

Trends in Compliance - Will you be HIPAA Security Compliant in April? How about six months after that?

Background

When the first question was recently posed to several security and compliance officers from a variety of healthcare firms, their lack of response spoke volumes. Many of these firms had begun to create and assign roles to evaluate the issue, but they had not completed their initial inventory of current security policies, practices, procedures and controls (PPP&C) or gap analysis and did not have enough information to determine the answer to the question. Many of them were also concerned that they did not have particularly large budgets to address the problems they might find. Additionally, the organizations were so swamped in doing these initial steps that many had not stopped to consider long term implications versus their short term compliance needs. For instance, while you become compliant at some point will you be compliant the next quarter after you have added some new technologies or begun a new information sharing program? The compliance process is not a one time event but an ongoing lifecycle of continual improvement. This paper provides some thoughts about how your compliance work today can be molded into an ongoing process.

Compliance process description

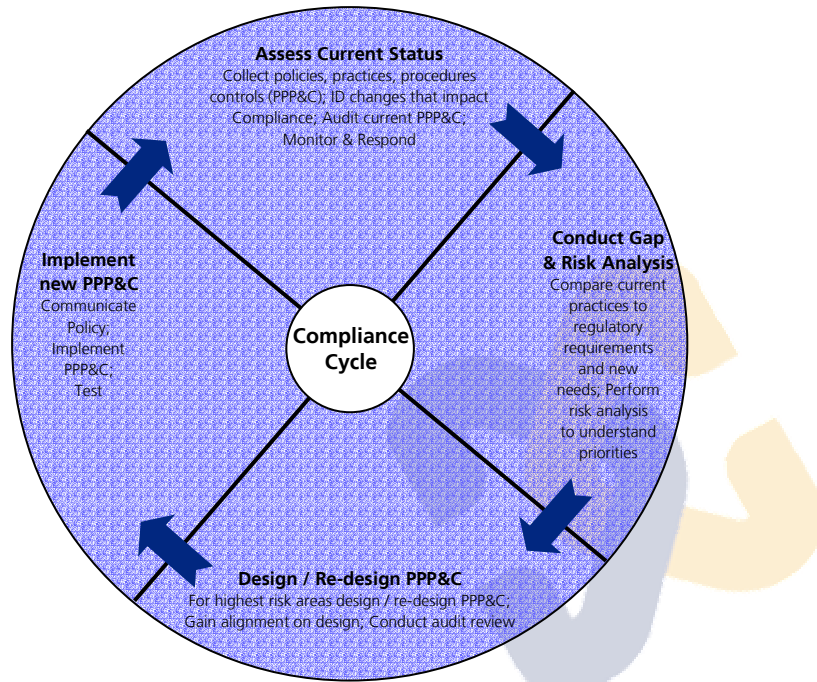
At a high level the process of becoming compliant with HIPAA security regulations is fairly simple and might be represented by the following steps:

1. collect an inventory of your current PPP&C,
2. perform a gap analysis between your current PPP&C and what is required by HIPAA and also perform a risk analysis on the gaps to understand priorities,
3. design new PPP&C and have them reviewed by auditors, and
4. implement and test the new PPP&C

Of course, the complexity of organizations and scope of regulations makes these activities much more difficult than they appear. First, not all of your PPP&C may be documented and you will have to conduct interviews to document them. Second, while policies, practices and procedures may be known they may not have associated controls that provide assurance the procedures are being followed. Additionally, once a gap analysis is complete and a risk assessment performed to produce priorities there may not be sufficient budget to implement desired changes. Finally, changes may be designed, but if all constituents do not agree on the priority of changes relative to other work that is required, the changes may not be implemented on time. Clearly there are many challenges to completing this relatively straight forward process. It is important to consider not only the costs of each these activities but also the ongoing cost drivers for maintaining compliance

Cost drivers

Clearly one of the biggest cost drivers is that **compliance is a continual process**. The work you do to document current practices and come into compliance today must be readily accessible in the future to determine if new regulations or changes in assets or processes will put you out of compliance. The following is a graphic of the life cycle:



As we have discussed this simple process can be quite complex and costly for large organizations. One of the biggest drivers of this complexity and cost is **federation of responsibilities**. In many large organizations it is more effective to have different departments (e.g., E-R, obstetrics, physical therapy) responsible for their own operating procedures. It is also likely that multi-location operations also maintain separate IT assets and staff. While these separations of duty and assets are valuable from an operations standpoint, they complicate management of compliance. For instance, different processes or IT configuration may require different policies between operating units or locations. It is important that you are able to efficiently keep track of these assets and PPP&C differences in order to efficiently manage future changes.

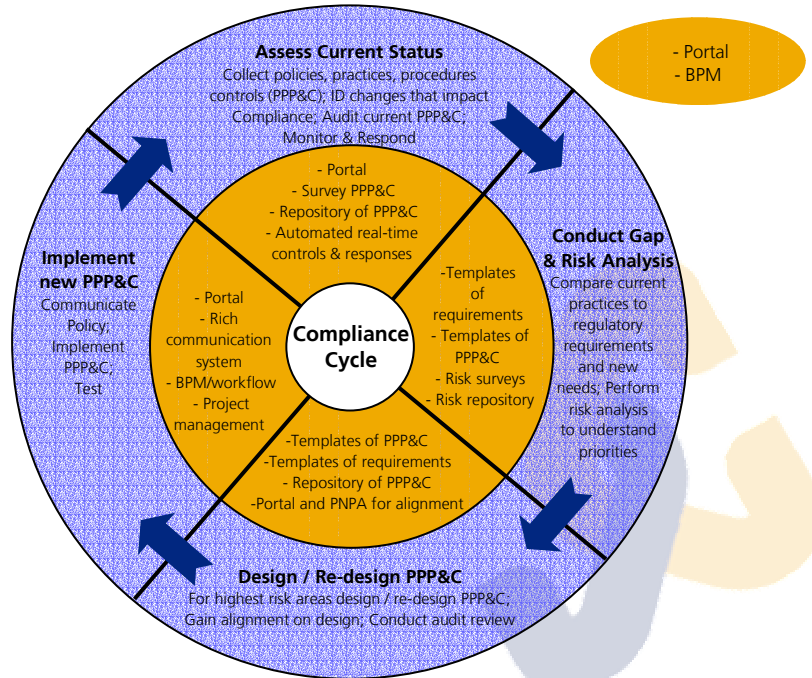
Another cost driver is the **time to identify gaps and risks**. Firms that do not have risk management as part of their standard operating procedure may benefit from templates of regulatory requirements and effective security PPP&C. The COBIT standard for information controls is one such template that can help. COBIT also includes techniques for assessing current and desired maturity levels.

The **alignment of multiple constituents to the change and implementation of PPP&C** can also be a significant cost driver. If you are part of a large organization, changes to PPP&C may involve many different functions (e.g., line of business, IT, auditors, and compliance) with other responsibilities. Failure to align their interest with compliance needs can result in compliance delays, penalties or excess costs to comply. An automated method to align on objectives could significantly reduce costs.

Another cost driver you should consider is the **cost of monitoring and responding to controls**. If risks (likelihood and impact) are sufficiently high, real-time monitoring may be required to mitigate those risks. The cost of manual efforts to monitor may be too excessive, but automation of monitoring may provide you with the ability to monitor more procedures for less cost, thereby reducing risk and cost at the same time.

Technologies to help

The following graphic supplements the previous compliance cycles with technologies that may help reduce risks and costs of compliance.



The following provides some brief insight into how some of the technologies can help

- Business Process Management (BPM) offers the ability to automate business processes such as the continual compliance cycle process or critical operational procedures. It provides benefits such as documentation of processes; audit trails of processes, and can drive process efficiency.
- Repositories offer the ability to efficiently organize, recall and reuse documentation of PPP&C, risk analysis results. There are a variety of techniques to store this information and the right approach for you will depend on your complexity and rate of change.
- Portals are an effective way to keep a large number of different participants up to date and involved in the compliance process. Portals can be an effective way to manage across a variety of locations, departments and even partners.
- Automated templates such as standard information controls provided by COBIT can simplify the effort to assure coverage of controls and speed time to design effective PPP&C. Some firms have even developed templates of regulatory requirements that can be used to help assure compliance.
- Project management is critical if you find you must make several changes to be compliant. Traditional project management software can effectively coordinate tasks among a variety of participants.
- PPP&C communication systems which provide rich content (i.e., text, sound, animation), a method to track who sees it and to assess comprehension may be much more valuable than traditional e-mail notification.
- Automated controls & responses can greatly reduce the cost to monitor procedures and respond to incidents. Additionally faster response tends to be more effective at reducing the cost of events and reducing overall risk. There are a variety of tools for automated monitoring and an understanding of your largest risks will help determine if any new ones are appropriate for you.

Questions to consider

While you are going through the process of making sure you are compliant with HIPAA security regulations you may want to consider the following:

1. What are your largest cost drivers?
2. Are there technologies that will provide quick payback against those cost drivers and allow you to do more with limited resources?
3. What are your largest security risks and would automation of monitors provide quick payback?
4. Does your organization change so rapidly that you need automated ways to manage the compliance cycle and your procedures?
5. Can some of these technologies provide other benefits (e.g., operating efficiencies) and further reduce payback time?

If you would like additional information on becoming compliant and maintaining compliance with HIPAA security regulations or on any of the above questions, please call our Information line toll free at 877-255-4798 or write us at info@complychain.com