Predict | Protect | Prevent

HIPAA

Compliance with ARCON | PAM

arcon

Objective of HIPAA

The objective of Health Information Portability and Accountability Act (HIPAA) is to protect personally identifiable electronic health information. The act mandates that any entity storing, processing and transmitting health information electronically should have a robust security framework to protect it from unauthorized access. The regulation is part of the broader Protected Health Information (PHI) act that requires to protect individually identifiable health information stored in any form- be it on paper, oral or electronically.

Which organizations should comply with HIPAA?

Any entity that maintains health information, directly or indirectly, in its information systems

- Specialty Hospitals / Nursing Homes
- Health Insurance Companies
- Pharmaceutical Companies
- Pathology Laboratories
- Medical Service Providers
- Medical Equipment Manufacturers

Consequence of HIPAA non-compliance

In case of a health information breach, the guilty entity is supposed to pay $200 per victim according to HIPAA.

Breach Investigation has to be done by any external organization to identify/ detect whether any suspicious activity or unauthorized access has happened in the official network.

As a **Remediation** process of a HIPAA breach, the digital security solutions should be installed/ implemented under close surveillance of the IT security officer.

Official **Breach Notification Letters** should be issued to each and every affected individual followed by subsequent developments and updates by the organization.

There has to be some **Temporary Operational Changes** by the administration after a breach incident in order to revamp the entire work-flow.

HIPAA demands **Identity Theft Prevention** norms to every individual breach victim for free credit monitoring for next 1-2 years.

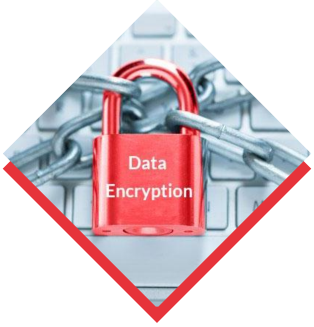
Due to **Loss of Business/ Reputation** after HIPAA breach, the consumers can switch their service providers without any hassle irrespective of any previous contract.

HIPAA breach victims are entitled to get a special and **Dedicated Helpline/ Website** where they can resolve their queries or seek any relevant information.

(*referred from http://ww2.cfo.com/search?s=HIPAA*)

HIPAA Compliance

Secure the information system of the organization



Encrypt each and every data

Detailed clarity of access records of the crucial data

Lucid and vivid documentation of the activities

What it Implies

- to formulate a centralized policy framework to administer and control a user's access to health information
- ensure access to critical information is made only after multi factor authentication
- end users are segregated based on job functions and responsibilities and access is restricted and fine-grained
- secure third-party access to health information
- robust access control if the health information is stored on cloud or maintain by Managed Service Providers (MSP)
- ensure that credentials (privileged credentials) are frequently randomised and securely vaulted
- audit trails are maintained

But Healthcare records are still vulnerable

Despite the legislation being effective since more than twenty years ago, healthcare organizations are yet to be HIPAA compliant.

In September 2018, three Massachusetts hospitals were fined nearly $1 million for non-compliance of HIPAA. (source: Healthcare ITNews)

Banner Desert Medical Center in Arizona suffered breach of 3.7 million patients' records in 2016 (source: hipaajournal.com)

Stephenville Medical & Surgical Clinic suffered breach of 75,000 medical records due to some unauthorized access in May 2017 (source: hipaajournal.com)

Enterprise Services LLC experienced worse breach involving 56,000 records due to unauthorized access in June 2017 (source: hipaa journal .com)

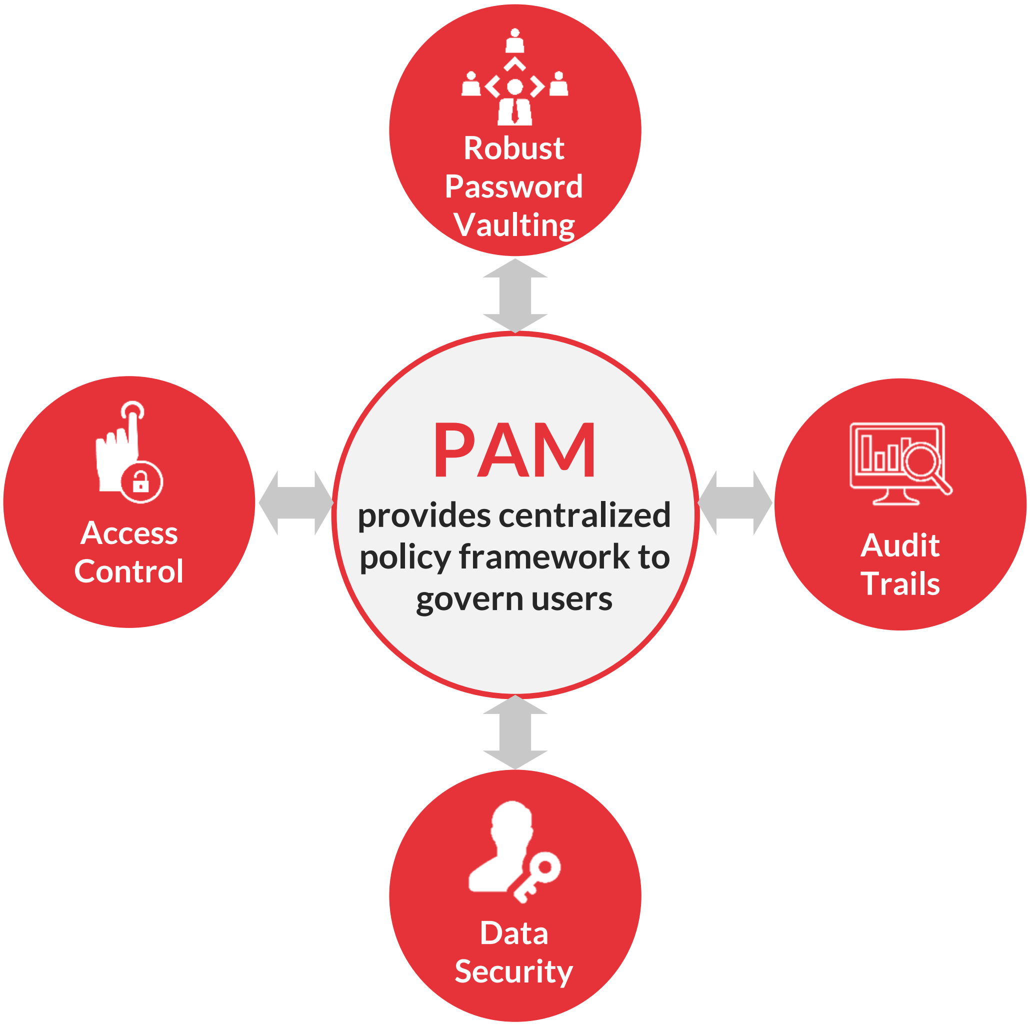
The healthcare industry witnessed largest number of hacking incidents in 2017, according to HIPAA journal.

.... and many more incidents

HIPAA

Privileged Access Management to protect electronic health information

Privileged Access Security takes the center stage when it comes to mitigating breach of electronic health information.   ARCON| Privileged Access Management (PAM) offers an organization the foundation for best IT security practice. It reinforces the user identity and access control in an enterprise IT environment. It ensures rule-based restricted access to OSes, databases and applications. It offers IT security team an additional protective layer to secure health information. With ARCON PAM any user will be granted permission to access electronic health information only after a thorough authorization and authentication process. In addition, the solution helps in addressing the HIPAA requirement that mandates any entity processing health information must maintain audit trails of each activity around health information. ARCON |PAM helps in controlling and monitoring the users.



PAM

provides centralized policy framework to govern users

Robust Password Vaulting

Access Control

Audit Trails

Data Security

ARCON | PAM is a robust tool to protect health information

ARCON | PAM functionalities offer IT security team with an added layer to protect data. The solution provides

Access Control

- Centralized policy engine to authorize privileged user access to protected e-health information
- Segregating, elevating, and controlling privileged users based on their job profiles

Data Security

- Database encryption using 256 bit AES encryption
- Multi-factor authentication using biometric device, hardware token and mobile OTP

Password Management

- Robust and secure password vaulting automates the privileged password management
- Frequent randomizing of privileged passwords

Audit Trails and Risk Analysis

- Capture each and every privileged session in a video and text format
- Threats alerts and risk analytics
- Dashboard provides real-time view of activities performed by privileged users

HIPAA Acts and Compliance mapping

HIPAA Standard	Act	Inference	ARCON | PAM Compliance
Data Access Management	164.308(a)(4)	The Act requires that any entity maintaining electronic protected health information should have an IT security policy framework and it should implement these policies and procedures to prevent, detect, contain, and correct security violations.	ARCON | PAM offers a centralized user access policy framework wherein the IT security staff can manage, monitor and control role-based user access to electronic health information.
Access Control	164.312(a)(1)	HIPAA mandates that access to electronic health information is protected from unauthorized users.	ARCON | PAM offers deepest level of granular access control. The solution enables to restrict and elevate commands for databases and offers command filtering capabilities for controlling critical activities on IT systems.
Audit Controls	164.312(b)	To implement procedures that record and examine the end users activities in Information Systems storing protected health information.	ARCON | PAM enables to record sessions both in video and text formats, monitor and log all activities. In addition, the solution provides customized reporting and threat analytics. These functionalities provides comprehensive reporting of all activities, enabling better decision making.
User/ Entity Authentication	164.312(d)	To implement procedures that verify that any end user seeking access to electronic health information is authenticated.	Multi-factor authentication process mitigates the risk of unauthorized access to e-health information. ARCON offers native software based OTP validation to initiate a session and the tool easily integrates with third-party solutions to provide biometric authentication.

Conclusion

Today's healthcare organizations maintain data electronically. This information is at grave risk from malicious insiders and cybercrooks. They exploit security gaps to steal critical information stored in IT systems. ARCON Privileged Access Management provides IT security team an added layer of protection around electronic health information. The solution mitigates data breach threats by seamlessly monitoring and controlling the privileged users.

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us