Improving Information Security by Automating Provisioning and Identity Management
INTRODUCTION

Many healthcare security professionals understand the need to enhance their security and privacy strategies, however, they are constrained by resources such as budgets and qualified personnel. There’s a constant tension between the need to implement new tools and processes with not having enough resources to execute those strategies. The key to resolving this tension is to find strategies that can improve the ability to maintain a heightened level of security in an efficient manner that doesn't burden IT staff.

Access risk is an example of a vulnerability where better security aligns with improved efficiency. It’s getting more challenging to manage “access” with frequent industry consolidation and the emergence of population health. Data is now being shared from a wide variety of applications with an increasing number of clinicians who need efficient access. Managing this risk is further complicated because it has multiple layers such as elevated privileges, remote and mobile access and multi-factor authentication.

Access management solutions such as single sign-on (SSO) are often looked upon as the first line of defense in controlling identity and access risk. However, providers need more than just SSO. They need their SSO solutions to work in conjunction with identity management solutions in order to improve inefficient processes that are burdening staff and creating risk.

NEW AFFILIATIONS, FLUID WORKFORCE, MORE DATA
THE BUSINESS CASE FOR AUTOMATED PROVISIONING AND IDENTITY MANAGEMENT

Larger organizations are allocating thousands to tens of thousands of staff hours in manual provisioning and identity management processes. Additionally, with the average cost of a breach being nearly $4 million, there is a strong business case for the investment in automated provisioning and identity management. An average sized healthcare organization will allocate four to six employees that must dedicate a considerable percentage of their time on manual provisioning and identity management processes. With automated provisioning and identity management, as much as fifty percent of that time can be reallocated to other value-added responsibilities. Also note that even if your current SSO vendor does not offer provisioning and identity management solutions, it can be integrated with third-party provisioning and identity management tools.

MANUAL PROCESSES CREATE RISK AND BURDEN STAFF

Let's explore the challenges of manual provisioning and identity management processes further. Below are five critical identity management activities required to control access risk that providers often address with time-consuming manual processes.

1) Provisioning and deprovisioning

When a large number of new employees start with an organization due to a merger, the process of provisioning those employees can take hundreds to thousands of valuable IT hours. While Active Directory scripting can automate some pieces, provisioning and deprovisioning access to all applications is a burdensome process. IT staff often have to manually make changes in every application, but the problem goes deeper. For deprovisioning, it is not safe to assume IT knows which applications that a user has access to. Employees often change roles or departments over time. They can accumulate different rights and never give any back. Over the course of ten to fifteen years, the accumulation can be significant. It's a risky practice to remove access to applications based on the employee's most recent job description, which can lead to orphaned application accounts. This puts organizations at risk for audits (e.g. The Joint Commission - JCAHO, HIPAA) that require the documentation and execution of security and privacy policies and controls.

2) Gathering the data needed to evaluate potential threats

Investigation of potential threats is another core identity management activity where manual processes are detrimental. When an organization becomes aware of potentially suspicious access behavior, they have to ask a number of questions in order to investigate the potential threat.

- Who is the user?
- What should the person have access to?
- What does the person have access to?
- What are they actually looking at?
For IT staff to answer these questions, they must often be pulled from other key activities (e.g. new application setup) to log in to many different systems in order to research and gather the required information. This is not only a time-consuming task, but also slows down the process to evaluate and remediate threats.

3) Proactive identification of access risk

It is possible to proactively reduce access risk by identifying users with mismatched entitlements or by identifying orphaned application accounts. However, this typically requires the manual creation of a report by multiple staff members who are each responsible for a specific set of applications. After the information is consolidated, it is typically emailed to management or posted on an intranet where it quickly becomes out of date. Due to the inefficiency of the manual steps, providers often don’t have the bandwidth to engage in the proactive identification of access risk.

4) Remediation

In order to respond to a potential threat, suspending or removing unauthorized access should ideally be a near instantaneous process. However, that’s not the case for most organizations because of the quantity of applications a user may have access to. IT staff typically have to go into each application separately to remove access, which hinders responsiveness.

5) Entitlement attestation

Manual attestation processes entail IT going into each individual application separately to gather the necessary information, then send to department managers for review. The process is so cumbersome that some providers are only able to perform user entitlement attestation for their most important clinical applications. This creates serious risk of failing a HIPAA audit.

MANUAL PROCESSES CREATE RISK AND INEFFICIENCY
AUTOMATION IS THE ANSWER

The key to successfully mitigating access risk through increased due diligence is to leverage automation, which enables providers to proactively manage credentials and access rather than just reacting. With the exploding number of applications and clinicians that must be managed, healthcare organizations must automate access related processes because manual processes are actually creating risk and consuming too much valuable resource time. Here are the ways in which automation reduces access risk.

Provisioning and deprovisioning

Setting up a role-based security model (i.e. proactive role definition and tracking of current access privileges) greatly simplifies provisioning, deprovisioning and role change processes. Integration with an HR or credentialing system can be leveraged to employ fully automated provisioning and deprovisioning, or the process can be partially automated to allow for approvals. It can also include attribute-based role definitions for precise access rights management.

Single view of the data needed to evaluate and remediate potential threats

By integrating SSO and provisioning and identity management tools, you can automate the process of gathering all the data needed in order to evaluate and remediate potential threats. With a combined view of user entitlement and user behavior data (e.g. who logged into a workstation, where did they log in from, what applications were launched, what do they have access to) from all applications easily available, security can take the appropriate action faster on potential threats.

Governance, Risk Management and Compliance (GRC): Proactive identification of access risk

By leveraging automation, providers can shift from a reactive to a proactive approach that is aligned with an overall GRC strategy. A GRC dashboard for access risk can be populated by reports that identify potential access risk such as orphaned application accounts or mismatched entitlements. Near real-time alerting based on configurable rules can also be used to notify security staff of a potential issue as it is happening.

Simplified remediation

With automation, it should only take a few clicks to remediate and instantly remove or suspend access from all applications.

Entitlement attestation

Entitlement reports that detail users and what they have access to can be pre-assigned to the appropriate managers so they can easily verify or make changes. Any changes that need to be made are made automatically without manual intervention.
## Automating Provisioning and Identity Management

<table>
<thead>
<tr>
<th>Provisioning and Identity Management Process</th>
<th>Before Automation</th>
<th>After Automation</th>
</tr>
</thead>
</table>
| Provisioning and deprovisioning             | Logging into every application separately  
No visibility into current access and privileges | Proactive tracking of current access and privileges  
Pre-defined attribute based role definitions  
Integration with HR/credentialing system  
Automated provisioning and deprovisioning | |
| Gathering info to evaluate a threat         | Logging into multiple applications separately to gather information | Integrated SSO and provisioning and identity management brings together user entitlements and behavior data  
Instant visibility into who the user is, what they have access to and what they are actually looking at | |
| Proactively identifying access risk         | Logging into every application separately to gather data  
Manually generate aggregate reports  
Email to management | Pre-defined reports on a GRC dashboard regularly refreshed with updated data  
Managers are given appropriate access to the dashboard and reports based on actions they need to take  
Near-real time alerting of potential threats as they happen | |
| Streamlined remediation                     | Multiple staff members logging into applications separately to remove access | One staff member removing or suspending access to all applications in a few clicks in a few seconds | |
| Entitlement attestation                      | Multiple staff members logging into applications separately to generate reports  
Manual aggregation of information and sending to managers  
If managers send back any adjustments, they have to be made manually in each application | Pre-defined reports are pre-assigned to appropriate managers for review  
Automated updates to access or entitlements | |
CONCLUSION

Given the increased threats healthcare faces today, the industry needs to enhance its approach to access risk. Ultimately, today's SSO solutions are not enough by themselves. The key is greater due diligence and a proactive approach, day in and day out. This requires SSO tools to work in conjunction with provisioning and identity management tools, which delivers the automation needed to improve both security and IT efficiency.
ABOUT US

Caradigm delivers the industry’s only end-to-end identity and access management solution that reduces risk across the entire governance, risk and compliance (GRC) lifecycle.

Built exclusively for healthcare, Caradigm’s integrated solutions address the operational challenges of access to clinical applications while protecting you from increasing security and compliance risk by safeguarding access to patient health information.

Provisioning Identity Management, a role-based identity management solution, automatically creates, modifies and terminates access to clinical applications. This improves clinician satisfaction by giving caregivers rapid access to the applications and data they need.

Single Sign-On (SSO) enables your clinicians to use a single set of credentials—entered once per session—and multi-factor authentication in an integrated clinical workstation. They can access applications quickly without signing on to each one separately.

Clinical Access Governance enables a healthcare organization to respond to increasing security and compliance risk by safeguarding patient health information. Governance capabilities are implemented through controls, automation, and analytics.

Clinical Application Integration leverages Caradigm’s extensive clinical application library, allowing Provisioning and SSO connectors to be created for hundreds of applications from vendors such as Epic, Cerner, GE, and McKesson.

Context Management maintains patient context across applications, allowing automatic access to the right patient record as clinicians move from system to system. This saves time and increases accuracy.

Password Management enables password synchronization across systems and clinical/business applications. Synchronization allows password changes to be propagated to all target systems and applications. These powerful coordination capabilities minimize the password management pains that users struggle with between applications and systems.

EPCS Authentication streamlines clinical workflow of electronic prescriptions for controlled substances (EPCS) and simplifies the two-factor authentication imposed by the DEA and state regulations. The required strong authentication is seamlessly built into the electronic prescribing workflow while providing an optimal experience for the clinicians.