

The CISSP, The CIPP and HIPAA

By David Nelson

So what does the Certified Information Systems Security Professional (CISSP) and the Certified International Privacy Professional (CIPP) have to do with each other? At best they are aware of each other and at worst acrimony has arisen in trying to meet independent organizational goals, compliance laws and budgets. Enter the Health Insurance Portability and Accountability Act (HIPAA). This law was far-reaching enough to not only indicate that these two disciplines should work together, but it has forced them into an intimate relationship.

The CIPP

In general, the CIPP focuses on privacy from a very broad stance, but not driven solely by one law. The CIPP must incorporate multiple laws, regulations, and standards to meet compliance, part of which includes information technology security. The real rub for the CIPP is that the health information interface between HIPAA Privacy and Security, and what information is shared is limited to the "minimum necessary to accomplish the purpose." This works for policy and procedures and sounds great on paper, but unfortunately when the information transmogrifies into electronic information, the edges of the Privacy domain begin to blur. How can the CIPP ensure compliance without an intimate relationship to electronic information security?

The CISSP

The CISSP, in general, understands the structure of information systems and protects the flow of electronic information. This includes the protection of data in transit or data at rest. If fully engaged, the CISSP creates risk assessments for data security so the primary focus on IT assets defines the CISSP realm. Yet there are many points where the CISSP must interact, support, or respond to policy and procedures from the HIPAA Privacy side. These are not usually electronically controlled interfaces. But how does an IT security manager know which laws affect their business or which information is in need of greater protections?

HIPAA Marries the Two Disciplines

At first blush, the HIPAA Privacy and Security rules seem only marginally engaged. Again, Privacy focuses on policy and procedures in handling paperwork, dealing with the health care customer, and the interaction with other providers. Security gives the look of being related only to ensuring security of Electronic Protected Health Information (EPHI). In reality, the general topic of privacy only tells us what to protect while security tells us how to protect it. The marriage of the rules happens because the premise

of being designated a "covered entity" by HIPAA hinges on the electronic transmission of health information. Furthermore, the HIPAA Privacy rule requirement to have "administrative, physical and technical" safeguards interleaves the information flow from the HIPAA Privacy rule directly into the HIPAA Security rule. But, there is no clear separation between the rules that says, "Privacy ends here and security starts here." There is a very gray area between Privacy and Security.

As a Privacy Official, when I first started reading the Security Rule, I thought, along with others, that it would be necessary to have someone who had an IT technical background to accomplish the proposed Security Rule standards. But as I began to study the structure of the Security Rule, and there is a surprising amount of structure, it became apparent that what was called for was an expert in IT *security management*. Not the daily activities that contribute to IT security like firewall settings, but someone with a set of skills in managing the IT security principles. The scheduling of when the firewall log review happens can be more important than the settings. No, you cannot ignore the settings, but it doesn't much matter if you set the firewall to record every event if no policy exists to enforce a review of the logs. Thus many entities have chosen a CISSP to lead the HIPAA Security effort rather than a security technician. Understanding the subtle difference made my course of study clear.

Specific Overlap in the Rules

A clear fit between the rules is the map of PHI in Privacy and the detailed Risk Analysis of the Security Rule. The mapping of PHI for Privacy should have happened way back in 2002 or 2003. But as a CIPP, if you somehow missed the mapping, the CISSP you bring to the table can help in the catch-up process, as the Security Official's focus is EPHI, a subset of the original PHI. Plus the security professional can suggest audit tools on servers to identify the underground applications and databases. All too frequently these applications and databases are necessary for the efficient operation of health care facilities, yet somehow staff "fail" to report them, especially to the Privacy Official who was doing the PHI mapping. Conversely, for the Security Official, the initial mapping of PHI can indicate which systems or database should be of primary concern. By having the PHI map, the identification of EPHI under the Security Rule can commence, or at least have a definitive starting point.

The marriage, or at least the engagement, of Privacy and Security activities is advisable from a budgetary standpoint also. For example, the use of virus protections has benefits for both Privacy and Security. The expense of purchase, updates and audits apply to both sets of compliance efforts. It is like getting double credit coupons for expense justification.


Additional benefits of the marriage of the two disciplines under the HIPAA overlap is that part of the CISSP arsenal is the application of a business mathematical model: Risk Analysis. This applies to the risk associated with ANY form of information. This is, of course, a business management tool. Since only in limited circumstances can the information covered by HIPAA be segmented from all other information, the required security risk analysis takes on a larger life as it supports all of the system information security. I would venture that for most covered entities, the HIPAA covered PHI and EPHI reside on systems that are not dedicated solely to HIPAA. So the CISSP is starting to become very attractive to the CIPP, as the CISSP can provide budget justification for segmentation, or extra security measures for PHI/EPHI.

With no clear line in separating Privacy and Security under HIPAA, other things are up for grabs, too. For example, workstation security. For Privacy it is addressed in reasonable safeguards for PHI. For the Security Rule it shows up a couple hundred times throughout the rule, but most importantly, it is a part of a detailed risk analysis. For the CISSP certification, workstation security falls under Physical Security and for the CIPP certification, it is under Information Security. Yet which official will have to address the Office for Civil Rights or the Secretary of Health and Human Services when they come calling?

How Are CIPP and CISSP Certifications Similar?

The certifications for the CISSP and CIPP, like the HIPAA Privacy and Security rules, have overlap in many areas. Some of the overlap is readily apparent like Law and Ethics for CISSP to the Privacy Law and Compliance for the CIPP. Workplace Security and Physical Security is another obvious commonality. Others are not quite so obvious. Rather than have a separate domain for Business Continuity Plan/Disaster Recovery Plan for CISSP certification, the CIPP certification rolls it into Information Security.

Summary

While it is clear that each certification's focus is different, and each is intense in a different way, if combined, these may as well be the outline for a fully Compliant HIPAA Official. Personally, working for a relatively small county, that is my goal. Being involved in HIPAA makes me an immediate pariah, but as a CISSP, I have earned some respect from IT technicians. As a CIPP candidate, I can corroborate to staff in the health field that all the work I have done over the last four years actually is useful toward a broader scope regarding compliance. 

David Nelson, CISSP, is a Yolo County HIPAA Privacy and Security Officer.

CISSP:	CIPP:
<ul style="list-style-type: none"> • Access Control Systems and Methodology • Telecommunications and Network Security • Security Management Practices • Applications and Systems Development • Cryptography • Security Architecture • Operations Security • BCP and DRP • Law and Ethics • Physical Security 	<ul style="list-style-type: none"> • Privacy Law and Compliance • Information Security • Web Privacy and Security • Data Sharing and Transfer • Workplace Privacy • Additional for Governments: • Government Privacy Laws • Government Privacy Practices

Figure 1: Concerns of the CISSP and CIPP