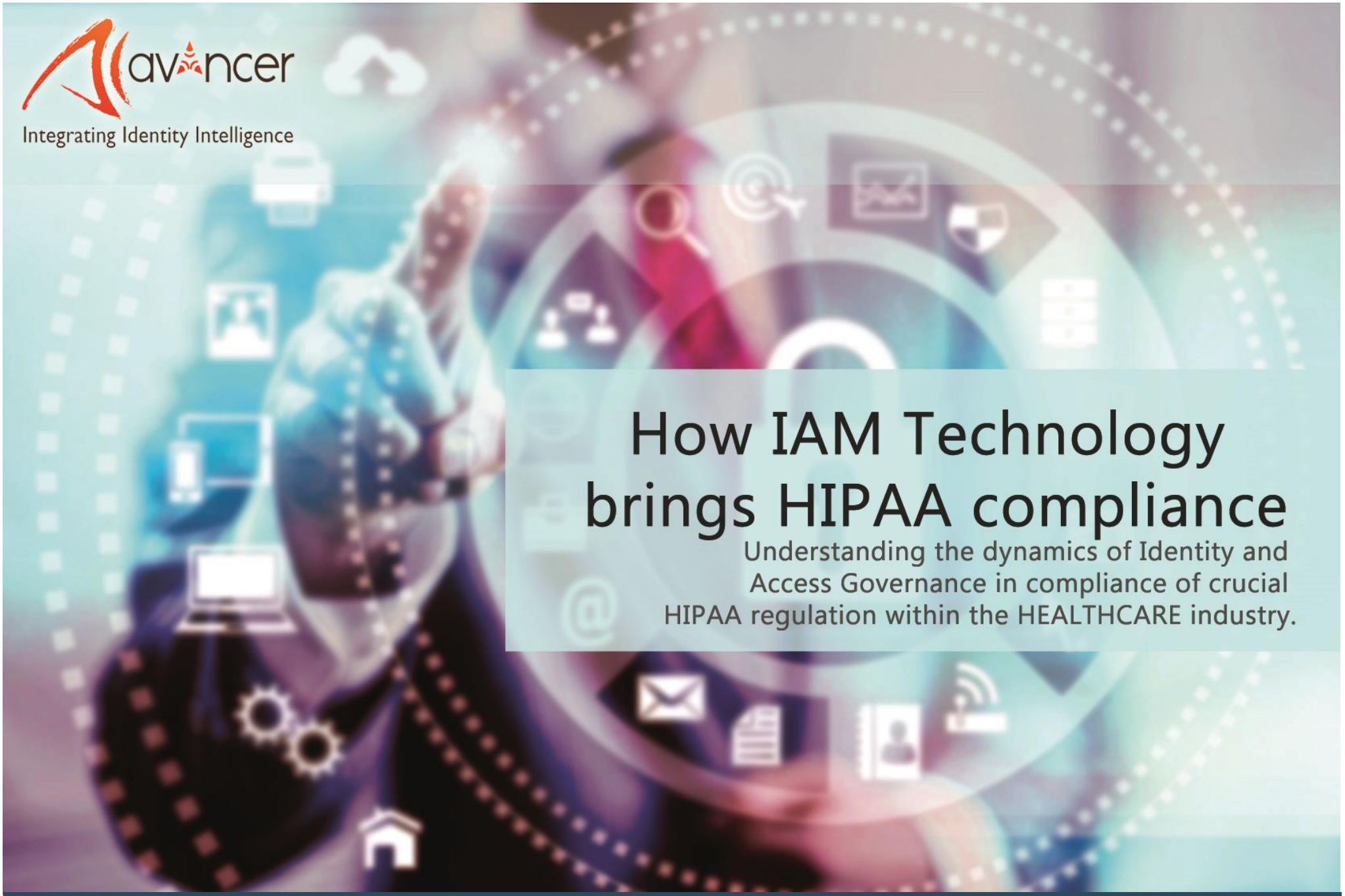



Copyright – Avancer Corporation | Release – June 2016

# Content


| | | | |
|---|---|---|---|
| 1. | Introduction | | 3 |
| 2. | About HIPAA | | 6 |
| | 2.1 | HIPAA Safeguards | 7 |
| 3. | Why bother being HIPAA compliant? | | 8 |
| 4. | Usage of IAM Technology to bring HIPAA compliance | | 9 |
| | 4.1 | How to integrate technology for HIPAA compliance | 10 |
| | 4.2 | Accessing ePHI through Identity Management | 11 |
| | 4.3 | Using Secure Messaging Platforms | 12 |
| | 4.4 | Implementing Technical Safety to prevent Data Breach | 13 |
| | 4.5 | Integrating Mobile Apps | 13 |
| | 4.6 | Addition of extra Security Layers | 14 |
| 5. | In conclusion | | 15 |
| 6. | About Avancer Corporation | | 16 |

# 1. Introduction

Since the implementation of Health Insurance Portability and Accountability Act (HIPAA) in 1996, there has been exponential and constant adoption of digital capabilities within the healthcare industry. Such capabilities include maintaining patient information in number of scattered sources, usage of mobile technology to access sensitive information by clinical staff, access to payment-related information by administrative staff, repository of numerous patient health records in custody of lab managers and so on.

This has brought in ease of access to information and many benefits to the healthcare industry. However, if the data or information is not secured, it may become target of cyber criminals, accessing medical data illegally. Threat of data theft has become a nightmare for the healthcare industry.

As per data released by the Identity Theft Resource Center (ITRC), during 2015 (as of December 1, 2015), out of the total data breaches reported, around 35 per cent were from the medical / healthcare industry. Although, the total breaches stood at 717, and medical / healthcare industry saw breaches at 248 organizations during the year, what is worrying is that from the total number of records compromised, almost 68 per cent stolen records were medical data. A whooping 120,077,576 medical records were compromised out of the total 176,275,271 data during the period[i].

Impact of medical identity theft on healthcare providers is considerable—both in terms of loss of revenue, regulatory penalization and dent on reputation. Calculating HIPAA data breach penalty cost is not a singular process. In addition to penalty, a healthcare organization incurs exponential costs for notifying patients about data breach, while undertaking damage mitigation, which further spirals the cost. In order to comply with HIPAA, healthcare providers need to implement various security tools in their IT environment and follow practices that protect confidential patient information.

**A strategic IAM System crafts a mechanism that monitors the access of protected data, authenticate identity of data user, delete information/identity and access algorithm that could result into breach of data.** A breach is possible if architecture is not designed properly. For example, loop in defining the information flow, work flow, access requirements depending on job role of a user, enabling APIs for greater information sharing, enforcing access governance, facilitating mobile access for delegated users, etc can pave way for a breach. These processes are to be executed while creating a system that detected, reported and rectified any breach on the system.

★★★★★★★★★★

This report highlights how implementation of HIPAA can help healthcare providers and other peripheral organizations to function seamlessly and place checks on limiting potential data theft, encroachments and infringements to none.

★★★★★★★★★★

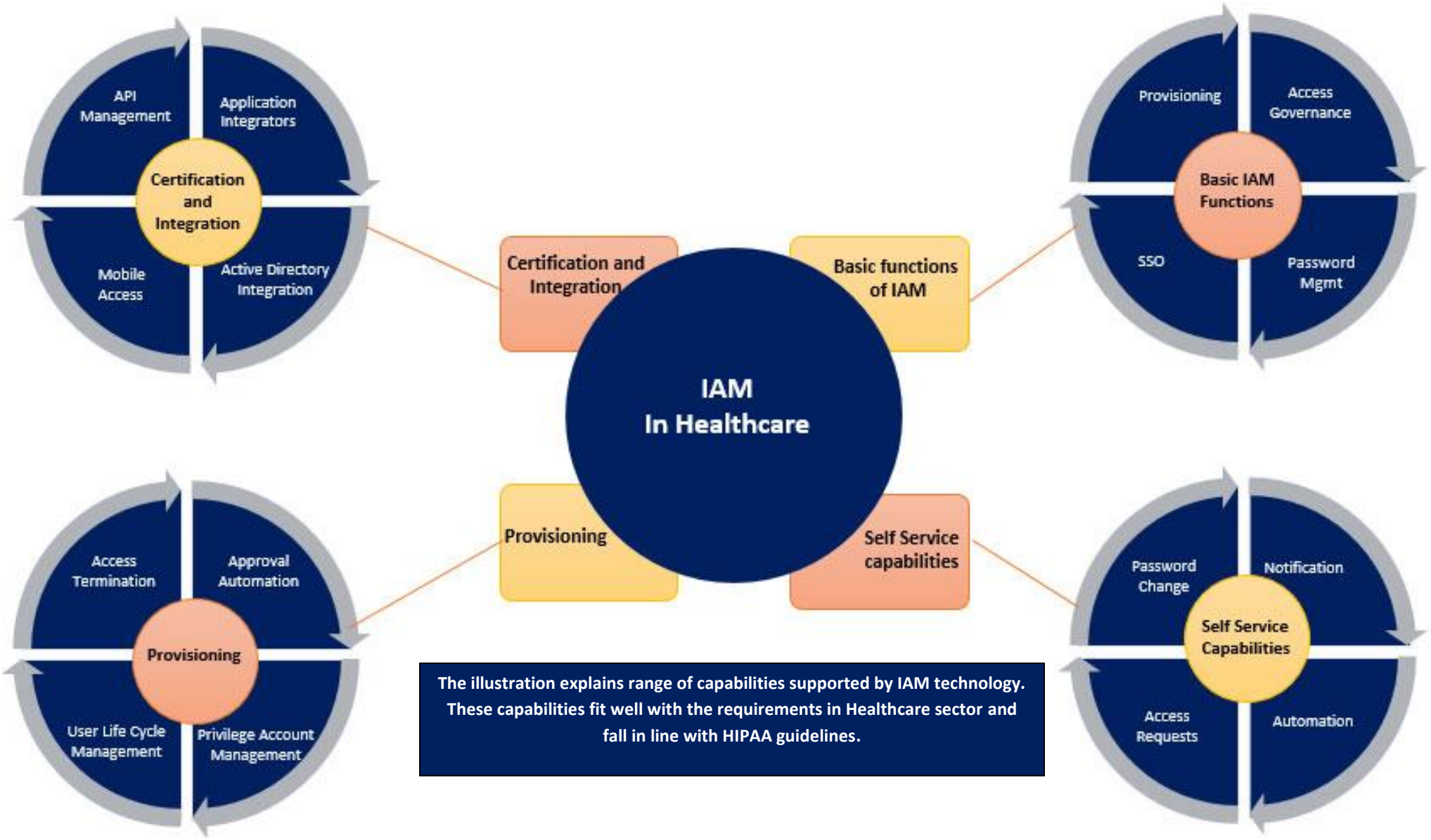
Identity and Access Management (IAM) Technology fits precisely to the requirements of any healthcare establishment to comply with HIPAA. In addition to various automated mechanisms such as audits, notifications, password self-service, strategically aligning business goals to identity management, access governance and IT security systems have become the need of the hour.

2016 Avancer Corporation | All rights reserved | www.avancercorp.com | USA

This report highlights how implementation of HIPAA can help healthcare providers and other peripheral organizations to function seamlessly and place checks on limiting potential data theft, encroachments and infringements to none.

It also elucidates the importance of technology for adhering to HIPAA regulations, which is to become an industry norm in the future. Protecting sensitive information and keeping them under scanner have been highly publicized and monitored, and healthcare providers being in the most vulnerable situation, technology may help in achieving higher efficiencies for gaining maximum utilization of resources.

With the healthcare sector becoming increasingly collaborative and access to enterprise resources are to be shared with a diverse set of users, the challenge of managing identities and governing accesses is often brought up. Avancer Corporation has implemented a range of tailor-made IAM security solutions to facilitate management of electronic identities for players in the healthcare sector. Our expertise in the field has brought us projects of many healthcare providers including medical establishments with over 70,000 user base to strategize IAM for a larger business specific goal without stalling the existing system. We have also served mid/smaller healthcare setups that require adherence to HIPAA compliance in order to do away with any possible penalty.




**The illustration explains range of capabilities supported by IAM technology. These capabilities fit well with the requirements in Healthcare sector and fall in line with HIPAA guidelines.**

2016 Avancer Corporation | All rights reserved | www.avancercorp.com | USA

# 2. About HIPAA

The **Health Insurance Portability and Accountability Act (HIPAA)** was implemented in 1996. Also known as the Kennedy-Kassebaum Act, HIPAA chiefly bifurcates into two titles, namely Title I and Title II.

Title I protects the prior health insurance coverage of the workers and their family members in cases of loss or unavailability of jobs. It also regulates the breadth and availability of individual health insurance policies and group health plans.

Title II enforces the establishment of the national standards for electronic healthcare transactions, combined with national identifiers for health insurance plans, providers, and employers**. It defines policies, guidelines and procedures for maintaining the security and privacy of individually identifiable health information.** It also outlines the numerous offenses related to the violations, frauds, data breaches and abuse in the healthcare industry. Title II is also known as the Administrative Simplification (AS) provisions.

HIPAA has come up with five rules as per the requirements of Title II—the Transaction and Code Set Rule, the Privacy Rule, the Unique Identifiers Rule, the Enforcement Rule, and the Security Rule. HIPAA has also manifested special considerations for confidentiality in federal-funded drug or alcohol rehabilitation services through its drug and alcohol rehabilitation centers.

Title III, Title IV and Title V correspond to tax-related health provisions governing medical saving grounds, enforcement and application of requirements for group health insurance, and revenue offsets deciding the tax deduction, respectively.

Violations of the rules of HIPAA commands legalized action from the Government, along with payment of hefty penalty charges (civil or criminal).

★★★★★★★★★★

Violations of the rules of HIPAA commands legalized action from the Government, along with payment of hefty penalty charges (civil or criminal).

★★★★★★★★★★

## 2.1 HIPAA SAFEGUARDS

HIPAA consists of three sets of safeguards that define the security standards and the prioritized confidentiality of the patient's information. It also prevents breaching of ePHI.

- **Physical HIPAA Safeguards** – It requires the covered entities (insurance companies, healthcare service providers, and third-party service providers, employers) to develop a faculty security plan with encrypted ePHI. The same should incorporate validation procedures for the authorized accessibility of the personnel.
- **Technical HIPPA Safeguards** – It requires the introduction of proper mechanisms for the monitoring of ePHI stored in the databases and computer networks. It should entitle a user with a unique user id and passcode for the authentication of the identity while remotely handling the PHI database.
- **Administrative HIPAA Safeguard** – It requires the appointment of a system administrator to guide the authorized users while communicating or accessing ePHI. The administrator can also revisit the policies either because of legislation demand or the technological advancement.

# 3. Why bother being HIPAA compliant?

**The sole reason for complying with HIPPA regulations is not just to minimize the theft of sensitive data and information, but to safeguard against non-compliance penalization.** HIPAA compliance renders the customers with a better framework of confidentiality for their personal information. Their records, addresses, other personal inputs, unique identification numbers, etc. can be maintained at higher levels of security devoid of any third-party illegal interference.

If an entity fails to undertake adequate security as well as privacy measures for protecting medical records, they might also be charged with financial penalties.

The ARRA – American Recovery and Reinvestment Act of 2009 – which was brought into law on February 17, 2009, was able to establish a tiered civil penalty structure in case of HIPAA violations. The Secretary of the Department of Health and Human Services (HHS) was still given the discretion of determining the penalty amount, which was based on the nature as well as extent of the violation. It was also determined in accordance to the extent and nature of harm caused due to the violationii.

The U.S. Department of Justice (DOJ) – in June 2005 had clarified people/organizations that can be held criminally under HIPAA. It was concluded by DOJ that criminal penalties with regards to violation of HIPAA would be directly applicable for companies including health care, health plans, healthcare providers or clearinghouses. These entities that transmit claims in electronic form and give medicare prescription drug card can come directly under the purview. Individuals including employees, directors or even officers of the entity that is covered – wherein, the covered entity is not an individual – would also be directly liable criminally under HIPAA – this is in accordance to the principles of 'corporate criminal liability'. If an individual of a covered entity is not directly liable under HIPAA, they can still be charged with aiding, abetting and conspiracyiii.

# 4. Usage of IAM technology to bring HIPAA compliance

Protecting a **Patient's Health Information (PHI)** has become difficult and significant. The final rule adopting HIPAA standards (published in Federal Register on Feb 20th, 2003) has specified a straightforward series of physical, technical and administrative security procedures to assure the confidentiality sought by users/patients/customers. The aforementioned Security Rule mentions following security specifications to comply with HIPAA –

- Encryption of all PHI whether in rest or transit.
- The use of any technology must have the options of automatic log-off to prevent unwanted and unauthorized access to PHI when the mobile device (or a computer) is left unattended.
- The licensed/authorized professional must have a Unique User Identifier for monitoring purpose of PHI.

Healthcare providers are required to increasingly integrate technology to safeguard unsecured systems that have following set of capabilities–

- **Understanding the necessity of computer security**– Digitalization of networks and widespread usage of computers has created newer vulnerabilities that involve greater risks. Installation of protections against hacking is better than being caught up in cyber theft.
- **Preparation for a disaster** – The electronic data should be protected against any loss or corruption, whether due to human error, virus attack, hard disk failure, natural disaster, or an equipment failure. A backup system, be it in the form of external hard drives or cloud computing can be utilized.
- **Robust network and communication safeguards** – Every computer network poses a varying amount of risk. Packets of data that are transferred over networks can be either deciphered or stolen. Organizations should install stronger firewalls to minimize such data theft. The credentials of network and authorization attributes should be equally taken care of.
- **Anti-virus software** – Emails, web browsing or online database management systems may get infected with malicious files or viruses. These viruses (software) may either lead to crashing of such systems or can transfer private data over the networks to the criminals. Installing a proper anti-virus will reduce such instances.
- **Encryption** – Encryptions should be implemented on the information transmitted from a service provider's database or employees sharing information over email. Though data encryption maybe a costlier procedure and requires decrypting compatibility at both the ends, it should be assessed to the maximum.
- **Vendors should understand and implement HIPAA standards** – Healthcare providers must be aware of the security measures taken up by their partners or vendors. A solid system that is complying with HIPAA standard can imply better returns on the future exchange of services. Electronic Health Record (EHR) systems should be employed for medium or small-sized vendors.

Furthermore, being HIPAA compliant also benefits various stakeholders in the healthcare industry, for instance–

- Clinical staff, including community nurses, physicians and first responders can communicate PHI instantly through secured texting services.
- Streamlining can be amplifiedfor the administration process of hospital admissions and discharges.
- Activity reports, when integrated with EHR, may reduce complexity in risk management.
- Integration of applications for secure messaging allows easier accessibility and efficiency in locating colleagues.
- Medical professional can securely collaborate from distant desktops over secure networks for accelerating patient diagnosis.
- Documents, images and videos can be attached to secure text messages for accurate diagnosis.
- Read receipts and automatic delivery notifications help in exclusion of unsecured networks, which are used for communication purposes.

## *4.1 How to integrate technology for HIPAA compliance*

In order to become HIPAA compliant, healthcare organizations could integrate the following technological processes:

- **Physical security of data** – Industry recognized certification helps in comprehensive safeguarding of data and ensure that there is a proper access to it. Biometric identification of the worker's palm and thumb that allow access to server and network infrastructure, round the clock supervision through video camera monitors, prohibition of the storage of PHI on personal laptops, and encryption of all the PCs using advanced encryption standards can be instances of physical security of data. PHI should be rendered in-decipherable or unreadable to unauthorized individuals.
- **Protection of sensitive subsets of PHI** – Some PHI data stand to be more sensitive, and at higher vulnerability than other sets of data, such as familial/genomic data, HIV data or mental health data. Hence, to access various categories of data, authorized persons can create subtle definitions of data at the metadata level. This will render granular control over the data, and the audits over it can be performed as per the requirement and sensitivity of the data.
- **Role-based security features** – Healthcare service providers can also render their users/customers with role-based security through the integration of Microsoft's Active Directory authorization and identification database. Varying active roles, i.e., varying levels of granted rights to access the numerous information can be given to the clients.
- **Limited user access to data** – A lower level of security is encountered when many users access the same data set. A limitation can be imposed on software and programs to reduce the number of active user per selected data. The 'least privilege' rule can be applied during the creation of the accounts of the users for finalizing the levels of access for a particular user.
- **Audit and tracking trails** – Solutions should be manifested in the fundamental technological framework of the service provider to log, check, review and verify user actions. These activities can be monitored at three levels, chiefly, the database, the visualization layers, and the Enterprise Data Warehouse (EDW). Configuring individual data elements is a must. Changes to more sensitive data have to be continuously audited and rechecked.

## 4.2 Accessing ePHI through Identity Management

Mature adoption of facilitated utilities not only eliminates the fear of data loss, but also protects the service providers through a secure system of operation. This is especially true in the case of accessing electronically protected health information or ePHI, which could be accessed securely through the use of identity management.

A robust IAM solution helps in creating governance, adhering to compliance, reducing risks, while generating critical business documents, processes and controls.

Healthcare providers are required to strike a balance between protecting sensitive patient data, while ensuring that the employees are provided with the right access. Healthcare IAM solutions help in developing a robust information sharing module that not only prevents unauthorized access, but also helps in adhering to government regulations.

**A holistic healthcare IAM solution should offer:**

- Standardized identification and authentication of users (external, internal, vendors), devices, medical systems, locations, and organizations within the healthcare community
- Scalable IAM system that supports strong user identity, access and security controls to uniquely and securely authenticate and authorize each user
- Adopt a governance-based approach to comply with regulations in the Healthcare Sector in healthcare business of small, mid or big scale.

**Further, it needs to offer the following integrated capabilities:**

- **Single Sign-On (SSO):** Usage of SSO-enabled credentials for employees to access patient information in a secure manner. It brings down the time spent in repeated logins and access related helpdesk requests.
- **API-based Modelling:** Automation of access for helping clinicians provides the right diagnosis, even while moving across systems. This is helpful in keeping consistency in updated information sharing.
- **Password Management:** Self-service and synchronization of password across systems and applications to reduce issues related to generating passwords.
- **Multi-Factor Authentication:** Multiple layers of identity checks to provide access to the right user and ensure data security. It makes use of biometric technology or device based identification capabilities.
- **Regulatory Compliance:** Compliant with various government regulations, such as HIPAA and HITECH, to protect patients' information. Electronic health records of patients are safeguarded through these set of compliances.
- **Mobile-Based Access:** Mobile-friendly access infrastructure to ensure quick, easy and secure access to patient's data on mobile devices as well.
- **Privilege Account Management:** It provides solutions that give administrators the ability for controlling access to various systems which manages confidential electronic health information of patients. This ensures that only authenticated and approved connections are established within the system.
- **Manage Certifications:** Managing or accessing certifications have become critical requirement for privacy regulations and data security, including HIPAA, Sarbanes-Oxley as well as others. With proper validation of appropriateness of access privileges of users, organizations would be able to meet compliance and audit requirements. This also helps in circumventing overall risk.

2016 Avancer Corporation| All rights reserved| www.avancercorp.com | USA

- **Self Service Access Capabilities:** This allows users who are hands-on with IT to take charge for managing their own identity management profiles as well as access.
- **User Audit and Notification**: Automating the entire process, establishes reliable and consistent user access reviews. An organisation saves huge amount of time and money by reducing pressure on IT as well as business staff for performing the work manually. It also helps in auditing and controlling the data in an efficient manner.
- **Integration with Healthcare Apps:** As users log-in through various devices to retrieve information, it becomes a daunting task to keep track of the controls in an organization – if conducted manually. Actively controlling access to various sensitive data through identity management has become the need of the hour. This is a huge challenge for large organizations wherein, individuals might have multiple roles. IAM helps in keeping a check on the accesses as well as provides a safe environment from hackers or others.

IAM technology (Identity and Access Management System) has dominatingly reduced the instances of unauthorized access to secure data. Capturing, recording and managing the user identities help in securing PHI as well as ePHI. Individual enforcement of password management, access controls, session recording and isolation, auditing, authorization, authentication, lifecycle management and provisioning, secure the accounts of the enterprise. Shifting to mitigation techniques with the help of Application Programming Interfaces (APIs) can also be an alternative. Applications created through API with Hash Message Authentication Code (HMAC) signature of Message Authentication Code (MAC) OAuth tokens can inhibit interceptions over unencrypted networks. Patching of clients, servers and gateways imply lesser perilous conditions.

## *4.3 Using Secure Messaging Platforms*

Secure messaging platforms help in devising administrative control for safeguarding the integrity of PHI. It fulfills technical possibilities by including the facility to retract messages that may be intended to breach ePHI. Secure texting enables medical professionals to maintain their convenient speed of data transfer, while on an authorized network. Secure texting applications can be easily downloaded on mobile devices or personal computers irrespective of operating systems installed in them. The application only connect authorized users and data can be shared over that network though securer gateways. System administrators can also define the life-spans of the messages in order to delete messages automatically from a user's application after a predetermined period. The same will imply remote retraction and deletion of messages in cases of stolen devices. These platforms have correspondingly modified the messaging policy of healthcare organizations.

## 4.4 Implementing Technical Safety to prevent Data Breach

Technical safety implies incorporation of simple, yet effective techniques to reduce instances of data theft. Following measures may help in diluting the effects of data breaches if devised in a right manner –

- Periodic risk assessment under healthcare models and operational processes may diminish the vulnerabilities and liabilities. Internal audit, combined with externally specified resources, can help in acquisition of newer levels of risks in the systems.
- Educating employees about technological resource they can opt for to secure the data can help in safeguarding IT systems against data breaches.
- Data minimization corresponds to powerful element of preparedness. Hackers cannot steal something the organization does not possess. Hence, collection of unnecessary data from the patients is inappropriate. Further, there should be a reduction in the number of places where the sensitive data is stored. Lastly, data that has no usage should be responsibly purged.
- Passwords of all secured networks should be strategically encrypted. In the sense that encryption should not just be considered as the only tool for defense. Periodic alteration of passwords for the databases, mobile applications, local networks and private networks should be employed.

## 4.5 Integrating Mobile Apps

Mobile devices that have accessibility to sensitive data can be integrated into a mobile device management system. The remote devices can be synchronized to one single administrator who can handle the actions of the device over a particular network. Pushed email, VPN settings or Wi-Fi can henceforth ensure device compliance. A proper and well-enciphered mobile management system also helps in the management of pass-codes, remote deletion or authentication, leveraging of device posture and an integrated identity.

## 4.6 Addition of extra Security Layers

Inclusion of extra features, embedded in the security systems, doubly ensure safeguarding the data. Tokenization system is one of the alternatives. It helps in securing card transactions (made for the payment of healthcare bills and likewise). The credit card numbers are replaced by a single token using random numbers. Other information of the patients or customers can also be fed into the back-end systems in a similar manner.

Further, a positive shift in thinking and infrastructure has given rise to Secure Cloud Systems. It provides innovative opportunities for purpose-built data centers for workloads, support suited for specific needs and intelligence driven defense solutions. Thereafter, integrated data loss prevention techniques include the services that extend to endpoint security, gateway messaging security, mail server security and control management.

2016 Avancer Corporation| All rights reserved| www.avancercorp.com | USA

# 5. In conclusion

Many healthcare organizations look at regulatory compliance as a liability. However, they fail to look at it as an opportunity to create agile IT systems by setting right networks, and placing application integrators that seamlessly interact with IAM system that ensures compliance. Regulations such as the ones in Healthcare sector – HIPAA, HITECH act as high-level guidelines rather than prescriptive recommendations, but many organizations treat them as comprehensive security rulebooks. IAM experts discourage this kind of approach as it leaves healthcare providers compliant with regulations, but not in the spirit of regulation.

From a healthcare setup standpoint, HIPAA compliance can exceptionally intensify the beneficial aspects of the contemporary healthcare organizations. The straightforward inclusion of secure texting solutions eliminates the capital funding for new hardware, software, and resources. Inhibiting data breaches can save billions, thereby, flipping on the positive side of the coin for the users and the organizations.

Although, technology alone may not fetch healthcare organizations a full compliance with the Health Insurance Portability and Accountability Act, its unhindered and appropriate usage will help the organizations with the administrative, technical and physical requirements of HIPAA.

★★★★★★★★★★

Regulations such as the ones in Healthcare sector – HIPAA, HITECH act as high-level guidelines rather than prescriptive recommendations, but many organizations treat them as comprehensive security rulebooks.

★★★★★★★★★★

2016 Avancer Corporation| All rights reserved| www.avancercorp.com | USA

# 6. About Avancer Corporation

Avancer Corporation is a systems integrator focusing on Identity and Access Management technology. Founded in 2004, it has over a decade's experience in Identity and Access Governance. We have collaborated with leading business organizations and have created expertise in implementing solutions offered by all leading vendors, including Oracle, OKTA, Cerner, CA, Microsoft, Ping Identity, and more.

We take pride in holding a Gold Partnership with Oracle, it signifies the exceptional services we deliver and the superior level of expertise we have time and again offered. Our specialized focus is on enterprise security through a range of end-to-end solutions in Identity and Access Management. Our services ranges from full-term project life-cycle implementation to tailor-made short-haul projects including software procurement, architectural advisement, design, and development through deployment, administration and training.

Avancer brings in ease when it comes to providing access control to patient data and taking it to the clinical level. Healthcare IAM solutions integration offered by Avancer include following features:

- Automate manual processes and cutting costs while boosting user productivity by arming organizations to manage end-to-end lifecycle of user identities across enterprise.
- Integrations and connectors for a variety of healthcare applications such as Cerner, McKesson, Kronos, E-clinical works, Alere, and others.
- Adopt a governance-based approach to comply with regulations.
- Address identity management challenges specific to healthcare industry as well as overall business optimization.
- Adopt customize solutions based on unique company needs – that could be complex or a simple structure.
- Easily and independently manage admin tasks, generate requests, approvals and manage access – minimize provisioning and user lifecycle management tasks.
- Achieve regulatory compliance of key regulations including HIPAA and HITECH.

Avancer has collaborated with big names in healthcare and life sciences industry. In addition to abovementioned capabilities and technological integration, Avancer specializes in almost all aspects of IT Security.

# CONTACT US


## Avancer Corporation

101 Interchange Plaza
Suite 201 Cranbury
NJ 08512, USA
Tel: +1 (609) 632-1285
Fax: +1 (877) 843-8594
Email: info@goavancer.com
Website: http://www.avancercorp.com/
To consult IAM Experts, **click here**.



© 2016 Avancer Corporation.
All rights reserved. All copyright in this presentation and related works is solely and exclusively owned by Avancer Corporation. This report may not be reproduced, wholly or in part in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this presentation), modified or in any manner communicated to any third party except with the written approval of Avancer Corporation.

This report is for information purposes only. While due care has been taken during the compilation of this report is to ensure that the information is accurate to the best of Avancer Corporation's knowledge and belief, the content is not to be construed in any manner whatsoever as a substitute for professional advice.

Avancer Corporation shall not be liable for any direct or indirect damages that may arise due to any act or omission on the part of the user due to any reliance placed or guidance taken from any portion of this presentation. Secondary information has been taken for the analysis is from the public domain.


[i] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
[ii] http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page
[iii] http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page