November 2024

Privileged Access Management: A Guide for Healthcare CISOs

TLP:WHITE This report may be shared without restriction.

Health-ISAC™
Collaborating for Resilience in Healthcare

health-isac.org

Contents

Scope Statement

Identity and access management systems manage the virtual front door for healthcare organizations. On one side, you have the employees, caregivers, and others who need access to a range of applications to do their jobs. On the other side, you have the patients who are using different portals and applications to reach out to physicians, request medications, and make appointments. But there is also a third side to this identity triangle: Privileged Access Management (PAM).

In previous white papers, A Health-ISAC Framework for CISOs to Manage Identity and Identity and Zero Trust: A Health-ISAC Guide for CISOs, we outlined a framework to help healthcare organizations manage identities. As we focus on PAM, we have updated the framework to show where privileged access fits in and the components this security technology impacts; we have also made some additions to the framework.

While enabling secure and simple access to systems is a goal of identity and access management for the workforce and patients, PAM purposely adds friction to the process to ensure the greatest possible security. Information and resources protected by PAM are an organization's most critical resources. A separate, higher security system is necessary for these systems as unauthorized access could mean exfiltration of critical data and compromise of networks and applications. To put it simply, the compromise of privileged accounts would be devastating to a healthcare organization.

In healthcare, PAM can protect a range of information, such as medication formulas, network and system administrator access, and database administrator access. Typically, access is highly restricted and only a small percentage of an organization's workforce accesses the PAM.

These systems are critical for healthcare organizations to help them protect their "crown jewels" and ensure secure access to privileged accounts.

Key Takeaways

- **How PAM** is different from an organization’s other identity and access management systems.
- **How PAM** fits into the Health-ISAC Framework for Managing Identities.
- **How PAM** can help secure the most critical workflows for healthcare organizations.
- **The challenges** that can arise with PAM systems for healthcare organizations.

What is PAM?

PAM is not just one application, but rather a series of products and services that enable a healthcare organization to have greater control over who accesses sensitive systems and data, both on premise and in the cloud. These components include:

Component	Description
Privileged session management	Privileged session management is a capability within a PAM tool that enables organizations to monitor, record, and control sessions for high-risk accounts in real time, providing enhanced oversight and security over critical systems accessed by privileged users. This feature helps prevent unauthorized actions and enables forensic analysis by capturing session activities for compliance and auditing purposes. PAM pairs multifactor authentication (MFA) to access the system. Typically, MFA for PAM is another modality that is separate from other access privileges. Often, organizations will use separate FIDO hardware security keys in these instances.
Least privilege enforcement	Ensures that devices, users, and applications should only have the minimum privilege to perform a task.
Password vault/ manager	Many of the systems and applications tied to PAM systems require passwords for access and may not easily integrate with MFA. The PAM password manager enables an organization to monitor, manage, and protect access to those privileged accounts. When an individual needs to access the account, they “check it out” from the PAM system, perform the necessary tasks, and then check the account back in. Once checked back in, the PAM system will rotate the password so that the password will no longer be valid. Changing the password will help protect the account in case a keylogger was present or someone attempts to phish the password later. The vaults also can change the password on a regular basis depending on risk and regulatory requirements.
Privilege delegation/ Just-in-time provisioning	Enables non-administrators to temporarily access sensitive systems and resources on a time-limited basis. Individuals will request additional access for a set period and then have the privilege revoked.
Access control	Establishes access control rules and requirements for access to PAM systems.

PAM providers can also have applications that identify and inventory privileged accounts, classify the accounts based on risk, and establish governance of privileged accounts. PAM also typically includes a governance function for those using the system with frequent certifications to make sure only appropriate individuals can access the systems.

It will also help organizations enforce least privilege and separation of duties. Implementing a PAM system should include a review of the roles and responsibilities of individuals who access these privileged systems with the goal of ensuring that only those who need access to these systems have it.

PAM will also help an organization implement separation of duties. This security tenet makes sure that individuals cannot approve their own transactions and that there are clear lines showing who can approve access to resources from those requesting access.

PAM Risk Assessment

Typically, before implementing a PAM system, an organization will look at the distinct types of accounts and create tiers based on risk. A sample may look like this:

Tier #	Description
Tier Zero	These accounts will be the highest risk and include system and network administrators. Access is only available through a designated PAM workstation that does not have email or web browsers. The PAM monitors and logs the session and devices are frequently wiped and reformatted.
Tier One	Access for some systems and application administrators.
Tier Two	Just-in-time access for workstations and employees who need to review sensitive information. Medical device administration could also fall under Tier Two.

Tier Zero and Tier One accounts may only be accessible through dedicated PAM workstations. These devices do not have web browsers or emails, so information from them cannot be easily exfiltrated. In certain cases, these devices undergo periodic reformatting to ensure that data is not stored on the devices.

PAM and the Health-ISAC Framework for Managing Identities

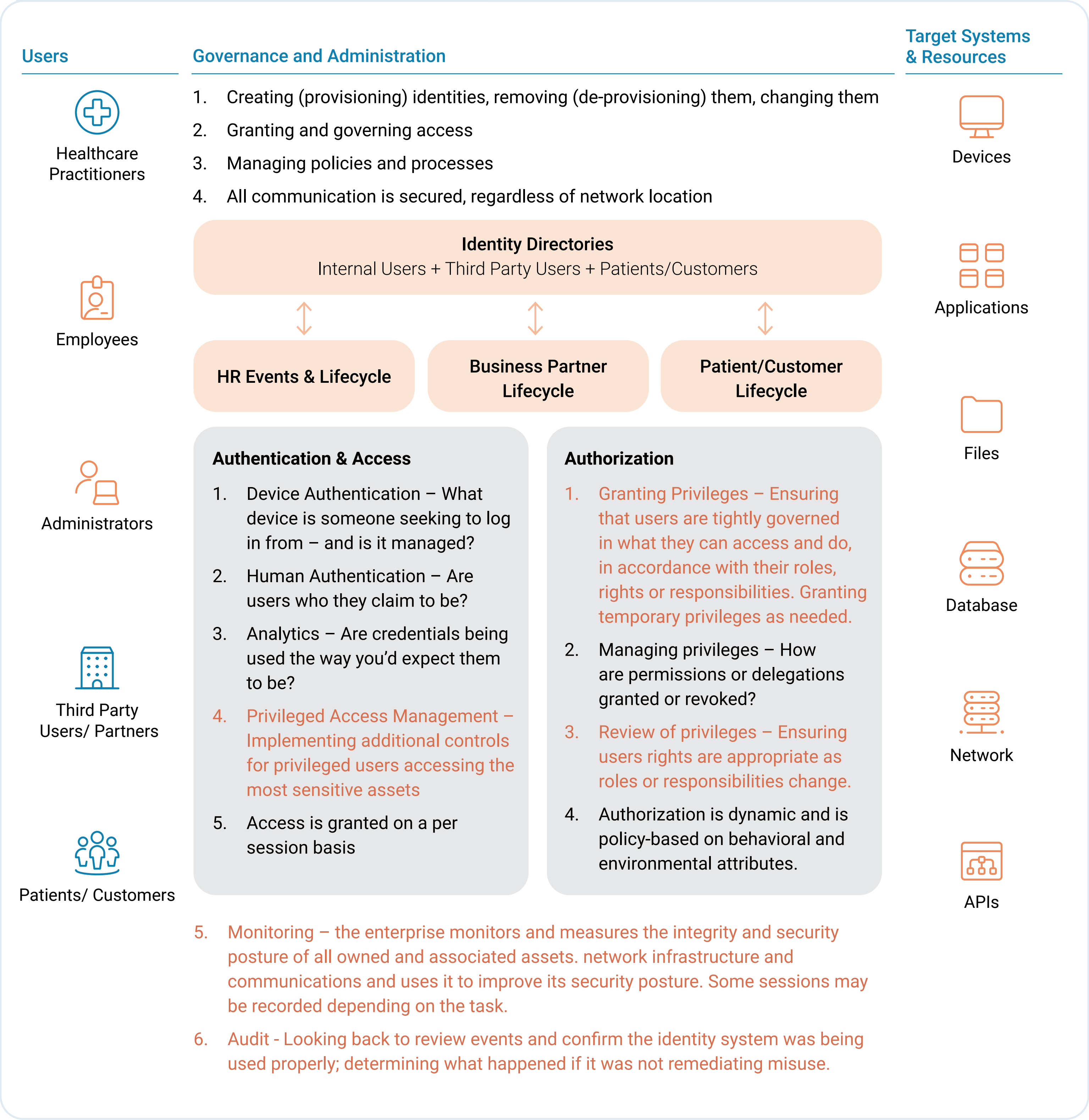
In 2020 Health-ISAC released A Health-ISAC Framework for CISOs to Manage Identity. It explained how to architect different identity and access management (IAM) solutions to enable an enterprise to manage the full identity lifecycle of employees, practitioners, patients, and business partners in a way that guards against common attacks on identity, materially lowers risk, and increases operational efficiencies. In 2022 the framework was updated to account for a zero trust architecture.

This paper revisits that framework and updates it with PAM in mind. The changes – shown in orange – incorporate additional controls to deliver core elements of PAM. The major changes include:

- Addition of administrators to the user column – and highlighting that temporary access may be granted to employees if certain access is needed.
- Highlighting PAM in the authentication and access category.
- Spotlighting that PAM may grant temporary authorization to materials as needed under authorization while also showing that PAM can perform privilege reviews.
- Adding more monitoring and audit capabilities for PAM. Depending on what is being done within the PAM the system may record the interactions.
- Inclusion of network to target systems and resources.

The new framework highlights all the targets and resources. This impacts the administrators of these systems – not all users.

An H-ISAC Zero Trust Framework for Managing Identity



Users

Healthcare Practitioners

Employees

Administrators

Third Party Users/ Partners

Patients/ Customers

Governance and Administration

1. Creating (provisioning) identities, removing (de-provisioning) them, changing them
2. Granting and governing access
3. Managing policies and processes
4. All communication is secured, regardless of network location

Identity Directories
Internal Users + Third Party Users + Patients/Customers

HR Events & Lifecycle

Business Partner Lifecycle

Patient/Customer Lifecycle

Authentication & Access

1. Device Authentication – What device is someone seeking to log in from – and is it managed?
2. Human Authentication – Are users who they claim to be?
3. Analytics – Are credentials being used the way you'd expect them to be?
4. Privileged Access Management – Implementing additional controls for privileged users accessing the most sensitive assets
5. Access is granted on a per session basis

Authorization

1. Granting Privileges – Ensuring that users are tightly governed in what they can access and do, in accordance with their roles, rights or responsibilities. Granting temporary privileges as needed.
2. Managing privileges – How are permissions or delegations granted or revoked?
3. Review of privileges – Ensuring users rights are appropriate as roles or responsibilities change.
4. Authorization is dynamic and is policy-based on behavioral and environmental attributes.

5. Monitoring – the enterprise monitors and measures the integrity and security posture of all owned and associated assets. network infrastructure and communications and uses it to improve its security posture. Some sessions may be recorded depending on the task.
6. Audit - Looking back to review events and confirm the identity system was being used properly; determining what happened if it was not remediating misuse.

Target Systems & Resources

Devices

Applications

Files

Database

Network

APIs

PAM Use Cases in Healthcare

Access to Service Accounts and Non-Human Accounts

Across all markets and sectors, service accounts are challenging to manage. Whereas a user account identifies a person, a service account is a non-human privileged account that an operating system uses to run applications, automated services, virtual machine instances, and other background processes. A service account assigns an identity and permissions to a computer program or process that performs a specialized task. These accounts have privileges that enable extensive access to system resources, either locally or across a domain.

These accounts are also typically used by multiple employees across an enterprise and passwords are shared amongst those several system administrators. They also typically do not include MFA. This is why it is imperative that the PAM manages service accounts so access can be logged and monitored to individual admins as well as enabling MFA. When it comes right down to it, if an attacker obtains access to service accounts, they can wreak havoc because of their escalated privileges.

PAM can protect access to service accounts. The account needs to be identified and then access regulated via the privileged access system. Employees would access PAM, use the requisite MFA, and the session should be logged and monitored while accessing the system. The password vault would store the complex password and then change it after the session is complete.

One of the challenges with this use case is identifying the service accounts in use within an enterprise. Often, the PAM vendor can help with this task, but, depending on the size of an enterprise, it could have hundreds, if not thousands, of service accounts.

Healthcare organizations should use phishing-resistant MFA. Nowhere is this more imperative than with PAM.

Admins are often the target of spear phishing attacks as their accounts enable attackers to escalate privileges quicker than a typical user. Organizations spoken to for this paper were using separate security keys for PAM access rather than the same authenticator technology used for normal access.

In past papers, Health-ISAC has highlighted the importance of phishing-resistant authenticators.

Medical Device Management

Healthcare organizations have hundreds to thousands of medical devices that run on different software platforms that typically feed into a central system in hospitals. Managing these devices can be challenging as they produce a large amount of personal health information that needs to be protected.

When it comes to these devices and the data produced, it is important to know who is managing them from a security, compliance, and regulatory perspective. Typically, these devices come with default passwords, which need to be updated, so organizations need to make sure they change these. Once changed, the PAM should manage access to these devices. The administrator accounts for these devices should be under an organization's PAM, as the devices and systems are connected to other healthcare systems. If an administrator account were compromised, it would be possible for an attacker to escalate privileges and move throughout a healthcare organization's network.

Using PAM for medical device management administrator accounts will help organizations comply with regulatory and compliance requirements while also protecting other systems from attack.

Just-in-Time Provisioning

Network and application administrators will use PAM frequently to make the necessary updates to their systems. But with PAM also protecting an organization's "crown jewels," others may sometimes need access to data that with the privileged management tool.

Just-in-time provisioning is a concept where a user does not have persistent access to a resource until they have a need to make a change or access specific data. PAM can enable just-in-time access to specific information or data for individuals without granting access to the entire system.

PAM's tools enable Just-in-time provisioning by allowing users to gain access to specific information only for a set period. The individual will request access to the resource and, if granted, will receive information to access it via the PAM system using an account that already has access. For example, access for an individual needing to review a drug formula is granted for a set window, with additional restrictions on what they can do during that session. When the session window closes, access is revoked. This minimizes the number of accounts that need to have access to a resource.

Once accessed, the session will be logged and monitored. Certain functionality may be disabled during the session, too, such as copy, cut, and paste commands, email applications, and outside internet access. After the session is complete, the password and access to the resource will be changed so the information cannot be used again for access.

Steps to Help Ensure a Positive PAM Rollout

PAM implementations are not simple. Performing the risk assessment and identifying the accounts that should be protected by PAM alone is a process that can take some time. Having an inventory of administrator accounts before the PAM implementation begins can be a helpful first step in the process.

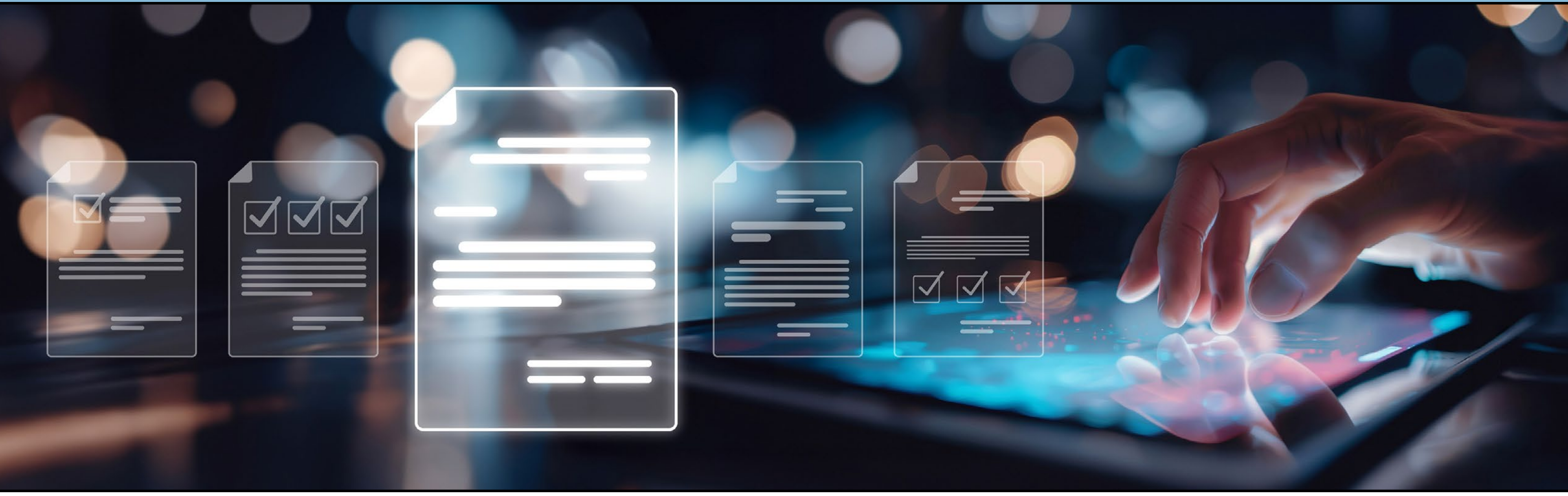
One organization we interviewed as part of the research for this whitepaper has been on its PAM journey for nine years and is still bringing on new components and adding accounts and applications. Implementing the system is just the start; it is then followed by a process of making sure new accounts and services are onboarded appropriately as PAM evolves in the organization.

PAM providers are also rolling out new components to help healthcare organizations secure systems. Securing non-person and service accounts is a new function, which is requiring organizations to identify those accounts and bring them under the PAM.

When it comes to moving the accounts into PAM, the process can take years. Part of the challenge is identifying accounts that need to be protected by PAM and then convincing the account holders that the systems need that level of protection. Since PAM adds friction to the process the business owners of these applications may be hesitant to bring them under the PAM. Having leadership support throughout the process is critical. To generate this support, it is important that the PAM team have metrics that show the number of accounts protected via PAM, the number of administrator accounts, and frequency of system use.

There will be pushback from employees in the organization who do not want to request access to certain data through the PAM system every time they need it. Since PAM adds friction to the process, and only gives individuals a limited window, users may not like going through the steps to access the data. To counter this, leadership buy-in is critical. The CISO and security staff need to discuss with leadership the critical nature of PAM and embed it into the security culture of the organization.

Lastly, PAM needs redundancy. While these systems are typically cloud-based and there are aspects of redundancy, if the entire internet is cut off to an organization, additional steps should be taken to maintain resiliency. As an example, one institution we interviewed has passwords in a locked physical vault in case of a catastrophic incident.



Conclusion

Only a small percentage of a healthcare organization's workforce may ever touch a PAM system. That does not make it any less critical than workforce or patient identity and access management systems. PAM is the equivalent to the bank vault, controlling access to the most critical resources and information an organization owns. Taking a phased approach to rollout is critical, identifying the accounts and systems that need protection, and expanding the scope from there.

This paper represents the ninth in a series of Health-ISAC papers designed to introduce CISOs to an identity-centric approach to cybersecurity. By providing an explanation of concepts, outlining a framework, use cases, and best practices for rolling out different identity systems, Health-ISAC intends to provide holistic guidance to assist CISOs in their approach to various aspects of identity and access management and managing risk.

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org.