

A perspective of compliance readiness of healthcare businesses as per Aegify.

Checking compliance and security, the Aegify way.

In 1996, the Health Information Portability and Accountability Act, most commonly known as HIPAA, was passed with one of its goals being to ensure uninterrupted coverage for patients. Health Care Organizations (HCOs) need to be able to pass patient records and other data back-and-forth. For this to happen efficiently and reliably, healthcare records would need to become more portable (hence the 'Portability' in the act's title). So the bill set forth new terminology and Electronic Data Interchange (EDI) code sets for transmitting data.

Page | 1

Two parts of HIPAA require attention:

1. The Security Rule (164.306), which establishes safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (PHI).
2. The Privacy Rule (164.502), which orders HCOs to protect PHI and defines the allowable uses and disclosures of PHI, in contrast to "de-identified" health information.

The assured portability of healthcare information plays a tremendous role in improving the safety, efficiency, and quality of healthcare. The act seeks to assure that anyone and everyone who participates in moving PHI from place-to-place accepts accountability that, at least in part, assures privacy.

Sweeping changes were made to the HIPAA privacy and Security Rules since they were first implemented with the Omnibus Final Rule, effective September 23rd, 2013.

Protected Health Information (PHI) includes any data, including demographic information that relates to any of the following:

- An individual's past, present or future physical or mental health or condition.
- The provision of healthcare to an individual.
- The past, present, or future payment for the provision of health care to an individual that also identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, and Social Security number).



The vast amount of communication for PHI is electronically exchanged whether through email, mobile devices or wireless networks. These transmissions need to be protected out of compliance with industry regulations for data privacy. The new regulations also put HIPAA enforcement in the hands of the Office of Civil Rights (OCR). Together, the OCR and the Federal Trade Commission (FTC) are increasing their scrutiny of HCOs and imposing penalties more severe than any imposed during the first decade of HIPAA enforcement.

How Does HITECH Impact Healthcare Providers?

The growing activity of identity theft, medical billing fraud, and other negligence have resulted in a financially debilitating effect that prompted the enactment of the American Recovery and Reinvestment Act (aka the "stimulus package") in 2009. The act also contains the Health Information Technology for Economic and Clinical Health (HITECH) Act and the new HIPAA regulations, which has the effect of

expanding the reach and impact of HIPAA—most importantly the penalties and patterns of enforcement.



What is meant when we say “expanding the reach and impact” is that the HIPAA/HITECH law now not only applies to healthcare providers, referred to in the Act as “Covered Entities,” and to medical providers, who offer medical services to end-customers, but also to any Business Associate that shares protected health information with Covered Entities or medical providers.

A Covered Entity could be any of the following organization that transmits information in electronic form for which HHS has adopted a standard:

Healthcare Providers	Health Plans	HealthCare Clearinghouses
<ul style="list-style-type: none"> • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies 	<ul style="list-style-type: none"> • Health insurance companies • HMOs • Company health plans • Government programs that pay for healthcare, such as Medicare, Medicaid, and the military/veterans' health care programs 	<ul style="list-style-type: none"> • Entities that process nonstandard health information received from another entity into a standard electronic format or data content, or vice versa

The above are impacted only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

Many Covered Entities discover gaps in their relationships with Business Associates:

- Determining the most important questions to ask Business Associates about privacy and security practices.
- Deciding which provisions are essential to include in Business Associate agreements.
- Identifying how Business Associate management differs based on the type of vendor involved.

Business Associates, which are now completely in scope with respect to HIPAA regulations, include the following entities:

- Third-party administrators that assist health plans with claims processing.
- CPA firms whose accounting services for healthcare providers involve access to PHI.
- Attorneys whose legal services for health plans involve access to PHI.
- Consultants that perform utilization reviews for hospitals.
- Healthcare clearinghouses that translate claims from a non-standard format into a standard transaction on behalf of healthcare providers and forward processed transactions to payers.
- Independent medical transcriptionists that provide services to physicians.
- Pharmacy benefit managers that manage health plan pharmacist networks.
- Other business partners.

The law extends not only to companies, CEs and BAs but also to individuals who work within them, making everyone who handles PHI personally accountable for their actions and exposed to strong incentives for investigators to uncover violations that can lead to the assessment of heavy fines and/or penalties.

Business Associates who routinely exchange or access the PHI of any Covered Entity may be subject to all the same privacy and security rules as the Covered Entity itself. The act requires Covered Entities to develop and implement comprehensive written PHI security policies and procedures while also making provisions for auditing of all Business Associates by the federal Department of Health & Human Services (HHS). Failure to comply can easily incur penalties. The act also requires breach notification to patients, HHS, and even major public media outlets.

With the Omnibus Rule implementation effective March 26, 2013, a significant change in the final rule relates to the definition of Business Associates, which now also includes BA subcontractors. Previously, if a BA engaged a subcontractor to assist in the performance of the Business Associate's services, then the BA merely had to "ensure" the subcontractor would comply with the terms of the Business Associate's agreement with the Covered Entity. The definition of BA was also revised to include health information organizations, e-prescribing gateways, and other entities that provide data transmission services and which require access to PHI on a routine basis, as well as entities that offer a personal health record product.

In addition, the Omnibus Rule directly mandates BA compliance with many of the requirements of the privacy and security regulations. Whereas before Business Associates were bound only by the terms of their Business Associate agreements, Business Associates (the definition of which now includes subcontractors) now must comply with parts of the regulations in their own right, and are subject to enforcement along with Covered Entities. This requires Business Associates to implement HIPAA compliance initiatives and measures

Aegify Post-Implementation Benefits:

- New efficiencies and simplification of the compliance process
- Timely management of updates
- Support for managing Business Associate compliance status
- Reporting to quickly identify organizational compliance status
- Simple-to-follow guide for implementing remediation changes
- Regulatory-based policies and procedural templates that the staff can tailor
- Subject-matter-experts to consult with for managing risks

Each of these benefits allows the internal staff to focus more time on other operational responsibilities.

Face OCR Audits with Confidence

As per reports healthcare data breaches have reached a near 138%. The Department of Health and Human Services' Office for Civil Rights, therefore, unveils its second round of audit program. Unlike the previous ones, this time, the OCR is looking to conduct audits across all high-risk areas. While this eliminates on-site visits, they are looking towards potentially integrating the audits into OCR's formal enforcement program.

While the audits for **HIPAA compliance** have become more common, many of the healthcare providers are not still effectively prepared for an audit. These healthcare providers and their business associates may, therefore, face serious consequences during the next round of OCR audits. What the healthcare providers need to understand is that while the Office of civil Rights is not out to get them, they definitely expect the healthcare enterprises to faithfully take good efforts to protect their vital patient data. Even after two years of 2012 OCR pilot program audits, the covered entities and business associates need to look for more effective measures to protect themselves and not fall victims to past mistakes.

In fact with technology being integrated into the audit process, the healthcare providers need to learn from their past mistakes and **be ready to face the OCR audits**. The 2012 OCR audits helped to expose the gaps in the healthcare compliance such as:

- Minimum to near to nil protection with absence of even the basic security tools and methods to identify vulnerabilities leading to exposure of patient data
- Clueless about the identification of data location while allowing anywhere anytime access to the data from the various handheld devices.
- Unavailability of training sessions for employees or techniques for data monitoring and reporting of data breaches.

Since the department of health and human services has recorded more than 500 cases of **data breaches** affecting 33 million PHI's in its wall of shame, the covered entities, and their business associates need to understand that OCR audits act as a vehicle to help them efficiently monitor HIPAA regulatory compliances. However, as the first step to the process, these establishments need to conduct a risk assessment to identify areas of vulnerabilities.

Nevertheless, with HIPAA dictating the need to protect PHI's, the covered entities and their business associates need to deploy more strategic methods that will help them identify the risks faced by their data. Deploying comprehensive security management solutions such as Aegify Security Posture Management and Aegify Secure GRC will help these healthcare providers face the OCR audits with confidence.

HIPAA Audits: Documentation Is Key

The Department of Health and Human Services' Office for Civil Rights has unveiled the new look of its Phase 2 audit program. Highly unlike the previous ones, the Phase 2 audit program will be seeing the OCR conducting audits, concentrating on high-risk areas, eliminating on-site visits, and potentially integrating the audits into OCR's formal enforcement program.

[A quick glance at what the Phase 2 audit program entails](#)

With the Phase 2 audits being conducted chiefly by OCR staff, this is likely to involve a slightly different methodology than previous audits. Unlike the comprehensive Phase 1 audits, Phase 2 audits are likely to be more narrowly focused. The OCR intends to audit 350 covered entities and 50 business associates. Concentrating on the compliance with requirements related to the notice of privacy practices and patient access to protected health information, the OCR will audit 100 covered entities on the Privacy Rule, and for the first time, business associates are to be included in these audits. OCR will request a list of business associates from covered entities.

The OCR has implied that the Phase 2 and future audits' adverse findings could lead to civil monetary penalties or a resolution agreement. The estimated "Round 2" of Phase 2 audits and those conducted in 2016 and beyond, are likely to focus on device and media controls, transmission security, Privacy Rule safeguards, encryption and decryption, physical facility access controls, breach reports, and complaint processes. However, there may be a significant impact on how the audit program ties to enforcement, keeping in mind that the OCR leadership is likely to change soon.

[Some of the differences](#)

This time, the OCR will audit 150 covered entities on security focusing on risk analysis and a corresponding risk management plan. The OCR learned in Phase 1 that with no address confirmation, a hard copy audit notification can take forever. This is why in summer 2014, the OCR gathered pertinent

details from 550 to 800 covered entities to get hold of information required for choosing a suitable sample. Following this, the OCR will follow up in fall 2014 with notifications and data requests to 350 covered entities. Taking into consideration the deficiencies identified in Phase 1, most of the Phase 2 topics are to be based on the same. Also unlike Phase 1, OCR does not intend for Phase 2 audits to include on-site visits. It may, however, return to on-site audits in the future, in the case of availability of additional funds.

[Here's how to prepare for the Phase 2 audits](#)

Having complete documentation of every aspect of your privacy and security strategy is the best way to prepare for an HIPAA audit, using the built-in documentation management system in Aegify.

If HIPAA compliance auditors discover an organization cannot produce adequate documentation, they'll suspect its compliance efforts are subpar.

Healthcare organizations need to have a long list of documents ready. Among those are:

- Security and privacy policies and procedures;
- A risk assessment and corrective action plan;
- An organizational chart outlining privacy and security responsibilities;
- A technology inventory, including all security tools used;
- Business associate agreements;
- An incident response plan; and
- HIPAA compliance training materials.

[Preparing for OCR Audits May Not be the same –A Few Tips to see you through](#)

All covered entities and business associates can keep in mind the following tips while preparing for the audits.

- Besides having an effective risk analysis, make certain your risk analysis detects & categorizes risks instead of simply documenting that controls are in place or recording the gaps in compliance with the Security Rule.
- It is essential that all policies need to be up to date, especially in case of:
 - Breach notification, risk analysis, and risk management (for both covered entities and business associates)
 - Notice of privacy practices and patient/enrollee access (only for covered entities)
- Make sure that all additional documentation associated with the above topics are easily accessible and clear in :
 - Breach investigations and risk assessments, risk analyses, and risk management plans (for both covered entities and business associates)
 - Responses to patient requests (for covered entities only)
- In the event of no patient acknowledgment, documentation supporting the reason why an acknowledgment was not obtained need collection. It is important to know how to gather documentation of patient acknowledgments of receipt of the notice of privacy practices.
- Keep an up to date record of business associates with relevant contact information (only applicable to covered entities).

It is a known fact that all health information must be viewed and safeguarded just like any other business asset. Healthcare entities need to conduct a reality check and prepare themselves with thorough risk assessments. Every covered entity needs to clearly understand the privacy and security rules and take a realistic approach to identifying potential threats and vulnerabilities in their systems that could put the confidentiality, integrity and availability of health information at risk. Implementing comprehensive security management solutions like [Aegify Security Posture Management](#) and Aegify SecureGRC can prove handy at this juncture, and help entities face the upcoming audits with confidence.

Meaningful Use Incentive Payments – OIG Audits Begin

The OIG (Office of Inspector General, US HHS Department) 2015 audits will focus on:

- The extent to which hospitals comply with the contingency planning requirements of HIPAA in terms of establishing policies and procedures for responding to any emergency or events that could compromise protected health information.
- How truly were the providers entitled to meaningful use incentives and how effective is the oversight of CMS (Centers for Medicare & Medical Services) on security controls over networked medical devices integrated with EHR Systems
- Adequacy of covered entities and business associates in securing electronic patient protected health information created or maintained by certified EHR technology and whether hospitals have conducted the required security risk analysis.

When you get an audit notice do you feel stressed? CMS audit rate is about 5% of facilities that have attested and according to Figliozzi and Co, “there’s a 4.7% failure for first-time audits”.

The reasons for failure could be due to some common myths surrounding the security risk analysis:

- 1) One security risk analysis is good forever – No. HIPAA Compliance mandates that you review the security risk analysis periodically.
- 2) My EHR vendor takes care of this – No. The EHR vendor is only responsible for providing you a certified system. Privacy and Security of your ePHI and having a complete security risk analysis conducted is solely your responsibility.
- 3) The security risk analysis is optional for a small practice like mine – No. Covered Entities, whatever the size, are required to conduct /review a complete security risk analysis under HIPAA guidelines.

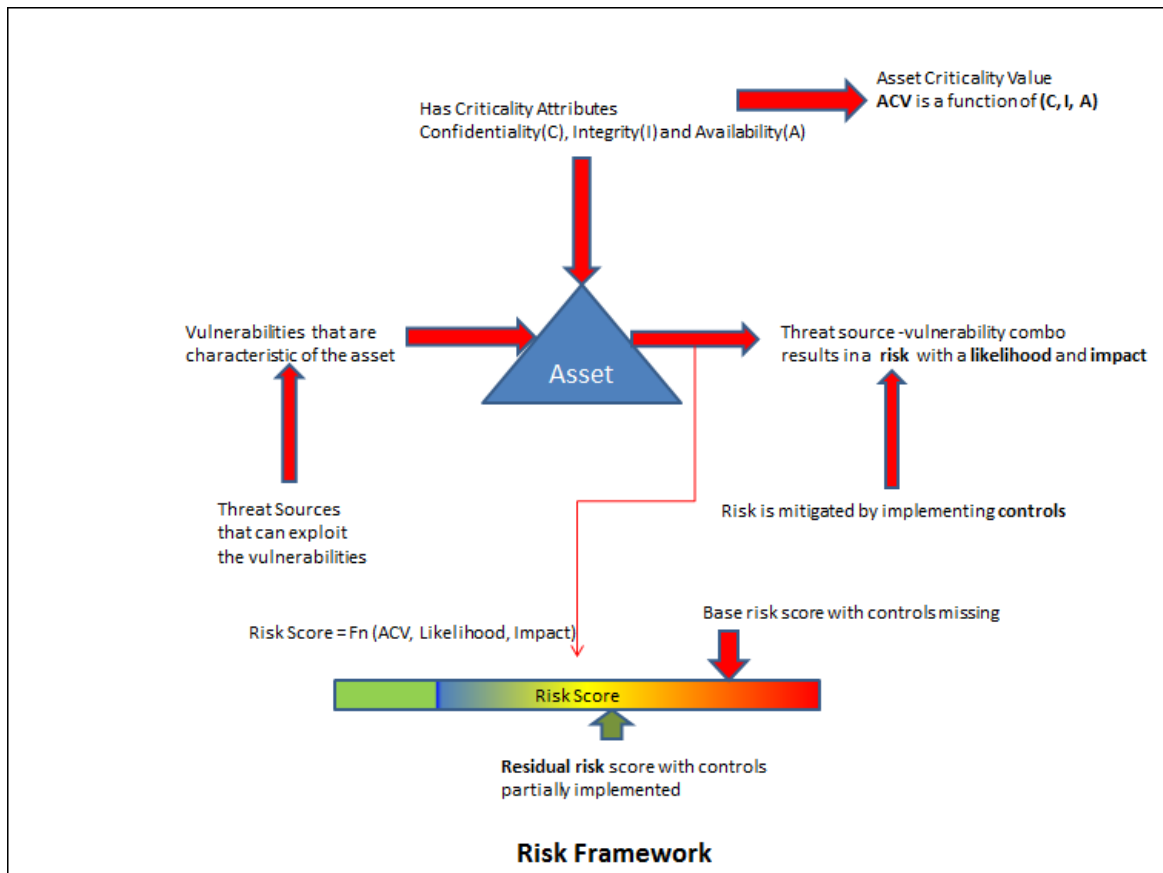
Audit letters are being sent out by OIG for documentary evidence of compliance with the particular meaningful use measures such as calculation reports printed from the EHR system, and security risk analysis reports. A study by OIG found that the estimated incentive payment of \$6.6 billion between 2011 and 2016 to professionals and hospitals is vulnerable that incentive payments could be made to those that do not fully meet the meaningful use requirements. OIG recommended in their November 2012 report that CMS should obtain and review documentation from selected professionals and hospitals and provide guidance on documentation procedures to establish and maintain compliance.

In submitting a response to the question on meaningful use measures you would be confirming that “you have conducted or reviewed a security risk analysis in accordance with the requirements of 45 CFR 164.308(a)(1) and implemented security updates as necessary and corrected identified security deficiencies as part of the risk management process.” The security risk analysis must be done at least once before the end of the reporting period being attested. Thereafter, you must review the security risk analysis before each reporting period that follows. All security deficiencies and/or breaches

identified during a risk analysis must be comprehensively addressed. Covered Entities, irrespective of their size, must treat the requirement to conduct a security risk analysis as a license to practice.

Businesses across the healthcare industry and its verticals, therefore, need to scan their PHI assets and conduct security analysis besides ensuring meaningful use of the EHR. Aegify has been developed as a **comprehensive security, risk, and compliance management** solution that not only addresses all of **HIPAA compliance** needs but also provides the covered entities with meaningful use attestation reports with proof of security and risk analysis. Further, Aegify automates HIPAA management through continuous workflow assessment cycle and provides instant remediation measures to correct the security deficiencies, a trusted Solution by 70+ MSPs with numerous customers. Aegify protects your assets, detects vulnerabilities proactively, and responds with appropriate remedial measures. Aegify is the only solution that unifies a comprehensive Security, Risk, and Compliance Assurance system.

A cloud-based Aegify walks you through simple steps in your risk analysis and management and helps you face the OIG audit on risk analysis through effective automated processes and documentation reports. Aegify Risk Framework is comprehensive:





The Aegify Risk Management Service meets the risk assessment methodology best practice as shown below:

Best practice	Aegify Risk Management Service
System Characterization	Manage Assets
Threat Identification	Assessing risk levels
Vulnerability identification	Configure risk settings
Risk determination	

Control analysis Control recommendations	Assess Compliance
Likelihood determination Impact analysis	What-if analysis
Results Documentation	Risk reports

Aegify’s automated risk management module helps you keep track of documents required as part of required evidences. Extensive report generation facilities provide an online resource with the following simple steps. Page | 8

 1. <u>Configure Risk Profile</u>	<ul style="list-style-type: none"> • Select Standards / Regulations against which the customer need to assess the organizational Risk. • Applicable controls to assets are identified based on the selected Risk Profiles here.
 2. <u>Manage Assets</u>	<ul style="list-style-type: none"> • Add assets, manually or through automated scan-based asset discovery, or from an uploaded asset-list file. • Define Asset attributes for each asset. • Assess the security risk for each asset.
 3. <u>View Dashboards/ Reports</u>	<ul style="list-style-type: none"> • View perspective-based security risk posture. • Generate risk reports for analysis.
 4. <u>Assess Risk Controls</u>	<ul style="list-style-type: none"> • Publish Risk Assessments or review risks from published and responded assessment. • Generate risk assessment report.
 5. <u>Do What-if analysis</u>	<ul style="list-style-type: none"> • Simulate various risk scenarios by changing risk parameters. • View security postures at different levels of risk settings. • Prioritize remedial actions based on what-if analysis.
 6. <u>Configure risk settings</u>	<ul style="list-style-type: none"> • Review and modify asset types. • Review risk scenario of each asset types and customize risk settings for different assets. • Work with various mitigation strategies in respect of non-compliant controls for meeting the regulatory control requirements. • Customize the list of ever-changing threat sources and vulnerabilities.

The default settings would normally be adequate in identifying and managing assets, assessing the risk levels of all or selected assets, assessing compliance with regulatory risk controls, and for doing detailed what-if analysis by changing various parameters in the risk assessment process. However, where risk configuration needs more customization to meet the specific characteristics of an organization the risk configuration settings provide the advanced customization options.

Offered as a cloud-based model, Aegify includes all security and IT GRC functions. Equipped with a built-in compliance framework that supports HIPAA, RBI, NSE, BSE, MCDEX, PCI, ISO, COBIT, FISMA and other



country based ones, Aegify also has advanced alert and monitoring systems that makes it a complete end-to-end automation solution for all security, audit, compliance and risk management needs of an enterprise.

Aegify offerings:

Compliance Management Through Aegify has been available for many years. Accompanied by complete vendor management support, the solution continues to support multiple compliance business frameworks such as PCI, HIPAA/HITECH, SOX, FISMA, and GLBA. Page | 9

Aegify Risk Manager: Provides risk analysis that identifies all assets that capture, process, store, and transmit ePHI as well as threats that can exploit the vulnerabilities in such assets. You mitigate the identified risks through implementation of HIPAA Security Rule controls assessed for their state of compliance. The report on controls found to be non-compliant come with recommended remediation that covers relevant security rule controls, gaps identified in the security requirement, and the recommended set of remedial actions.

Security Posture Management (SPM) – Aegify SPM is powered by the Rapid7 Nexpose vulnerability management engine, which scans physical and virtual networks, databases, operating systems and Web applications to enable customers to remediate vulnerabilities and misconfigurations as well as enforce policies. The solution supports interoperability with other standard, industry-based scanners such as Qualys, Nessus, and Retina.

Customers can purchase and deploy Aegify Security Posture Management (SPM) or Aegify Compliance Manager separately or combined with each other as an integrated solution.

eGestalt offers both Aegify solutions through four editions to cater to different business requirements: **ULTIMATE, PROFESSIONAL, STANDARD, and COMMUNITY.**

