LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

# HC3 Intelligence Briefing
# Access Control on Health Information Systems

**OVERALL CLASSIFICATION IS**

**TLP:WHITE**

**April 9, 2020**

***Report #: 202004091030***

# Agenda

- Introduction
- Access Control Overview
- Identification and Authentication
- Authorization
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- References
- Questions

Icon Finder

## Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

# Introduction

- The widening use of healthcare information systems such as the Electronic Health Record (EHR), which allows for the collection, extraction, management, sharing and searching of information, is increasing the need for information security (e.g. confidentiality, integrity and availability)
- Also the development of computer science and smart health-care technology, has created an outlet for patients to employ medical care at home.
  - Taking the growing number of users in the Smart Healthcare System into consideration, access control is an important issue developers need to take into account.
- Access control is essential to provide for the confidentiality and protect the integrity of the EHR and because it is part of the authorization process where the system checks if the user can access the resources they requested.

CSO Online

# Access Control Overview

- Access control is a paramount feature of any secured system. Generally speaking, it provides for subject-to-object segregation according to a security policy implementation at a given system.
- **Subject**. A subject is the active entity that accesses an object. For example, when a user accesses a file, the user is the subject.
  - Other subjects include programs, processes, and any entity that can access a resource.
- **Object**. An object is a passive entity that is being accessed by a subject. For example, when a user accesses a file, the file is the object.
  - Other objects include databases, computers, printers, or any other resource that can be accessed by a subject.

Computer Hope

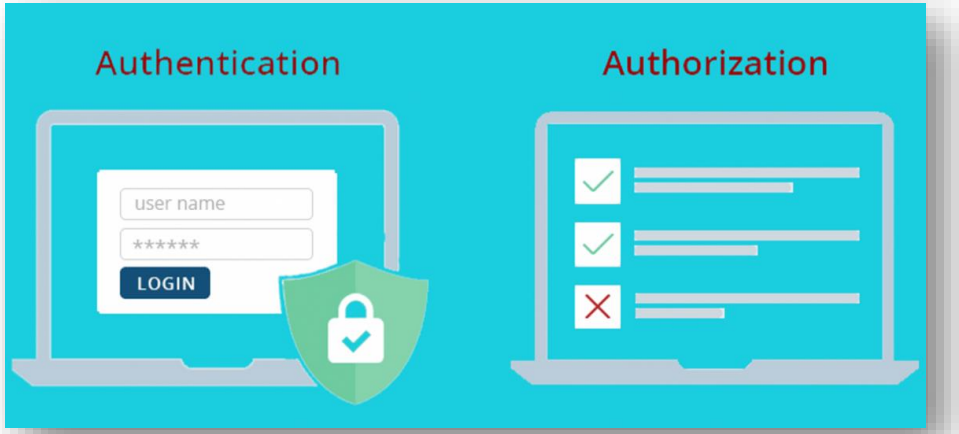
# Identification and Authentication (I&A)

- **Identification** is the ability to identify uniquely a user of a system or an application that is running in the system.
- **Authentication** is the ability to prove that a user or application is genuinely who that person or what that application claims to be.
- The I&A process assumes that there was an initial validation of the identity, commonly called identity proofing.
- Authenticators are commonly based on at least one of the following four factors:
  - **Something you know**, such as a password or a personal identification number (PIN).
  - **Something you have**, such as a smart card or security token.
  - **Something you are**, such as fingerprint, voice, retina, or iris characteristics.
  - **Where you are**, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.


NCMEP

# Authorization

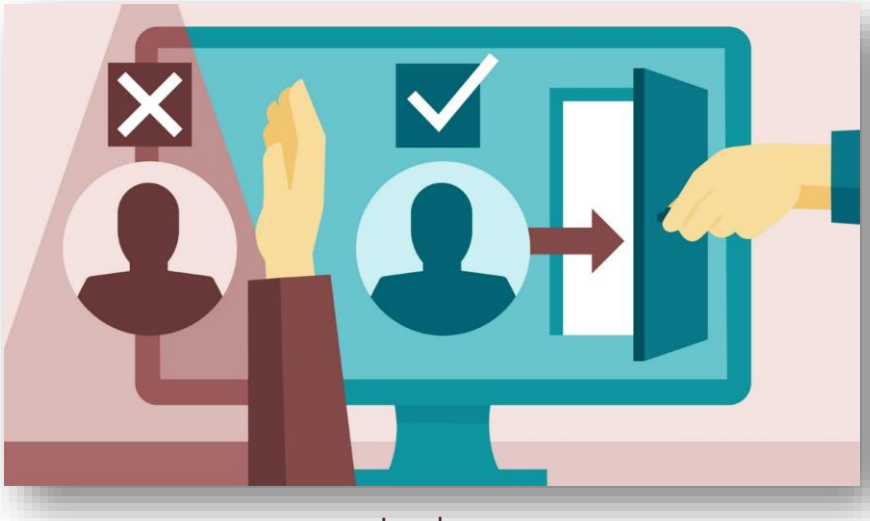
- **Authorization** is the function of specifying access rights/privileges to resources, which is related to information security and computer security in general and to access control in particular.
- More formally, "to authorize" is to define an access policy.
  - For example, human resources staff are normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system.
  - During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected).




Ilantus

# Mandatory access Control (MAC)

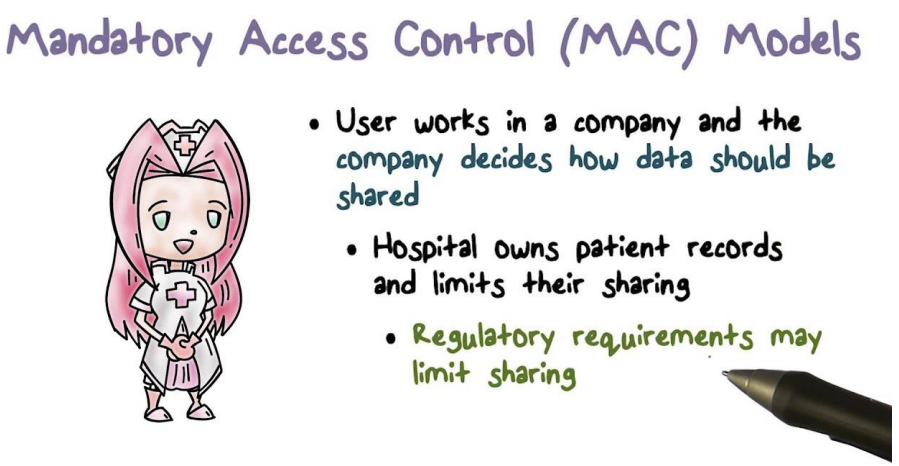
- **Mandatory access control** refers to a type of access control by which the operating system constrains the ability of a *subject* or *initiator* to access or generally perform some sort of operation on an *object* or *target*.
    - Any operation by any subject on any object is tested against the set of authorization rules (aka *policy*) to determine if the operation is allowed.
- With mandatory access control, this security policy is centrally controlled by a security policy administrator; users do not have the ability to override the policy and, for example, grant access to files that would otherwise be restricted.



Lynda.com

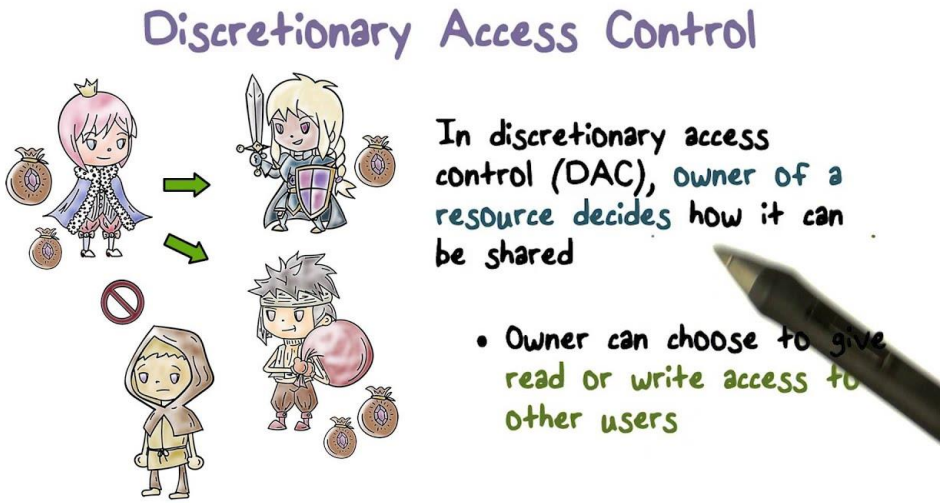
# Mandatory access Control (MAC) cont…

- Mandatory Access Control is by far the most secure access control environment but does not come without a price.
  - MAC requires a considerable amount of planning before it can be effectively implemented.
  - Once implemented it also imposes a high system management overhead due to the need to constantly update object and account labels to accommodate new data, new users and changes in the categorization and classification of existing users.



# Discretionary Access Control (DAC)

- **Discretionary access control (DAC)** is a type of access control defined as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong.
- The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)".




Youtube

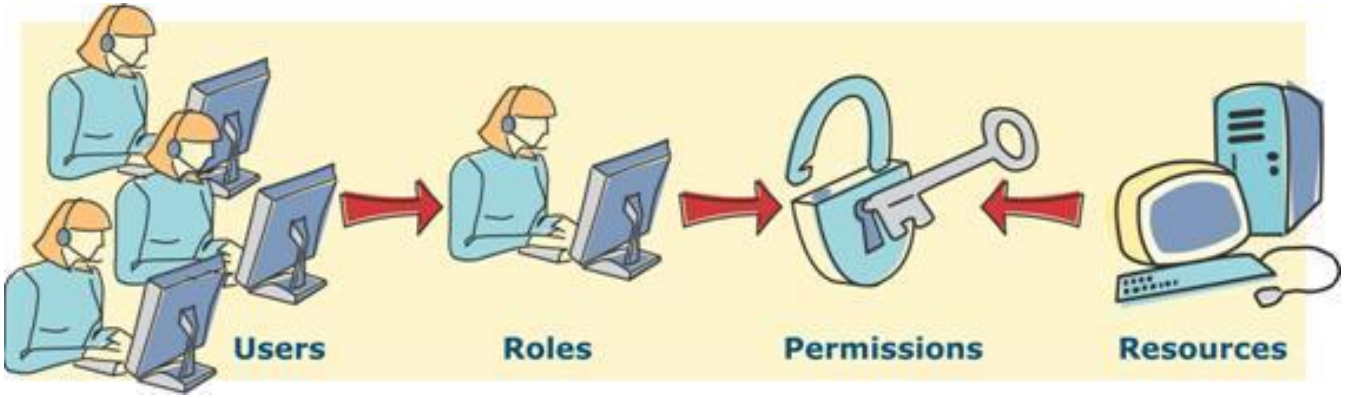
# Role Based Access Control (RBAC)

- **Role-based access control (RBAC)** is a policy-neutral access-control mechanism defined around roles and privileges.
- The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.
- Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles.

CSO

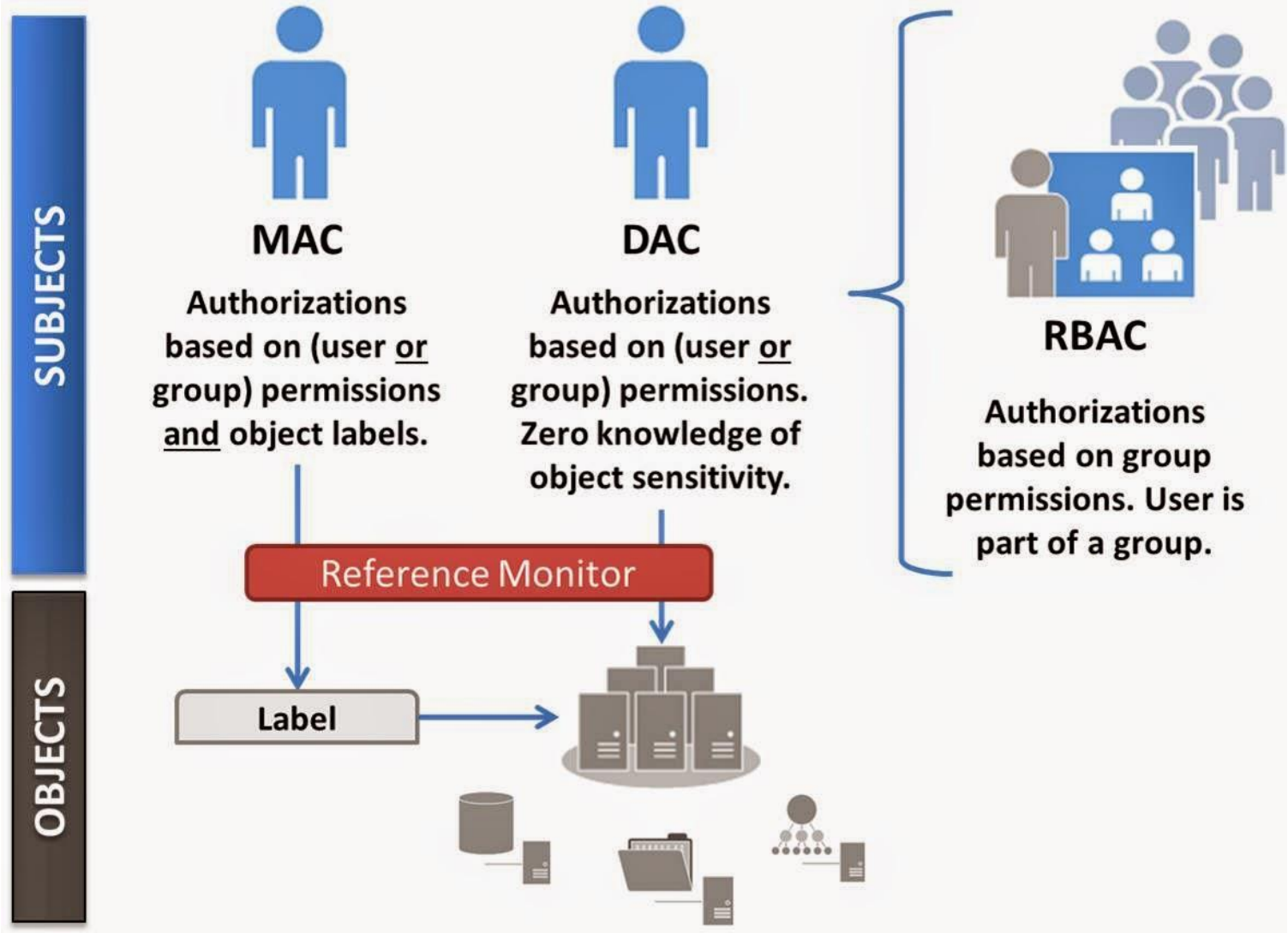
# Role Based Access Control (RBAC) cont…

- Three primary rules are defined for RBAC:
  - **Role assignment**: A subject can exercise a permission only if the subject has selected or been assigned a role.
  - **Role authorization**: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
  - **Permission authorization**: A subject can exercise a permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.




Tasdik Rahman

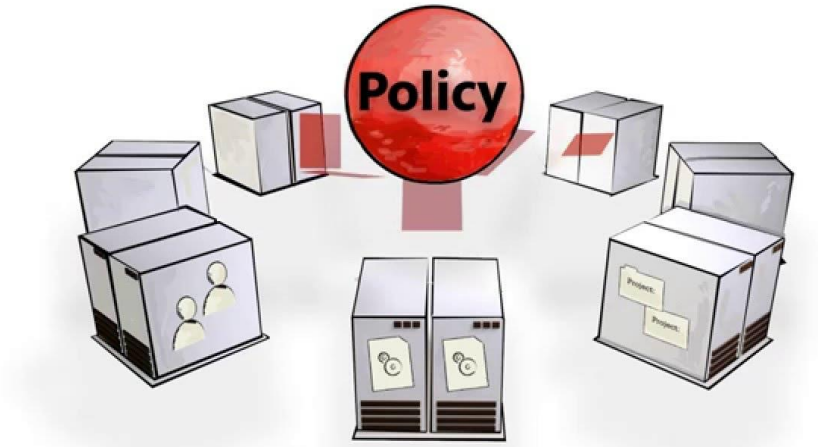
# Access Control Model Comparisons



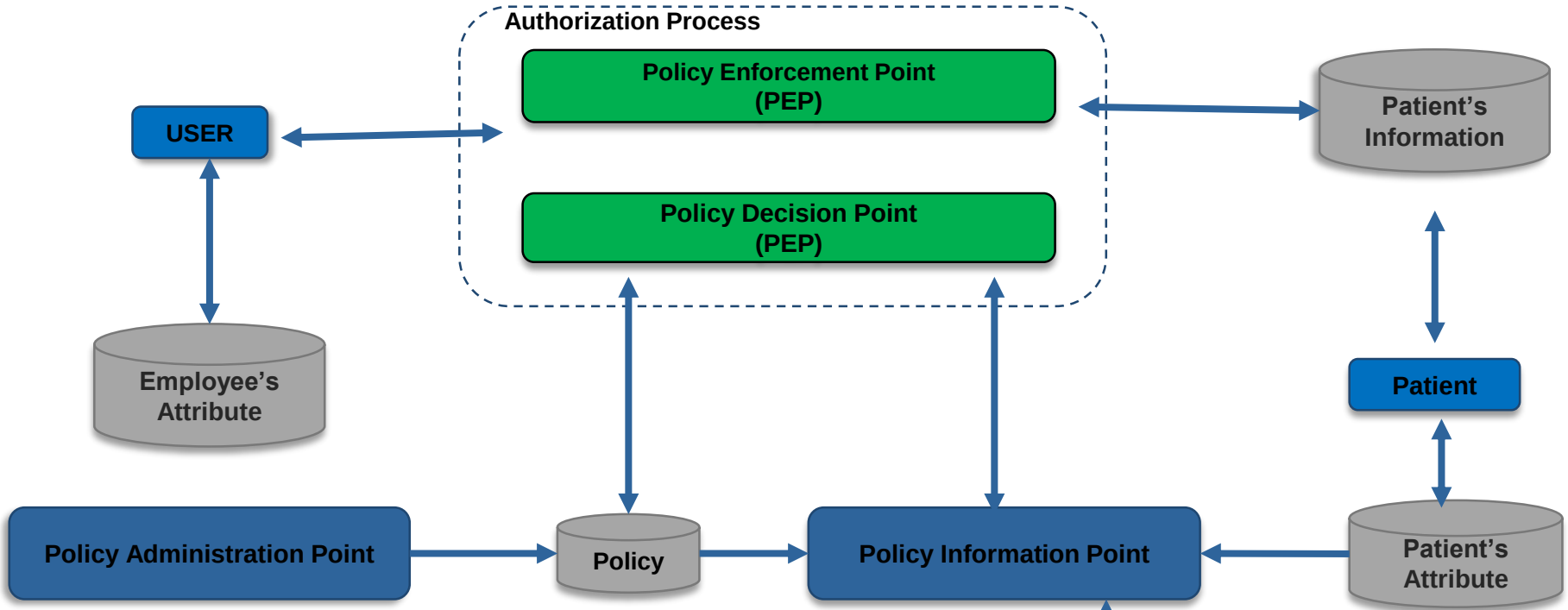

Cloud Audit Controls

# Attribute Based Access Control (ABAC)

- **Attribute Based Access Control (ABAC)** describes an access control model where access rights are admitted to users by the use of policies.
  - Attributes are properties that describe specific features of the subject, object, environment conditions, and requested actions that are predefined and preassigned by an owner or administrator or authority.
  - The policy is the description of rules or connections that determine the set of permissible operations a subject should run upon an object in authorized environment conditions.
- This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action.
  - For example: IF the requestor is a dentist, THEN allow read/write access to dental history but only read access to medical history.



# Attribute Based Access Control




**The Main Policy Set by The Hospital**

| Data Requester | Type of Resource | Action |
|---|---|---|
| Doctor | Patient's history records | Read, Write |
| Nurse | Identity information of patients | Read |
| Researcher | Statistical Information | Execute if Patient count> 50 |
| **Supplementary Segment** | | |
| Doctor | Patient's history records (only last 5 years) | Read, Write |
| Nurse | Identity information of patients | Read |
| Researcher | Statistical Information (all years expect two last years) | Execute if Patient count> 50 |

Axiomatics

# References

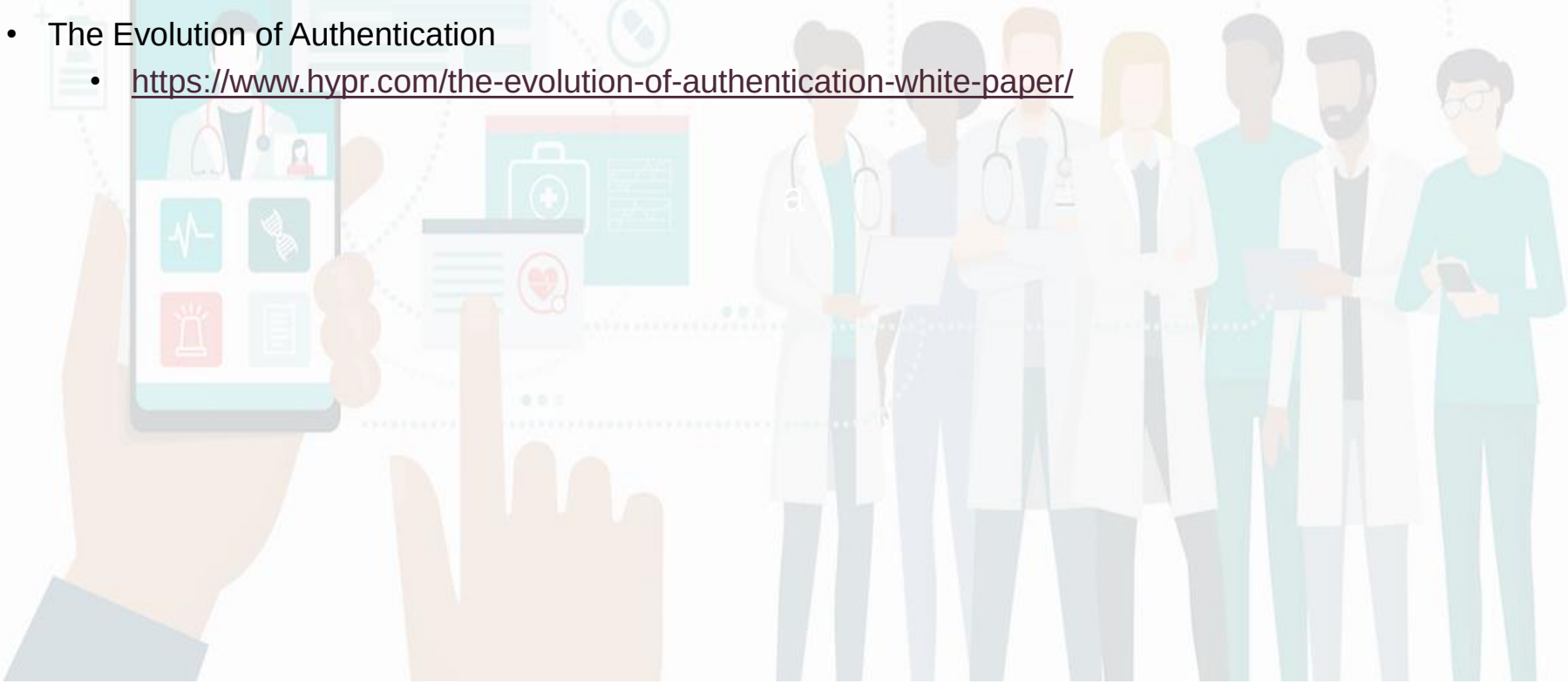

- Role based access control and best implementation practices
  - https://www.cyberdefensemagazine.com/role-based-access-control-and-best-implementation-practices/
- Multi-Factor Authentication Gains Traction In Healthcare
  - https://www.healthitoutcomes.com/doc/multi-factor-authentication-gains-traction-in-healthcare-0001
- Access Control: how can it improve patients' healthcare?
  - https://pdfs.semanticscholar.org/607c/132fc24ac1572518cb5f1d4a996c4dffad93.pdf
- Access Control: Models and Methods
  - https://resources.infosecinstitute.com/access-control-models-and-methods/
- Overview of Access Control Systems
  - https://www.securityindustry.org/2019/10/08/overview-of-access-control-systems/
- Usable access control policy and model for healthcare
  - https://ieeexplore.ieee.org/document/5999035
- Unifying Identity Management And Access Control
  - https://www.securityinformed.com/insights/co-2415-ga.9535.html?utm_source=SSc%20International%20Edition&utm_medium=Redirect&utm_campaign=International%20Redirect%20Popup
- MAC vs DAC vs RBAC
  - http://www.cloudauditcontrols.com/2014/09/mac-vs-dac-vs-rbac.html

# References


- Towards dynamic access control for healthcare information systems.
  - https://www.ncbi.nlm.nih.gov/pubmed/18487814
- Role-based access control in healthcare
  - https://www.healthcareitnews.com/blog/role-based-access-control-healthcare
- A Knowledge-Constrained Access Control Model for Protecting Patient Privacy in Hospital Information Systems
  - https://www.researchgate.net/publication/316442843_A_Knowledge-Constrained_Access_Control_Model_for_Protecting_Patient_Privacy_in_Hospital_Information_Systems
- Implementing Role Based Access Control
  - https://tasdikrahman.me/2017/06/01/Implementing-role-based-access-Control-easyrbac-python/
- NIST Special Publication 800-162:Guide to Attribute Based Access Control (ABAC) Definition and Considerations
  - https://web.archive.org/web/20160305222004/http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
- DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
  - https://web.archive.org/web/20060527214348/http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
- Technical Approaches to Protecting Electronic Health Information
  - https://www.ncbi.nlm.nih.gov/books/NBK233433/
- A context-related authorization and access control method based on RBAC: A case study from the health care domain.
  - https://www.researchgate.net/publication/290810808_A_context-related_authorization_and_access_control_method_based_on_RBAC_A_case_study_from_the_health_care_domain

# References


- Organization based access control
  - http://www-master.ufr-info-p6.jussieu.fr/2005/IMG/kordon/grar/sv-5.pdf
- Access Control Systems
  - https://www.computerhope.com/jargon/a/acs.htm
- OWASP Top 10
  - https://owasp.org/www-project-top-ten/
- The Evolution of Authentication
  - https://www.hypr.com/the-evolution-of-authentication-white-paper/

# Questions

## Upcoming Briefs

- AZORult
- COVID-19 Cyber Threats

## *Product Evaluations*

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

## *Requests for Information*

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**