Ostendio

MyVCM™
Trust Network

A Buyer's Guide to Managing Compliance

Table of Contents

Who Should Read This Guide?

Whether you are just establishing your compliance program, looking to extend compliance across your existing value chain, or need a way to more easily demonstrate your compliance, this guide is for you.

Any organization that has access to personally identifiable data (PII) or protected health information (PHI) must ensure they are securely handling that data in line with standards and regulations.

Managers and executives in any of these organizations need to understand current compliance obligations:

- Digital Health Companies – innovative IT companies needing to work with regulated entities
- Hospitals and Health Systems – seeking to take advantage of cloud-based and mobile healthcare solutions being developed by digital health companies
- Clinics and Practitioners – interested in providing the best healthcare service, but are worried about compliance
- Medical Colleges and Associations – interested in advancing their specialties through clinical trials and research
- Medical Device Manufacturers – interested in improving individual healthcare though patient-oriented hardware advances

Having a defensible compliance program is not an option; it's required to do business in today's health industry. In this guide we'll explain the needs and approaches for compliance to standards and regulations including HIPAA, NIST, OSHA and FDA.

Introduction

The health care regulatory environment is complicated. Whether it's HIPAA, OSHA, FDA, NIST or a host of other regulations and standards, there's a good chance your organization is covered by one or more of them. A solid information security and compliance program will help your organization manage and demonstrate compliance to the regulatory authority or standards bodies you are governed by.

As with most regulations and standards, the rulings on health care compliance continue to evolve. Unfortunately, pleading ignorance of the law won't get you very far with most of the regulators. For example, the term "did not know" is actually one of three penalty categories for violating the new HIPAA-HITECH rules, along with "reasonable cause" and "willful neglect." All of them come with penalties. In the "did not know" category, a breach can cost you between $100–$50,000 for each infraction.

Enforcement is not just in hospitals and healthcare systems anymore. HIPAA – HITECH extends responsibilities deep into the value chain of healthcare. While the previous rulings included covered entities and business associates, the new rulings include secondary business relationships and consultants; basically everyone who might have contact with PHI is now liable.

And the likelihood of getting caught is rising, as the US Department of Health and Human Services (HHS) has been training state attorneys general who, through the HITECH act, are empowered to bring civil action on behalf of their residents for HIPAA-HITECH violations. The chances of being reported are also increasing— mandatory disclosure of breaches were the highest yet in 2014, and is growing at a rate to exceed those totals in 2015. And many states allow consumer reporting of violations at any time.

But it's not all doom and gloom. There are a lot of benefits to a "healthy" compliance program including:

- Boost revenues – a good compliance program can help a healthcare system provide the latest in innovative services by taking advantage of

cloud-based and mobile solutions. And Health IT providers can grow and prosper as long as the compliance ecosystem is functioning properly.

- Reduce risks – a good compliance program reduces risk throughout the entire value chain. If every organization can attest to compliance in a standard way, the cost of compliance can be reduced and the level of compliance certainty can be improved.
- Focus on healthcare – a good compliance program allows every organization to focus on healthcare, not compliance. Compliance becomes part of the culture, not an interruption to be dealt with.

Let's start by understanding the origins of the need for compliance management.

Since the enactment of HIPAA and other healthcare regulations, there have been three unprecedented shifts within the health industry:

- An industry-wide shift from paper to electronic health records;
- A move from fee-for-service to more quality- and cost-focused practices
- And the availability of mobile and cloud based technologies that now make it easier to store, analyze, and deliver information instantly.

As a result, there is acceleration in demand for technologies to analyze data, engage patients, and reduce costs. Healthcare IT executives are increasingly looking towards the cloud to reduce costs and obtain greater flexibility.

But the majority of innovation arising from the $7 billion invested[1] in Digital Health last year is not coming from within Hospitals and Health Systems; it is coming from the roughly 7,000 digital health companies who provide mobile and cloud-based solutions.

Now Hospitals and Health Systems face a dilemma. If they embrace these new cloud-based technologies, they increase their risk of a breach as they

[1] Start Up Health Insights™ Digital Health Funding Rankings - Q3 2015 Report

share sensitive data with many cloud-based vendors. This risk is compounded by the following factors:

- Health data is becoming increasingly more valuable to hackers with a health record cited as being between 10-50 times more valuable than financial data. According to the World Privacy Forum, a stolen credit card or Social Security number fetches $1 or less on the black market—but a person's medical information can yield up to $500.[2] 2015 was already being cited as the year of the healthcare breach before the largest singe breach in US healthcare history was announced in January[3] (Anthem/80,000,000 records)

- Healthcare IT infrastructure is aging and only about 3% of IT Budgets are allocated to Security. This is forecasted to increase ten-fold as entities grapple with increasingly sophisticated attacks. (Forbes.com)

Bottom line, if you or your IT systems collect, process, or transmit any of this information, you are at risk and should have a defensible compliance system in place.

Different Approaches to Managing Compliance

There are three vastly different approaches to managing compliance that vary in cost, time, and work required.

DIY approach

DIY (do it yourself) is usually reserved to the larger organizations that can dedicate staff and resources to develop and manage an acceptable risk management plan (RMP) for their own internal use. Typically these are custom built plans designed for the specific needs of the organization. This is the most expensive approach due to the resources it consumes within the

[2] Aberdeen Group 2014
[3] Wall Street Journal 2015

business. This approach does not scale well and is not recommended for smaller organizations.

Audit approach

Bringing in a specialist to help establish your compliance program is a good first step. A good auditor will start by conducting a Risk Assessment. An auditor visits your location, verifies what safeguards have been implemented, completes a risk analysis, and essentially outlines a risk management plan for you. This process usually takes one to three months. However, this can be expensive. Depending on your organization and the PHI it handles, an annual HIPAA audit can range from $17,000 to $59,000 depending on scope and complexity[4].

However an effective security and compliance program is not just a one time or once a year effort. It requires ongoing management. Companies must build security into their everyday business processes and train all employees on the principles and best practices.

Cloud Solution approach

This method gets its name because the companies in the space use software as a service (SaaS) as a means of assessing risk, defining a RMP, and ongoing compliance management. In these solutions, best practices are replicated and standardized across the company's client base. Security and compliance experts work with you remotely to prioritize threats found in your risk analysis.

If you find a good Compliance SaaS vendor, they guide you through the creation, implementation and management of a RMP. We recommend that you look for a solution that addresses both the initial development and ongoing management and improvement of your compliance program. We also recommend you look for a solution that covers multiple standards and regulations and is not limited to HIPAA.

[4] "What Does a HIPAA Audit Cost" Caltayze.io blog 2015

A good cloud solution incorporates a workflow solution to help you manage the ongoing tasks that are a critical part of a compliance program. These include employee training, document management and asset management.

The cost of a cloud-based solution varies but typically if a company has an established program and leverages a good SaaS based workflow solution; the audit process is typically quicker, easier and cheaper.

Implementing a Compliance Program

There are four broad phases involved in establishing and managing a compliance management program. Each of these efforts must be completed and continuously managed as part of a defensible compliance program.

First – Conduct a Risk Assessment

The first phase, Risk Assessment or Analysis is designed to accurately and thoroughly identify vulnerabilities and threats that impact PII or PHI. The outcome of the assessment is then used to assess the potential risks to the confidentiality, integrity and availability of PII/PHI located or held at the company.

The Risk Assessment should follow industry best practice standards as described by organizations such as US Department of Health and Human Services (HHS) or NIST, and performed no less than one time a year or after successful implementation of any major system change including an office relocation, replacement of EHR system containing PHI, etc. A Risk Assessment should include but not necessarily be limited to:

- IT Risk Assessment – how secure is your physical infrastructure
- Security Awareness – the easiest way for an attacker to gain access to your business network is through the weakest link- your employees
- Policies and Controls – do you have comprehensive sets of policies and procedures in place to govern your security and compliance

Second – Implement a plan to Manage Identified Risk

Once the assessments are completed, any gaps must be addressed in an organized and timely manner. The Risk Management Planning Phase is the compliance step that works through issues discovered in the risk analysis and provides a documented instance proving your active acknowledgement (and correction) of risks against regulatory requirements.

Third – Demonstrate Compliance Progress

It is not enough to take the steps to plug the compliance gaps and address risks. You also have to demonstrate evidence of compliance. Whether you need to demonstrate your compliance program to a client or a regulatory authority, you must have documented evidence in place that you have conducted the necessary actions. Documented evidence offers substantiation and verification of policy compliance by providing confirmation of timely performance of recommendations detailed in the Risk Management Plan.

Finally - Continuous Improvement

Compliance is not a one-time activity. Once you have a solid compliance program in place, you must continue to manage and monitor it to ensure your organization remains compliant and is actively managing risk.

Assessing Compliance Management Solutions

Now that you know the types of solutions available, and the components of an effective compliance solution, how do you know which one to choose?

Since compliance is a requirement, you should select a solution that helps you accomplish the following:

- Does it help me build a culture of compliance?
    - Make sure the solution reinforces support of top management because a culture of compliance starts at the top. Solutions that

provide critical executive reports and dashboards keep executives engaged in the program.

  - Make sure the solution helps you teach employees how to recognize and address compliance issues. Training should be an on-going process with employees revisiting topics regularly. The best solutions track individual progress and set reminders to help employees stay current.

  - Make sure the solution helps you learn from mistakes. Mistakes will happen. Look for a solution that helps you recognize mistakes and discuss how policies can be adapted. It should also help you communicate and implement a plan on how others can avoid these similar situations.

- Does it boost security and privacy capabilities?
  - The solution should allow you to conduct regular risk assessments to ensure proper technologies and techniques are in place to prevent and detect data breaches. It should also help you launch and manage employee training and awareness programs on handling sensitive and confidential information.

- Does it help me keep pace with a changing compliance landscape?
  - A solution should help you stay current on the latest rules and regulations supporting your business. Look for solutions that provide regular updates supporting new legislation and helps you manage conflicts of interest in competing guidelines. The solution should help train your employees on the latest compliance issues and identify possible third-party risk.

What to look for in a Vendor

Now you know what your solution should provide, the next step is to select a vendor that meets your needs. In general you should select a vendor that has the following traits:

- Experience – Compliance is a complex subject. It combines legislative know how, technical ability, and organizational awareness. Look for a vendor that demonstrates capabilities in each of these areas.

- Customers – Nothing breeds success better than success. Look for a vendor that has customers that will openly recommend its services.

- Multiple Standards and Regulations – Companies typically have to comply with multiple standards and regulations. Look for a vendor who will support multiple standards and regulations and not just HIPAA.

- Support – Product is not the only factor in decision making. Look for a vendor that provides the comprehensive and responsive support you need to be successful. It does not good to select a solution you can't understand and can't find anyone to help you.

- Flexible pricing / contractual arrangements – Don't get locked into complex arrangements with your vendor. Look for pricing models and agreement that can scale with your business.

- Security/ Privacy – It goes without saying that firm specializing in security and privacy compliance needs to demonstrate that their operations are secure.

- Robust infrastructure – Make sure your vendor has the capacity to help you in your compliance efforts. Select vendors that can prove they have the capacity to scale with your needs.

Other Considerations

There are other considerations to take note of when selecting a solution. It's good to know the full impact of your choice.

- Understand if and how a vendor's product will impact the key goals of the business. Some solutions can help you short cut acceptance times

when onboarding a new customer or supplier because they readily demonstrate currency in compliance efforts.

- If the solution is not SaaS-based, clarify pricing, including costs for hardware, software, implementation assistance, training, interfaces, and ongoing network support and maintenance fees. These can add to the total costs of the solution.

- Clarify roles, responsibilities, and costs for a data migration strategy if needed. Sometimes, being selective with which data or how much data to migrate can influence the ease of transition. If these are not clear there may be some wasted efforts and false starts during the engagement.

- Make sure the vendor's product is able to document meaningful use. You not only have to prove you're secure; you also need to prove you need the data in the first place. This capability ensures you have a complete solution.

- Consider whether you will replace your compliance management system and how you will handle the conversion or interface. A proper plan will help smooth transition.

- Consider costs of using legal counsel for contract review. If the contract is complex, it may cost you to have it reviewed and negotiated.

Conclusion

The increasing pressure to implement meaningful use, reduce healthcare costs, and improve care outcomes while still protecting patient interests has led to strategic review and overhaul of the value chain by many healthcare providers and vendors. Expanding solutions to include innovative cloud-based, mobile, and personal solutions are an obvious part of the equation.

However, balancing the medical advances and resource benefits of the solutions with the risks of engaging an off-premise business associate is daunting in the wake of increasing PHI (protected health information) breaches and penalties.

Ultimately, finding the best blend of resources that can fulfill the availability, integrity, and confidentiality requirements to protect ePHI - and thereby protecting the patients, covered entities, and business associates - is the challenge at hand.

Obtaining full HIPAA-HITECH compliance is achievable and necessary. There are specific steps you can take to protect the client's PHI, your business and your career. Consider adopting a compliance management solution to ensure you'll have a better response than "I didn't know.

If you have any additional questions or need help developing or improving your compliance program, please contact us at info@ostendio.com.

✔ Checklist: 10
Questions to Help With Solution Selection

As you narrow down your choices for Compliance Management, use this checklist to make sure the solution and its provider are going to meet your immediate and long-term needs.

Solution	Yes	No
1. Does it help me build a culture of compliance?		
2. Does it boost security and privacy capabilities?		
3. Does it help me keep pace with a changing compliance landscape?		
Vendor		
4. Experience – Does the vendor demonstrate capabilities in legislative know how, technical ability, and organizational awareness?		
5. Customers – Does the vendor have customers that will openly recommend its services?		
6. Multiple Standards and Regulations – Does the vendor support multiple standards and regulations and not just HIPAA?		
7. Support – Does the vendor provide the comprehensive and responsive support you need to be successful?		
8. Flexible pricing / contractual arrangements – Does the vendor have pricing models and agreement that can scale with your business?		
9. Security/ Privacy – Has the vendor demonstrated that their operations are secure?		
10. Robust infrastructure – Can your vendor prove they have the capacity to scale with your needs?		