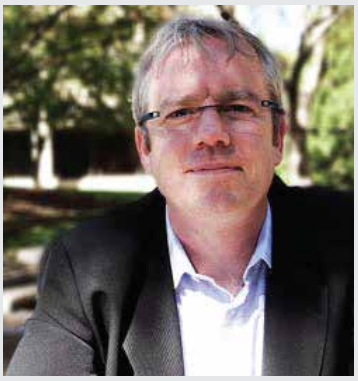
IF HIPAA COMPLIANCE SEEMS TOO HARD …

By Chris Cronin
ISO 27001 Auditor
Governance & Compliance Services

…THEN YOU'RE DOING IT WRONG. HERE ARE THE BASICS OF DOING IT RIGHT.

In April 2013 the Office of Civil Rights, the branch of the Department of Health and Human Services that oversees compliance with the HIPAA Security Rule, started releasing analysis from their pilot audit of Security Rule compliance. In 2012, OCR and their audit partner KPMG set out to assess 115 organizations: hospitals, insurance companies, clearinghouses and business associates. Their essential goals were to develop and test a new HIPAA audit program, and to see what the current state of HIPAA compliance was. And what they found was that in terms of HIPAA Security Rule compliance … you're probably doing it wrong.



Chris Cronin's primary focus at HALOCK is to help organizations comply with regulatory and legal requirements for securing information. Because risk management is at the core of these regulations, Chris delivers policy design, security controls, audit, risk assessments and Information Security Management Systems all within a cohesive risk management process.

Chris combines his deep experience in many regulatory environments with a strong technical and management background. Because information security laws and regulations encourage organizations to find "reasonable," "appropriate," and "acceptable" methods for compliance, Chris' approach to helping his clients find and develop those methods has been critical to their success.

Two thirds of the organizations audited in the pilot program were not aware that they were supposed to conduct a risk assessment.

This one fact is stunning because when you read the HIPAA Security Rule the first specification is that you must conduct a risk assessment. This is probably evidence of both the fact that people are not reading the regulation and/or the guidance material from OCR, and people do not know what risk assessments are.

On the first point, I'll remark that I very often encounter people who show me the research they've done on HIPAA compliance, and they provide hyperlinks from every known web site but for one ending in the domain "hhs.gov" or ".gov" for that matter. For some reason people do not read the source material. They instead look for opinions or guidance from people who are not the authorities on the subject. But the regulation and the guidance from OCR are readable and understandable. You may need someone to help implement the requirements in the regulations and guidance, but the instructions are very clear. To make things worse, many of the websites I am being sent hyperlinks to just do not understand the core of the HIPAA Security Rule, which gets us to our next point.

Management generally doesn't know what information risk assessments are. So before we go much farther, let's be clear about what we mean by an information risk assessment.

1. An information risk assessment is the means by which we both identify and justify our information security safeguards. This is true for any U.S. regulation that protects personal information.

2. Information risk assessments are management's analysis of what negative impacts might occur if information is somehow compromised.

What HIPAA is trying to tell us is, "Don't try to implement all possible safeguards to their fullest extent. Just implement safeguards that reduce your risks to a reasonable and appropriate level." The way we calculate reasonable and appropriate risk is through a risk assessment.

Further, the OCR is telling us, "Use the freely available standard 'NIST Special Publication 800-30' to estimate that risk." NIST SP 800-30 provides detailed guidance for building a risk register that will help you identify your organization's "duty of care" for protecting health information, and will help you determine which safeguards would help you meet that requirement.

You may hear criticisms that risk assessments, and particularly NIST SP 800-30, are insufficient for identifying true risks. These criticisms are also in line with complaints that "compliance is not security." While both of these criticisms are defensible, consider this point; if two-thirds of organizations that must be HIPAA compliant don't even know they should conduct risk assessments, then starting with a method as simple as NIST SP 800-30 moves them further ahead than where they are today.

So let's also discuss what you will need in order to conduct a quality information risk assessment.

1. Ensure that you are using a simple process, such as NIST SP 800-30 or ISO 27005, especially if you are just starting your risk management processes. These standards will guide you toward making a spreadsheet that helps you systematically identify and score your information risks.

2. Define your impact scores using values that matter to your mission. If you use impact scores such as "High," "Medium," and "Low" without defining those values, then your risk assessment participants will be using widely varying criteria for determining what those values mean to them. Rather, use guidance language such as "'High' means more than 500 patients will have their PHI exposed. 'Medium' means up to 499 patient records will be exposed, and 'Low' means none will be exposed."

3. Ensure that your highest level executives help you define what the impact score values will mean. When you budget and plan your safeguards, you will be comparing the cost of those safeguards to the potential impact that they are reducing. This comparison will be helpful if the people who approve budgets and priorities agree with the impacts, knowing that the impacts are based on the mission of the organization.

4. Properly identify your vulnerabilities. Examine each information asset that will have some contact with PHI. Determine what kinds of controls should be applied to that asset using an information controls standard such as NIST SP 800-53 or ISO 27002 [eg. being sure to at least include the Security Rule specifications]. If those controls are not in place or are not effective, then you have found a risk.

5. Work with experts to determine what threats could take advantage of those vulnerabilities and compromise your assets. This is critical. If you are estimating your duty of care in a risk assessment, then you should know what threats you could expect to experience. Neglected network services, advanced malware, theft, loss of equipment, hacks, careless or uninformed employees, weak web applications, poorly configured devices and user devices on the network are all threats that ebb and flow in their probability. If you do not have this expertise on hand, then hire it. A risk assessment that does not include currently expected threats will not identify your risks and you will not know your duty of care as a result.

6. Use the same risk calculation for the proposed safeguard as you are using to calculate the initial risk. This way, you can justify your safeguard as one that will be reasonable by comparing the cost of the safeguard against the originally assessed impact.

Your HIPAA Security Rule compliance effort needs that risk assessment. Not only because it is a requirement, not only because it will tell you what you should do, but it will also tell you what not to do. If you try to apply all of the Security Rule specifications and to their fullest extent then HIPAA compliance will be too hard. As a result, it may also be unsustainable.

So do what the OCR is asking you to do instead; assess your risks, then apply controls that will reduce your risks to a reasonable and appropriate level.

When you read the HIPAA Security Rule the first specification is that you must conduct a risk assessment.