April 2020

# WHITE PAPER

## AN H-ISAC FRAMEWORK FOR CISOs TO MANAGE IDENTITY

H-ISAC™
HEALTH - ISAC

www.h-isac.org

# AN H-ISAC FRAMEWORK FOR CISOs TO MANAGE IDENTITY

## ABSTRACT

Our first paper *"Identity for the CISO Not Yet Paying Attention to Identity"* detailed why healthcare CISOs need to embrace an identity-centric approach to cybersecurity – including where and how to get started.  If you've read it, perhaps you've been convinced that identity should be a priority.

But what does that mean, and how should you get started?  This paper was written to address those questions.  It outlines a comprehensive Framework that health CISOs can use to architect, build and deploy a modern identity system that will protect against modern attacks and also support key business drivers.

## INTRODUCTION

*"Identity for the CISO Not Yet Paying Attention to Identity"* explored how technological evolution and organizational shifts have fundamentally changed how businesses operate, how traditional cybersecurity approaches are no longer adequate to meet today's threat environment, and how a radical rethinking of cybersecurity has led to an emphasis on identity-centric security solutions.

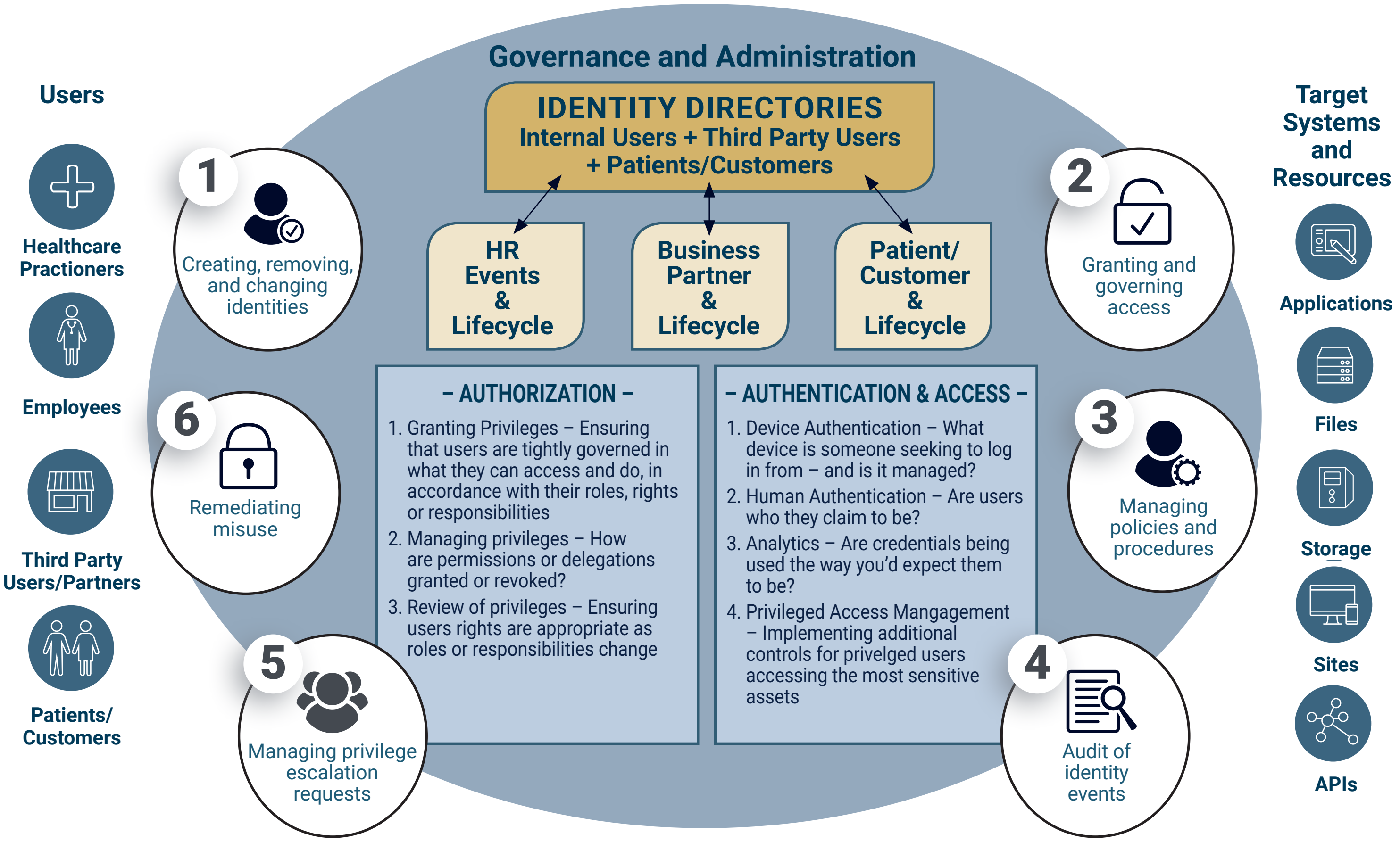
That paper outlined four key takeaways:

1. Identity matters. It's where attackers focus, making it imperative that defenses are oriented around identity. With the explosion of cloud, mobile, and BYOD, organizations have reduced control of their endpoints, elevating the importance of identity.
2. Identity is not just about internal workforce; it's about an organization's entire ecosystem including customers and external partners.
3. Identity should be owned and operated by an organizational function motivated by risk (e.g., the CISO), not one motivated by service levels and speed (e.g., the Service Desk or HR).
4. CISOs should use an identity-centric approach to cybersecurity.

You already use some Identity and Access Management (IAM) tools today.  Authentication, provisioning, authorization, and access control – these are all important technologies on their own. When treated as point solutions and deployed in isolation, they fail to deliver a holistic approach to identity that can protect against identity-centric attacks.

When integrated as part of a more holistic Framework, however, these solutions and others 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.  The Identity Framework that follows details the different components needed for a modern identity-centric approach to cybersecurity, and outlines how these different components should integrate and inter-relate to secure the enterprise.

## An H-ISAC Framework for Managing Identity


Users
Healthcare Practioners
Employees
Third Party Users/Partners
Patients/ Customers
Governance and Administration
IDENTITY DIRECTORIES
Internal Users + Third Party Users + Patients/Customers
HR Events & Lifecycle
Business Partner & Lifecycle
Patient/ Customer & Lifecycle
1
Creating, removing, and changing identities
2
Granting and governing access
3
Managing policies and procedures
4
Audit of identity events
5
Managing privilege escalation requests
6
Remediating misuse
Target Systems and Resources
Applications
Files
Storage
Sites
APIs

– 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
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

– 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 Mangagement – Implementing additional controls for privelged users accessing the most sensitive assets

The Framework is designed to be flexible and is agnostic to the size, structure, and other particulars of your organization. Importantly, the Framework is not designed to prescribe specific solutions or products; while certain controls or solutions may be referenced in the use cases, they might not apply to your organization.  Every CISO should assess her organization's resources and unique risks to determine how to best apply the Framework.

**We strongly recommend that IAM services, including the provisioning and deprovisioning of access, be performed within the security function, separate from shared IT services such as the help desk or infrastructure operations.** This ensures that access and authorization maintain a healthy tension with availability, and that one of the integral elements of protecting critical data and resources is not unwittingly sacrificed for temporary and potentially less valuable interests.

# BREAKING DOWN THE FRAMEWORK

At its core, the Framework revolves around a simple concept:  how to enable users – be they employees, third party partners, or patients – to access resources in a way that protects against attacks while also being easy to use and administer.

At the heart of the Framework is a focus on Governance and Administration.  Other elements (Directories, Authentication and Access, Privilege Access Management (PAM), etc.) are tucked inside the Governance "box" to make clear that they cannot be deployed in isolation; each element is most effective when it is one component of a broader Identity and Access Management system. For example, some organizations have rushed to install PAM solutions without integrating them with systems that provision and govern identities and accounts – creating gaps in the visibility and security model of the overall IAM system.

That is not to say that all elements of an IAM system need to be deployed all at once, however – such an approach is neither practical, nor affordable for most organizations.  What is most important that organizations embrace an architecture that places identity at the forefront and integrates components into that architecture to ensure that all components are part of a bigger system.

# FRAMEWORK COMPONENTS

This section of the paper will walk you through the Framework's sections, outline those sections' interrelationships, and provide a detailed breakdown of the component parts.

## Governance and Administration

As we noted above, the H-ISAC Framework is rooted in Governance and Administration; these tools are the "nervous system" that tie all of the other components together and ensures all parts are working in concert with each other.   Note that when we talk about "governance" in this section, we talk not about the broader need for governance across an organization, but rather the specific systems that are used to manage and enforce it.  Identity Governance and Administration (IGA) systems extend across the full lifecycle of an identity and ensure that each component is working toward a broader goal.

### DEFINITIONS:

- **Provisioning: Granting of accounts, credentials and permissions to enable access**
- **de-Provisioning: The disabling or revoking of access**
- **Audit: A review of logged events to detect misuse or anomalies**

An Identity Governance and Administration (IGA) system allows an organization to establish firm rules and processes to:

- Create (provision), remove (de-provision), and change/update identities – along with the accounts that are associated with them
- Grant and govern access, and recertify those access decisions on a regular basis
- Manage the policies and processes used to govern all aspects of the IAM system, such as how authorizations to access resources are updated as roles or attributes change
- Manage privilege escalation requests
- Audit what happened when something goes wrong, or for compliance purposes
- Take action to remediate any misuse of IAM systems, including blocking or revoking access when potential misuse is detected

## Identity Directories

If the Governance and Administration solution is the “nervous system” of an IAM system, Directories are the “heart.” A directory provides the authoritative identity store for an organization – providing details about each identity including the roles, accounts, attributes, and privileges that go with them.

While it’s important for the CISO to own identity (as noted in our previous paper), directories are one component of an IAM system that will need to closely integrate with other elements of the enterprise – both on a technical and a governance level.

- Employees will need to integrate with authoritative sources owned by Human Resources (HR), given that the journey to employment (or termination) starts there. As a CISO, your IAM team must be very tightly partnered with the HR function. HR also must trigger employee identity lifecycle changes to the IAM team, as employees change jobs or are terminated. It’s very important to confirm accountabilities in this area, especially when considering contingent workers and outsourced partners.
- Third Party Business Partners and Contractors may be tied to authoritative sources owned by product teams, operations, or other elements of the business. For contingent workers and third-party service providers, it’s imperative that notifications of job changes and/or terminations are made in a timely manner so access controls can be adjusted or deactivated accordingly.
- Healthcare Practitioners may be employees or third parties. A physician, for example, may be credentialed in multiple facilities or health systems.
- Patient and Customer identity is generally viewed as a customer-facing function – and onboarding or termination of customers will be driven from the perspective of a public-facing system.

Given the multiple situations where an identity might be created, modified, or removed thanks to a driver from another part of the enterprise, it's important that your directories (and the governance process around access to them) be integrated with key identity lifecycle events.  This is reflected in the Framework.

**After an identity is created, the next most important questions are:**

***1. What is that identity allowed to access or do?***

***2. How is access secured and granted?***

**Authorization answers that first question;**
**Authentication and Access answer the second.**

## Authorization

Authorization is the process of determining what privileges a user should be granted based on his roles, rights, and responsibilities. Authorization is closely tied to the Governance and Administration function, as all authorization decisions need to be rooted in governance.

Key elements of authorization include:

- **Granting Privileges –** Users should be tightly governed in what they can access and do, in accordance with their roles, rights or responsibilities
- **Managing privileges –** Authorization is rarely static. As circumstances change, there needs to be a firm process for permissions or delegations to be granted or revoked
- **Review of privileges –** As roles or responsibilities change, user rights should be reviewed to ensure that users are restricted only to the privileges needed.

### DEFINITIONS:

- o **Authorization: allowing or disallowing access based on attributes, groups, roles, etc.**

## Authentication & Access

After an identity is created from an authoritative source and permissions are authorized, you can now turn to authenticating the user and granting him access to systems and resources.

Once upon a time, this involved nothing more than a password.  As attacks on passwords have increased – and their security utility has diminished – authentication and access now typically layer in several tools.

Passwords still may be needed in some environments, though the H-ISAC recommends the use of multi-factor authentication (MFA), given how easy it has become for hackers to compromise a password.

Our Framework goes a step beyond MFA, however, to recommend a multi-layered approach that enables continuous, risk-based authentication. It is based off of the following components:

- ***Device authentication*** can be a valuable tool for authentication and access in three scenarios:
  1. If a PC, smartphone, tablet, or device has been issued by your organization
  2. If the device is not issued by your organization but is managed – through Mobile Device Management (MDM) or a similar capability
  3. If a customer device has been used previously and can be determined to be "trusted" to an acceptable extent

  Device authentication answers a simple question: before I think about letting a person (or service) try to access my organization's resources, are there things I know about the device they are using? Device authentication typically relies upon a certificate or browser cookie, but may use other tools as well.

- ***Human authentication.*** Once a device is authenticated, it is important to verify that the person trying to access the resources associated with an account is the person to whom that account was issued.

  Passwords may play a role here, as part of a broader MFA authentication solution that uses a combination of knowledge-based (i.e. passwords), inherence-based (i.e., biometrics) and possession-based (i.e. security keys or certificates on a device using the FIDO standards).

- ***Analytics*** are increasingly used alongside traditional authentication – to continuously evaluate whether credentials are being used the way you'd expect them to be. For example, if a credential used in New York to login to a resource is then used an hour later to try to login from Moldova, that should trigger an alert that the credential may be compromised.

  Effective analytics systems are able to determine if credentials are acting abnormally and can be automated to take various actions. If a credential suddenly exhibits behaviors that fall sufficiently outside the baseline of expected behavior, the system can trigger an alert, ask for additional forms of authentication, or even curb access and revoke privileges. At their best, analytics are integrated with both the authentication and access platform as well as the governance and administration platform.

## DEFINITIONS:

- **Authentication: Enabling users to prove they are who they claim to be – via multiple factors, so that the compromise of one factor does not enable access**
- **Access: Ensuring that users, once authenticated, can easily access the right applications and resources, prevent unauthorized users from gaining access, and implementing additional controls for privileged users**

- ***Privileged Access Management (PAM)*** focuses on applying additional controls around access to a subset of resources that are particularly sensitive.  Privileged Access solutions may include session monitoring, additional layers of authentication, and other features to prevent credential compromise and limit privilege escalation.

  Privileged accounts are of particular interest to perpetrators not only because of the resources they can access, but also because other IAM controls often cannot easily detect operations performed by these accounts.  Not surprisingly, many of the worst breaches of the last decade targeted privileged accounts as part of a cyber kill chain.

## APPLYING THE H-ISAC IDENTITY FRAMEWORK TO REAL LIFE USE CASES

As we noted earlier, the Identity Framework outlines how different core IAM components should integrate and inter-relate to secure the enterprise.  The Framework we've outlined is not a one-size-fits-all approach, however – depending on your organization's particular environment or uses cases, the Framework components may be applied differently.

In this section, we illustrate how the Framework can be applied to four different use cases:

### NEW EMPLOYEE ON-BOARDING

Errol is starting as a new hire working as a nurse at a hospital.  He will need to have access to many of the hospital's core systems, including those used for patient care.

#### *Governance and Administration Layer*

- HR systems pass a request to the CISO organization prior to Errol's start date, and also lay out what applications and data he should have access to in his new job.  These access requests are supplemented by authorization requests from his manager.
- The IAM system 1) creates a new record with Errol's information in the firm's identity directory, and 2) provisions access.
- Errol is provisioned a credential requiring MFA to log in and access resources.
- The identity system logs all future authorization, authentication and access events, should an audit of these events be required.

#### *Authorization Layer*

- On his third day of work, Errol becomes aware of two additional hospital resources that he needs to access as part of his job.  He places a request for access privileges through the IAM system and his supervisor approves it.
- Should he need additional resources, his supervisor can request them from the IAM system and – within reason – grant access privileges.

#### *Authentication and Access Layer*

- All requests to access hospital resources – be they when Errol is on premise or remote – are authenticated using both device authentication and human authentication using MFA.
- Identity analytics systems monitor the ways in which Errol's credentials and devices are used each day, to check for any anomalies.

## AN EMPLOYEE'S ROLE CHANGES

Sara is being promoted to a new role leading product development at a pharmaceutical company; the product she will lead is different than the one she worked on previously. As a result, some of the resources and systems she will need to access will change. In addition, her role as a senior product manager means that some of the data around the products she is working on is considered "privileged" based on its particularly sensitive nature, as it represents the company's core intellectual property; privilege access controls will apply here.

### Governance and Administration Layer

- HR systems pass a request to the CISO organization about Sara's new job and her start date, as well as her new manager, Jeremy.
- Jeremy determines what resources she should have access to in her new job and visits an IAM portal run by the CISO organization to request these access rights are provisioned in the IAM system.
- Sara's old manager is directed by the CISO organization to review Sara's existing access rights and revoke any privileges that are no longer appropriate. Among other things, this minimizes risk in the event her credentials are ever compromised – access is limited to a small subset of company's data.
- Sara's updated access privileges are recorded in – and enforced by – the company's IAM system.
- The identity system logs all future authorization, authentication and access events, should an audit of these events be required.

### Authorization Layer

- On her fifth day of work, On her fifth day of work, Jeremy decides there is an additional company resource that Sara needs to access as part of her job. He places a request for Sara to be granted new access privilege through the IAM system, and after confirming the request is consistent with previously established authorization policies, the system grants Sara access.
- Should Sara need additional resources, her supervisor can request them from the IAM system and – within reason – grant access privileges. Though authorization for some resources may require additional levels of clearance.

### Authentication and Access Layer

- All requests to access company resources – be they when Sara is on premise or remote – are authenticated using both device authentication and human authentication using MFA.
- Identity analytics systems monitor the ways in which Sara's credentials and devices are used each day to check for any anomalies.
- For those systems containing data that is particularly sensitive – such as the company's core intellectual property – Privileged Access Management (PAM) are applied, putting additional controls in place to secure access to these assets.

## CREDENTIALING A THIRD-PARTY BUSINESS PARTNER FOR LIMITED SYSTEMS ACCESS

Letting any outside actor into your systems increases an organization's level of risk, but engaging with third-party business partners is unavoidable for most organizations. By credentialing a third-party business partner for limited access to necessary systems – and by putting controls in place that preclude any "privilege escalation" of those credentials – risk can be mitigated.

Errol's Hospital has outsourced its cleaning services to the Acme Corporation.  Five Acme managers need access to three of the hospital's systems in order to manage and deliver these cleaning services, but should not have access to any hospital systems beyond that.

### *Governance and Administration Layer*

- The Hospital's COO office that oversees the Acme contract requests that the IAM system provision accounts with limited access privileges to five Acme managers.
- As part of this request, the COO organization outlines the rationale for granting access to these systems.
- The IAM system (under control of the CISO) 1) creates five new records in the directory it uses to manage contractors and, and 2) provisions access to the three requested systems.
- The five Acme managers are provisioned a credential requiring MFA to log in and access resources.
- The identity system logs all future authorization, authentication and access events, should an audit of these events be required.

### *Authorization Layer*

- Given the limited access requirements of the Acme personnel, the IAM system is configured so that it is not possible to grant additional privileges.
- Because of the heightened risk involved with third parties accessing the hospital's systems, the authorization system is configured to create an alert if any additional privileges are requested, granted or escalated, given that these changes would violate company policy.

### *Authentication and Access Layer*

- All requests for Acme personnel to access hospital resources are remote.  They are authenticated using both device authentication and human authentication using MFA.  In this case, the hospital issues five hardware-based FIDO Security Keys to Acme for their personnel to secure their accounts.  This ensures that if passwords are ever compromised, the attacker cannot gain access.
- Identity analytics systems monitor the ways in which the Acme personnel's credentials and devices are used each day to check for any anomalies.

## WHEREVER POSSIBLE, FEDERATE

***While we show Errol's Hospital directly issuing credentials to the Acme employees, ideally, the hospital could instead trust the credentials that Acme issued to its employees – by federating its system with theirs, or by leveraging a trusted shared service for credentialing.***

***Beyond the hassle and expense of issuing new credentials, Errol's Hospital will not have direct visibility into the status or position of the Acme employees should anything change.  But by embracing a federated approach, a revocation of an Acme credential will result in that credential being useless in the hospital.***

***Federation is not always easy – both parties must rely on common standards based on trust levels.  However, federation not only offers a simpler approach to third party IAM – it also allows organizations to focus more on authorization.***

## CREDENTIALING A NEW PATIENT

Denise is a new patient in the medical practice of Dr. Cincera. She has a right to log in and access her health information – and only her health information – from the Electronic Health Record (EHR) system used by Dr. Cincera's office. This is tricky in that the EHR system is an enterprise system – but it's one that holds patient data, meaning access has to be governed to allow her to get to it.

### *Governance and Administration Layer*

- As part of the new patient onboarding process, Denise's identity is created in the patient identity directory.
- Denise is provisioned a credential requiring MFA to log in and access her health information.
- Alternatively, she is granted the option to federate an existing credential she has with another service (such as her bank) with Dr. Cincera's office.
- The medical practice's IAM system logs all future authorization, authentication and access events, should an audit of these events be required.

### *Authentication and Access Layer*

- All requests to access Denise's EHR come from devices under her control. They are initially authenticated using MFA – and as these devices become trusted over time, the IAM system also incorporates device authentication.
- Identity analytics systems monitor the ways in which Denise's credentials and devices are used each day, to check for any anomalies.
- Should Denise wish to download her health data or request that it be transferred to a third party, the IAM system authenticates her request with MFA.

# WHAT'S NEXT?

This paper represents the second of an H-ISAC series designed to introduce CISOs to an identity-centric approach to cybersecurity; the first paper focused on the "why" while this paper delved into the "how." By providing an explanation of key concepts, outlining a framework and best practices, investigating the various solutions and vendors, and highlighting the aspects of effective implementation, the H-ISAC intends to provide a holistic guide to assist CISOs in the health sector on how to best approach Identity and Access Management (IAM) and its role in managing cybersecurity risk.

### *More In-depth Analysis*

Members should expect subsequent releases to provide in-depth analysis and guidance on many of the issues and technologies introduced in the first two papers.

### *Help Shape Future Papers*

As we go through this process together, your input will be vital to crafting these follow-on papers. Furthermore, we will provide a means for H-ISAC members to submit feedback as we consider future papers, so that we may ensure that this series thoroughly examines the aspects that need further clarification or elaboration.

### *Helping Organizations of All Sizes and Maturity Levels*

The H-ISAC is committed to improving the entire healthcare cybersecurity ecosystem; this series will assist organizations of any size and of any cybersecurity maturity adapt their defense models to address the current threat landscape and become more secure.

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

www.h-isac.org