authentication	Two Factor Authentication-With a smart card and PIN code
Workstation Security	Eliminate shared accounts- Two Factor Authentication- Lock workstation once user walks away

About Tools4ever's Enterprise Single Sign-On Manager:

Tools4ever's Enterprise SSO Manager (E-SSOM) is an organization-wide Single Sign On software solution enabling end-users to log in just once, after which access is granted automatically to all of their authorized network applications. E-SSOM includes SSO, two-factor authentication, Authentication Management and Follow-Me. E-SSOM makes automatic login possible.

To learn more about how Tools4ever Enterprise Single Sign-On Manager can help with compliance visit: https://www.tools4ever.com/software/enterprise-single-sign-on-manager/



Eastern US

300 Merrick Road, Suite 310
Lynbrook, New York 11563

T +1-516-482-4414

Sales nasales@tools4ever.com
Support support@tools4ever.com

Western & Central US

PO Box 8200
Bonney Lake, Washington 98391

T +1-888-770-4242

Sales nwsales@tools4ever.com
Support support@tools4ever.com