# AuthAnvil™
## for Healthcare IT

scorpion software | A Kaseya Company

# Executive Summary

The transition to Healthcare IT (HIT) is an important step towards improving the quality of care and overall health of patients, everywhere in the world. In the United States, several key legislative efforts have established policies to help increase the quality and efficiency of healthcare. To help modernize the system, the US government instituted stimulus packages like the American Recovery and Reinvestment Act (ARRA) to assist in the conversion of antiquated record keeping systems and reduce the overall long-term costs of records management, while helping deliver instant access to patient information.

Healthcare IT is becoming a key component to not only help reduce costs in healthcare, but for the United States to transform the nation's evolving economy. The potential net benefits of a stronger economy from a more digital healthcare system become more apparent when you consider annual savings of about $80 billion, relative to the total spending for healthcare of over $2 trillion per year[1]. Or the fact that the implementation of Healthcare IT is expected to increase employment of medical records and health information technicians by more than 20 percent through to 2018[2].

With benefits of both healthcare optimization and economic growth, Healthcare IT has to be carefully implemented in a way so that medical providers can continue to focus on patient care, and not be distracted with complex and expensive requirements in technology and compliance obligations. Especially when you consider the security that has to surround the protection of patient information.

This paper is written to help guide IT Service Providers through the labyrinth that has become healthcare IT. While it is focused on many compliance aspects of the United States' Health Insurance Portability and Accountability Act (HIPAA), much of the guidance provided here is still valuable to customers and partners using AuthAnvil Password Solutions globally. When thinking about Healthcare IT, think about data protection. That supersedes national borders and legislative governance of any one country.

# The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

## What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by the US Congress and signed by Bill Clinton in 1996[3]. Its original goals were to help protect health insurance coverage for workers and their families when they change or lose their jobs, and to establish national standards for electronic healthcare transactions.

The Department of Health and Human Services (HHS), has two specific reasons for pushing HIPAA:

1. To protect the confidentiality and security of patient health data by setting and enforcing standards;

2. To reduce costs and improve the efficiency of healthcare delivery through the standardization of electronic data interchange.

HIPAA established the "Privacy Rule" and the "Security Rule" for the handling and security of medical records. The Privacy Rule governs the use and disclosure of Protected Health Information (PHI) in any form (electronic, written and/or oral), while the Security Rule is concerned with the security standards for PHI in an electronic form (ePHI). We will be focusing on the Security Rule when discussing how AuthAnvil can help with Healthcare IT.

## Comparing the Privacy Rule to the Security Rule

The Privacy Rule requires that Covered Entities (CE) develop appropriate administrative, physical and technical safeguards for protected health information (PHI) and to reasonably implement those safeguards. The Security Rule is focused exclusively on protecting the confidentiality, integrity and availability of electronic PHI (ePHI). The key distinctions between the Privacy Rule and Security Rule include:

1. The Privacy Rule covers all forms of PHI (electronic, written and oral) where the Security Rule only applies to the EPHI that is created, received, maintained or transmitted.

2. The Privacy Rule contains several provisions requiring Covered Entities to implement safeguards for PHI. In contrast, the Security Rule provides specific requirements at a more granular level of detail.

## Who is Affected?

Any healthcare organization (HCO) storing health information electronically, or using electronic transactions for the exchange of such information, must achieve HIPAA compliance. In general, the following are considered to be Covered Entities (CE):

- *Healthcare providers* that engage in certain electronic transactions, including any healthcare provider that makes claims against a patient's health insurance;
- *Health plans*, including health insurers and group health plans; or
- *Healthcare clearinghouses* that translate electronic health transactions formats

But the affects aren't just to the CE. Business Associates (BA) and their subcontractors are also affected through the Health Information Technology for Economic and Clinical Health (HITECH) Act. Originally, this required the CE to maintain administrative, technical and physical safeguards to ensure confidentiality, integrity and availability of PHI. However, recent changes to the act make it a responsibility for those working with or for the CE to also comply.

For IT Service Providers this provides new challenges, as a material breach could costs tens or hundreds of thousands of dollars in civil fines and possible criminal penalties. The range in civil fines go from $50K to $1.5M... a crushing amount for IT firms, and usually not covered under traditional E&O insurance.

What's worse is that there are data breach notification requirement laws that differ between states. While the HITECH Act requires notification in 60 days, some states like Massachusetts requires it in 45 days. As a Business Associate, if an IT Service Provider should have known that a breach occurred through reasonable diligence (such as through IT monitoring and auditing) they may be liable under 'willful neglect' provisions. It is advisable that IT Service Providers understand their obligations under both federal and state laws. A good starting point for state specific data breach laws can be found on the NCSL website[4]. At this time 46 states have their own provisions. Only Alabama, Kentucky, New Mexico, and South Dakota have not declared specific state data breach laws.

In several states like California, the data breach notification law include private right of action provisions. This allows residents to file civil action against the Covered Entity and Business Associate that subjects the IT Service Provider to significant legal exposure and risk. The cost to defend such a civil lawsuit, regardless of merit, can be devastating to a small firm.

## Are IT Service Providers really liable?

As of September 23rd, 2013 all Business Associates are liable for compliancy regardless of whether they have a Business Associate Agreement (BAA) with the Covered Entity or not. In other words,

**it is by the "act" of being a Business Associate, not the contract**. As part of these provisions, a Business Associate needs to implement a full compliance program, which includes the management of subcontractors to create a *chain of compliance*. In accordance with the *HIPAA Omnibus Final Rule*, organizations that 'maintain' data are now considered Business Associates, even if they do not access the data directly[5]. This includes data centers, online backup providers, cloud service providers, hosted email providers etc.

One additional consideration is the use of remote monitoring and management (RMM) agents like Kaseya. The fact these agents have the ability to create conduits to access systems directly or indirectly that may host ePHI immediately make the provider a Business Associate. As does access to centralized security software management (think antivirus and antimalware), and mobile device management (MDM) solutions that have the ability to access the information.

> If you manage software that accesses servers, workstations or mobile devices that collect, host or access ePHI, you are a Business Associate.

## What are the Penalties for Non-compliance?

New changes to the HIPAA Security Rule removed 'harm' from the data breach law, making a breach assumed until proven otherwise… unless documented risk assessment shows "low probability" of release (e.g. validated device encryption like Bitlocker on a lost laptop)

Under the new rule, civil monetary penalties for noncompliance have been increased based on the level of violation. So any breach of ePHI, whether intentional or accidental, can potentially assess fines to an IT Service Provider of up to $1.5 million USD. Continued violation could go past that, with no theoretical maximum as it is up to the discretion of the US Department of Health and Human Services. And they have authorized the State Attorney General to enforce civil penalties.

The final Omnibus rule established four categories of violation and four corresponding levels of penalties based on the gravity of the violation. The new penalty structure is summarized in the table below:

| TYPE OF VIOLATION | EACH VIOLATION | REPEAT VIOLATIONS/YR |
|---|---|---|
| Did Not Know | $100 - $50,000 | $1,500,000 |
| Reasonable Cause | $1,000 - $50,000 | $1,500,000 |
| Willful Neglect – Corrected | $10,000 - $50,000 | $1,500,000 |
| Willful Neglect – Not Corrected | $50,000 | $1,500,000 |

The biggest burden now falls on Business Associates like IT Service Providers whose responsibilities are to manage and monitor the IT systems for Covered Entities like small medical practices. If an Attorney General from a state feels the firm has put one or more of their citizens at risk through willful neglect, such as offering "managed IT services" that explicitly are supposed to be managing and monitoring systems hosting ePHI and don't, they could assess fines of up to $50,000 per violation to the IT firm. Even if your business is registered in another state. As an example, the California Attorney General can sue a CE and/or BA whose business is based out of Texas, if a California citizen's patient information is breached. In states like California it gets worse, as the citizen can separately sue under the private right of action provision. This allows residents to file civil action against the CE and/or BA. Several class action lawsuits[6] are now starting to appear under this legislation.

Examples of the costs of breaches under HIPAA include:

- Walgreens had to pay an Indiana woman $1.44 million after her privacy was breached by a pharmacist[7].
- CVS Pharmacy reached a $250,000 agreement[8] with the Maryland Attorney General over willful neglect with patient data.
- Idaho State University was fined $400,000 by HHS after it was found their IT department disabled the firewall for over 10 months that was meant to protect patient data[9].
- Affinity Health Plan reached a $1.2 million settlement[10] with HHS for a data breach that happened over several years, when they failed to properly erase photocopier hard drives before sending them back to the leasing company.
- WellPoint fined $1.7 million by HHS for failing to secure[11] an online application database containing sensitive information.
- Massachusetts Eye and Ear Infirmary fined $1.5 million by HHS for not encrypting doctor's laptops and tablets[12] containing ePHI, including patient prescriptions and clinical data.
- Phoenix Cardiac Surgery was fined $100,000 for posting clinical and surgical appointments for its patients on a publically accessible Internet-based calendar[13].
- Hospice of North Idaho settles for an assessment of $50,000 for the theft of a shared laptop that was not protected under their mobile device management program[14].

These are just a few examples. From doctor's losing laptops to pharmacists leaking information about famous actors they were not supposed to have access to, it is important that IT Service

Providers demonstrate reasonable diligence in the protection of patient information that they may be exposed to or responsible for under their IT management duties.

# The AuthAnvil Solution in Healthcare

While HIPAA compliance by itself is applicable only to the entities covered in the regulations (healthcare organizations, their business associates and their subcontractors), the technical security controls employed in AuthAnvil meet or exceed HIPAA technical standards.

More importantly though, AuthAnvil excels at helping stakeholders in healthcare, like physicians and their staff, improve their quality of life while delivering better quality care to their patients. Some examples include:

- Using identity assurance protection like multifactor authentication to allow physicians the ability to finish necessary dictation, charting and data entry remotely instead of being shackled to their desk to access EMR systems.

- Allowing careworkers who are in the field immediate access to sensitive ePharma systems through mHealth (mobile health) with established password automation systems that are easy to access, audit and control.

- Making it possible through single sign-on for practice managers and their office staff to easily access web-based billing systems that interact with Health Plan systems without needing to know where to go or what passwords to use.

It doesn't end there. AuthAnvil helps IT Service Providers working in Healthcare IT to reduce business liability and associated risks. AuthAnvil aids in increasing appropriate safeguards and allows them to more readily demonstrate reasonable diligence and trust on behalf of their medical practice customers, to those organizations that enforce regulatory compliance governance, like the Department of Health and Human Services and the Centers for Medicare and Medicaid that fall under the Federal Information Security Management Act (FISMA). It helps to meet the technical objectives in the HIPAA Security Rule and delivers confidence to all parties concerned that the IT Service Provider has the custodianship of the systems responsible for producing, hosting and protecting patient data in good hands.

Let's explore ten ways in how AuthAnvil does that.

| | HIPAA Security Rule | How AuthAnvil Can Help |
|---|---|---|
| 1. | **Security Management Process**<br>164.308(a)(1): Information System Activity Review | • Streamline audit reviews with centralized access & activity reporting and logging. |
| 2. | **Workforce Security**<br>164.308(a)(3): Authorization and/or Supervision, Termination Procedures | • Centralize authorization – user, application and computer access controlled in one place<br>• Simple access revocation with just a few clicks when staff leave or are let go<br>• Built in audit reports to determine access to passwords of sensitive systems and the ability to automatically expire and change credentials as required |
| 3. | **Information Access Management**<br>164.308(a)(4): Access Authorization, Access Establishment and Modification | • Centralized user provisioning and access control through Role Based Access Control (RBAC)<br>• Open API to help enable transaction-level strong authentication to support audit integrity for ePrescribing, chart signing and Computerized Physician Order Entry (CPOE). |
| 4. | **Security Awareness and Training**<br>164.308(a)(5)(ii)(C): Login Monitoring<br>164.308(a)(5)(ii)(D): Password Management | • Centralize login monitoring and auditing of successful and failed login attempts to sensitive systems hosting ePHI.<br>• Simplify password management through a centrally managed system with built-in change management controls and change automation. |
| 5. | **Security Incident Procedures**<br>164.308(a)(6) | • Proactively report and alert on anomalous behavior relating to failed login attempts.<br>• Built-in auditing and assessment reports to test change management controls |
| 6. | **Workstation Security**<br>164.310(c) | • Enable console-based strong authentication requirements.<br>• Deliver temporary offline strong authentication through cached credentials tied to the user at the workstation. |
| 7. | **Access Controls**<br>164.312(a)(2)(i): Unique user identification<br>164.312(a)(2)(ii): Emergency access to ePHI | • Provide identity assurance through two-factor authentication, preventing credential sharing.<br>• Permit credential sharing for accounts like administrator and root while still binding the transaction to the individual.<br>• Enable emergency override procedures through security policy and temporary passwords. |
| 8. | **Audit Controls**<br>164.312(b) | • Centralize auditing of all workstation and application access through login and single sign-on audit logs. |
| 9. | **Person or Entity Authentication**<br>164.312(b) | • Implement strong authentication available in a variety of form factors to meet caregiver needs.<br>• Enable transparent authentication through single sign-on to validate entity access at time of request. |
| 10. | **Transmission Security**<br>154.312(e)(1) | • Provide endpoint validation for VPN and SSL through strong authentication.<br>• Enhance and promote secure access to web portals through single sign-on. |

## Regulations require Multifactor Authentication

The National Institute for Standards and Technology (NIST) updated their Special Publication 800-63 Electronic Authentication Guideline which, in conjunction with the Office of Management & Budget (OMB) Memorandum 07-16, applies to all Federal information and information systems, and requires "*remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access.*". Centers of Medicare & Medicaid Services (CMS) therefore requires this level of authentication for all access to information and information systems that contain ePHI.

The 2010 DEA Interim Final Rule for electronic prescribing of controlled substances adopted this same standard. The tightening of security requirements and enforcement procedures under the HITECH Act of 2009 makes serious consideration of these issues imperative in every Healthcare IT (HIT) system, and the HIT Policy Committee created by that Act has recommended that authentication for remote access to the Nationwide Health Information Network (NwHIN) must require at least two factors. In addition, at least two states (NY & CA) have adopted the same policy for state based HIEs.

AuthAnvil delivers this with AuthAnvil Two Factor Auth. It provides two-factor authentication through the delivery of single use one-time-passwords (OTP) from an app on the user's phone (called an AuthAnvil SoftToken), or through standalone hardware keyfobs and USB YubiKeys.

## Supporting Transparent Authentication

Under HIPAA Security Rule 164.312(a)(1) it is critical that users who hop around in different secure web-based applications, or different areas in the same application, can do so without the need to constantly enter credentials. Transparent authentication (TA), which can occur with the aid of single sign-on, should be a serious consideration.

# Best Practices for Access Management

Healthcare IT should be implemented with the ultimate goal of improving quality of patient care and without distracting caregivers with complex technology that will slow them down. This usually puts IT professionals at odds, as security requirements demanded by HIPAA can conflict with the need of the physicians and facilitators. It is a balancing act to protect patient information while giving access to those that need it most to promote patient, family and clinician collaboration.

Access management is critical for this to work. Understanding the technical requirements of Federal guidelines like OMB M-04-04 and NIST SP 800-63 help to align where AuthAnvil may be applicable when considering access management, especially taking into account the interoperability of access across systems that might fall under HIPAA compliance governance.

## OMB 04-04 E-Authentication Guidance

OMB Memorandum 04-04 defines four levels of identity assurance for electronic transactions requiring authentication, where the required assurance level is designed in terms of the consequences of authentication errors and the misuse of credentials:

- Level 1 - Little or no confidence in the asserted identity
- Level 2 - Some confidence in the asserted identity
- Level 3 - High confidence in the asserted identity
- Level 4 - Very high confidence in the asserted identity

## NIST SP 800-63-1

NIST SP 800-63 defines technical requirements at the four assurance levels in the areas of:

- Identity proofing and registration
- Tokens
- Management processes
- Authentication protocols
- Assertions

**Mapping OMB M-04-04 to NIST SP 800-63**

| M-0404 E-AUTHENTICATION LEVEL | NIST TECHNICAL GUIDELINES |
|---|---|
| 1. Little or no confidence that the asserted identity is valid | • Identity proofing *not* required<br>• Single Factor Authentication<br>• PIN or knowledge-based password |
| 2. Some confidence that the asserted identity is accurate. | • Online verification of identity elements<br>• Single Factor Authentication<br>• PIN or knowledge-based password |
| 3. High confidence that the asserted identity is valid. | • Identity proofing either *in-person* or *online*<br>• Online verification of identity elements *and* financial account information<br>• Multi-Factor Authentication |
| 4. Very high confidence that asserted identity is valid. | • PKI digital signature<br>• Biometrics<br>• Multi-factor Hardware token |

# Conclusion

When considering Healthcare IT, the dominating factor that needs to drive all decisions is to do everything reasonably possible under the circumstances to protect patient information, while enhancing the quality of patient care. It would seem these two objectives may be at odds, but the reality is that IT firms responsible for Healthcare IT must prevent inappropriate use and sharing of ePHI by medical professionals with legitimate access to the information. All while preventing access by unauthorized parties.

AuthAnvil is designed to help IT Service Providers do just that. It ties together proper user authentication and application access, while enabling proper privacy controls. One identity validated with strong authentication opens up access to required applications such as prescription orders and patient records through single sign-on (SSO). It eliminates the need for health practitioners to remember multiple passwords, while retaining a high level of security for each application. When systems cannot support enterprise-class SSO, AuthAnvil gracefully falls back to traditional password management enhanced with automation to eliminate the need for the health professional to get involved in changing or managing passwords, all while injecting the credentials on behalf of the user so they don't have to, giving them a similar experience to real SSO. AuthAnvil accelerates access, and medical staff spend less time fretting about login problems. All good things when having to tackle the world of Healthcare IT.

When properly implemented, AuthAnvil maintains the security of countless applications, tracks and logs access to systems containing ePHI, and speeds up access to critical information when needed most. It is an effective method of authorizing access to personal health data and resources, and holds both technical and medical staff accountable for their activities. By deploying AuthAnvil, an organization can substantiate that it has made a reasonable effort to protect patients' privacy by ensuring secure and reliable access.

## Want to learn more? Let's talk.

If you're interested in learning even more about how AuthAnvil can benefit your business and bolster your own compliance with HIPAA, have one of our authentication experts contact you for a no-obligation assessment of your current access management processes.

Let us ***show you*** how AuthAnvil can help you build confidence and trust with each and every practice you work with.

Let's talk!

# References

[1] Congressional Budget Office, Evidence on the Costs and Benefits of Health Information Technology: http://www.cbo.gov/publication/41690

[2] Bureau of Labor Statistics: http://www.bls.gov/ooh/Healthcare/Medical-records-and-health-information-technicians.htm

[3] Wikipedia definition of HIPAA: http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[4] National Conference of State Legislatures (NCSL) State Security Breach Notification Laws: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

[5] Clarity on HIPAA Omnibus Final Rule for Data Centers: http://www.datacenterknowledge.com/archives/2013/07/09/what-the-hipaa-final-rule-means-for-data-centers-and-cloud-providers/

[6] Class Action lawsuit against Advocate Medical Group: http://healthitsecurity.com/2013/09/06/patients-file-class-action-suit-v-advocate-medical-group/

[7] Walgreens HIPAA breach: http://healthitsecurity.com/2013/08/13/will-walgreens-breach-ruling-affect-future-hipaa-violations/

[8] CVS Pharmacy settles with Maryland AG: http://healthitsecurity.com/2013/08/30/cvs-agrees-to-250k-data-privacy-resolution-with-maryland-ag/

[9] Idaho State University fined for disabling firewall: http://healthitsecurity.com/2013/05/22/hhs-fines-idaho-state-university-400k-for-data-breach/

[10] Affinity Health Plan settles with HHS: http://healthitsecurity.com/2013/08/14/ocr-affinity-health-plan-reach-hipaa-violation-agreement/

[11] WellPoint fined for failing to secure database: http://www.esecurityplanet.com/network-security/wellpoint-fined-1.7-million-for-hipaa-violations.html

[12] MEEI fined for unencrypted laptops and tablets: http://www.hhs.gov/news/press/2012pres/09/20120917a.html

[13] Phoenix Cardiac Surgery fined for using iCAL: http://www.hhs.gov/news/press/2012pres/04/20120417a.html

[14] HONI settles HIPAA case: http://www.hhs.gov/news/press/2013pres/01/20130102a.html