Complying with multiple regulations and contending with conflicts

by Chris Apgar, CISSP

This tip reviews how to comply with multiple regulations and what to do when they conflict.

Complying with multiple regulations has become a way of life. Between the Gramm-Leach-Bliley Act (GLBA), the Health Information Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX) and other state and federal regulations, organizations are finding it increasingly difficult to comply with conflicting regulations that govern day-to-day operations. Let's review how to comply with multiple regulations and what to do when there's a conflict.

The best approach to complying with multiple regulations is to evaluate each and determine which requirements are the same or similar, and which are different. For example, GLBA and HIPAA address privacy of customer or patient information. Instead of developing projects and separate policies to address each set of regulations, develop a set of policies that address the more stringent aspects of each, thus complying with the less stringent regulation at the same time. This is also true when state law intervenes and presents a more stringent regulation. Instead of approaching regulations as separate sets of rules to adhere to, look for a common approach to complying with multiple sets of regulations that often overlap.

When determining which practices are necessary to comply with a variety of regulations, start by creating a matrix. List the variety of requirements and look for commonality, exceptions or conflicts between them. This matrix is an integral part of a sound risk assessment and forms the foundation for developing appropriate practices, policies and procedures for an organization to follow. There are a number of resources available that provide the outline or process for developing and implementing a risk assessment, such as the NIST 800 series (http://www.nist.gov) or ISO 17799 (http://www.iso.org/iso/en/ISOOnline.frontpage). However, for specifics regarding how federal and state regulations fit within a risk assessment, seek advice from legal counsel and compliance officials. They will help you determine how to modify your risk assessment to incorporate the regulations your organization must comply with. With that in hand, a risk assessment becomes a powerful tool for building operating practices that look at the convergence of regulations rather than each as a separate requirement.

Multi-state operation challenges

Organizations operating in multiple states face a greater challenge given the variance in state laws. State and federal regulations create myriad problems when viewed separately. Again, the best approach is to begin with a list of the most stringent regulations (state and federal) and develop processes, policies and procedures to address them. Keep in mind, however, that this isn't always feasible or appropriate. For example, healthcare in California requires that all security incidents or suspected security incidents be reported to the state within 24 hours. A multi-state company with an office in California may elect to follow the state's reporting requirements for business within the state, but not for business in other states. This creates a situation where organizations create policies that cover all the regulations they are required to follow with exceptions noted. It is far better to clearly identify exceptions to the rules and apply them where appropriate than to create a separate set of practices for each federal and state regulation (especially at the state level).

Contending with conflicts

The challenge facing organizations is where regulations conflict. First, determine if a state regulation is superseded by a federal regulation or merely appears to conflict because it is more stringent. Where regulations do actually conflict, it is better to err on the side of caution and adhere to the more stringent regulation. Consult legal counsel and clearly document where regulations conflict and what compliance path the organization has elected to follow. Documentation is critical to any compliance program. As they say in legal circles, "If it isn't documented, it didn't happen." Performing a risk assessment is the first form of documentation followed by having a risk management program. This includes the development of a sound compliance program that is fully documented, especially where regulations conflict at a state or federal level.

Organizations operating in multiple states may have state regulations that conflict. In these cases, develop state-specific practices, policies and procedures that govern operations within a given state. These state-specific requirements can be added to existing standard practices that address non-conflicting state and federal regulations. This doesn't mean an organization needs completely separate policies and procedures for each state in which it operates. It means the organization needs to implement separate policies that are followed at the state level in addition to already developed standard policies and procedures. It may be practical to look across the state horizon and determine where the most stringent state regulations exist and develop organization-wide policies that adhere to the most stringent regulations. This enables the organization to adopt common practices across the states in which it operates while addressing the most stringent state practices. This isn't always practical, but where it is, it is a sound practice to follow.

The more an organization is able to standardize practices to cover a multitude of regulatory compliance requirements, the easier it is to comply in general. It is also easier to build a compliance culture where standardization is the norm, and it creates an easier environment to train employees. Regulations will continue to be promulgated and the regulatory environment will become more complex. As long as multiple regulatory agencies have their fingers in the proverbial regulatory pie, there will be variances that bear review. This doesn't mean standardized practices that cover the regulatory spectrum and decrease the complexity in compliance cannot be developed. In the end, the key is a thorough analysis of what is required and solid documentation related to compliance.

About the author

Chris Apgar, CISSP, is president of Apgar & Associates, LLC and former HIPAA Compliance officer for Providence Health Plans in Oregon and SW Washington. He is a nationally recognized data security, privacy, transaction and code sets, regulatory and HIPAA expert. He is a member of the HIPAA Compliance Insider Advisory Board, the Security Compliance Insider Advisory Board, the URAC Privacy Advisory Committee, and chairs the Oregon and SW Washington Healthcare, Privacy & Security Forum and the Forum's Transaction & Code Set Workgroup. Mr. Apgar now operates an independent consulting firm specializing in security, privacy, HIPAA, global and detailed business process review, information systems project development, and lobbyist activity.