



HIPAA Security:

What Now?

By Ward Keever, CTG HealthCare Solutions Executive Director of Executive Services

The HIPAA accountability requirements continue their march! Effective April 20th, covered entities must now comply with standards and implementation specifications for maintaining the security and confidentiality of patient electronic health information. This is one of many milestones that healthcare providers and other covered entities must accomplish to demonstrate HIPAA compliance. How do you plan to address these additional requirements after the first step of assigning the tasks to your Chief Security Officer (CSO)?

Well for starters, you need to understand that this set of tasks has a different focus than the gap analysis performed in response to the original HIPAA security requirements. The initial response was to identify tasks necessary to achieve compliance. By contrast, this regulation requires you to validate compliance. The necessary validation is achieved through periodic technical and non-technical evaluations that confirm employee compliance with your organization's policies. Additional evaluations should include your HIPAA posture as it relates to environmental or operational changes that could affect the security of electronic protected health information. For example, as your user community becomes more mobile and complex, the tasks required to monitor and validate compliance become more challenging and may require additional policies, skills and monitoring tools. The primary goal of the compliance evaluation is to determine if a covered entity has met the minimum requirements of the HIPAA Security Rule. A secondary goal is to determine if a covered entity has repeatable and lasting security organizational processes. These are the highly desirable traits that will keep an organization compliant once senior management removes the spotlight.

There are two different methods for evaluating compliance – the **process** and **practice** models. The process model includes a review of the documentation starting with the initial gap analysis and ending with the organizational policies and procedures. This model works best to validate the documented security foundation. The practice model evaluates how well staff are complying with the policies and procedures. Within this model, personnel are interviewed, system safeguards are evaluated, and the response of the workforce is compared with the results predicted in the documented policies and procedures. Any variations from the predicted results can be further explored to determine if they are statistical anomalies or indications of systemic problems. I suggest that the best approach is to use a hybrid of process and practice models to validate compliance.



Special appreciation and acknowledgment to Jim Wagner, Director, CTGHS Executive Services, and Clyde Hewitt, CTG Manager of Information Security Services, for their contributions to this effort. For further information regarding the CTG HIPAA vCSO program, please contact me at ward.keever@ctghs.com

The HIPAA Security Rule requires every covered entity to designate a “security official” with responsibility for the security management process, including the development and implementation of the HIPAA required policies and procedures. This person has been blessed with the title of Chief Security Officer (CSO). Many organizations have struggled to identify an appropriate and qualified individual for that position, since the magnitude of managing an enterprise-wide security compliance program requires a wide range of technical, organizational, and training skills. As a result, some providers may resort to appointing individuals without the strong executive leadership abilities, in-depth knowledge of the regulatory and compliance environment, and technical skills required to implement the broad spectrum of actions required by the Rule.

One solution is to engage a trusted partner to complement your in-house staff by supplying a virtual CSO (vCSO). A vCSO can serve in various capacities, including 1) as an interim CSO until the appropriate individual can be hired, 2) as a mentor for a selected individual, or 3) as the provider of supplemental resources when special skills and/or monitoring tools are required. Such a partnership can be a cost-effective solution via a combination of on-site and off-site support. This approach offers a unique advantage by making years of CSO experience from many different providers available to your organization. It also leverages industry-proven strategies and tools to solve common problems. For many smaller organizations, a vCSO functioning in a part-time role with a combination of on- and off-site support may be an excellent long-term strategy and solution.

Another answer for organizations that have identified a CSO lacking the full complement of skill sets and experience is to develop that expertise in-house using an experienced third party for mentoring in an advisory capacity. A structured personal development program can be designed that assesses and targets specific areas to enhance CSO knowledge and experience.

Successfully addressing the HIPAA Security Rule can be a challenging and lonely task—one that may leave executives with more questions than answers. A proven and trusted partner that can help overcome these obstacles represents money well spent in minimizing risk and cost down the road.