Third Party Assurance in Healthcare:
How vendors can strengthen trust and transparency

June 2016

pwc

Heart of the matter

Increased cyber risk and additional regulatory pressure have changed the face of healthcare, and the demand for trust and transparency continues to grow—not just for traditional healthcare companies but for anyone currently doing business within or wishing to do business within the industry. Here's what vendors providing or looking to provide services to healthcare companies need to know about third party assurance and a common way to obtain it: using the HITRUST Common Security Framework (CSF).

As healthcare companies outsource more business functions, use cloud-based services more frequently, and connect their digital systems with those of hundreds of organizations across the healthcare spectrum, more parties are exposed to Protected Health Information (PHI), and the task of protecting it becomes ever more complex. (See sidebar on page 4, "What is considered PHI?") The new and growing interdependencies among traditional healthcare companies, as well as their "business associates" or vendors operating along the healthcare continuum, pose systemic risks. Regulators, in turn, have increased their demands for compliance as well as fines for noncompliance.

In 2013, the Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Rule, for example, drastically increased fines. The Office for Civil Rights (OCR)—enforcer of HIPAA regulation—increased the maximum civil monetary penalty for a single incident to $1.5 million from $25,000. And for the first time, the rule now reaches beyond traditional healthcare payers and providers, casting the HIPAA net over any "business associate" or vendor operating along the healthcare continuum, including prospective vendors that may come into contact with PHI in the future. Regardless of whether a company houses, transmits, stores, processes, or views the protected data, all entities that might be exposed to PHI are held to the same standard as traditional healthcare covered entities and are now subject to random audits by the OCR. HIPAA compliance is now truly an industry-agnostic expectation.

Many organizations that touch PHI are struggling to understand the new rules and industry demands, as well as what they must do to comply. Those who authored the HIPAA laws and other healthcare regulations purposely did not prescribe mandated-control and detailed-implementation requirements. Their intent was to leave management teams with the flexibility to interpret and determine their own requirements based on their own identified risks. In our experience, however, many organizations are struggling with the ambiguity around control requirements, and they remain unsure of what's required or whether they have adequate controls in place to address the demands of both the regulators and customers. The ambiguity around what's required of vendors combined with the fact that they already feel burdened by existing requirements, has made healthcare vendors hesitant to change course or add yet another third party assurance report to their list of priorities.

But add one they must. Several of the largest global healthcare payers—including Anthem, HCSC, Highmark, Humana, and United Healthcare—require that their vendors obtain a Health Information Trust (HITRUST) Alliance certification by 2017. In addition, the Blue Cross Blue Shield Association has announced to all 36 affiliates that they must implement a control framework focused on the protection of PHI—such as HITRUST—and obtain a SOC 2 report using that framework by 2017. Such third party assurance mandates have changed relationships and heightened the expectations and influence of both regulators and customers.

Those heightened expectations and influence are making relationships for vendors more complex—with their regulators and customers, as well with competitors—even for those vendors not facing a third party assurance mandate themselves. Some might call it "pin action," where the mandate is the bowling ball and vendors are the pins—even if the mandate ball hasn't directly hit an individual organization, in order to stay competitive it must follow suit. Similarly, other healthcare organizations are beginning to follow suit with what their competitors have done and will soon enforce similar requirements.

What is HITRUST?

The HITRUST Alliance estimates that at least 7,500 organizations will need to comply with these mandates and obtain the certification by 2017, or discontinue serving these customers altogether. Others who aren't yet facing a mandate must consider the potential effects of market forces, determine how to evaluate and adjust their controls to protect against a data breach, and provide the level of assurance that their customers need. These adjustments may be especially worthwhile for vendors new to the healthcare industry, as well as for current vendors looking to differentiate themselves in the marketplace.

What is the HITRUST CSF and certification?

Whether or not they're facing a HITRUST mandate, many healthcare vendors struggle with competing priorities when it comes to data privacy and security. It is challenging to adhere to regulations that are constantly changing, implement leading-practice controls, and make sure these things happen efficiently and consistently across business units.

To help vendors meet this challenge, the HITRUST Alliance created a Common Security Framework (CSF) built specifically for the healthcare industry.

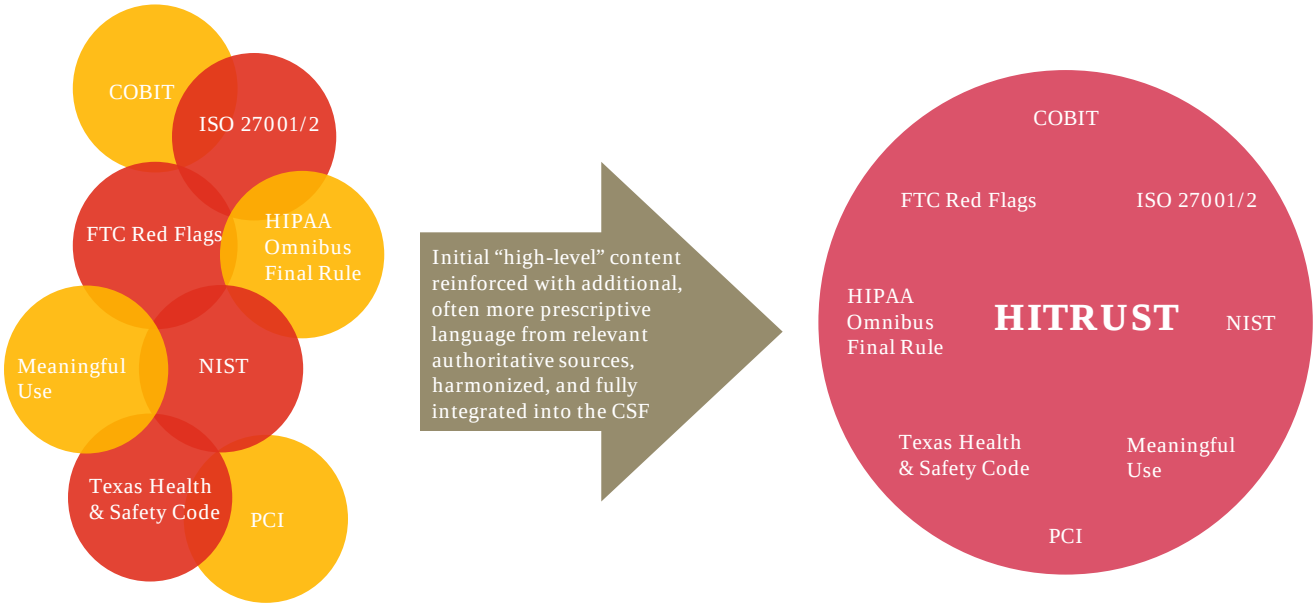
The HITRUST CSF incorporates 19 federal, statutory, and numerous other healthcare regulations and common cross-industry standards (see exhibit below). The intent of the control framework is to provide a common vocabulary that smooths out communication and helps align everyone's expectations. The HITRUST organization regularly updates the framework, integrating new regulations to stay current as regulations change.

As is the case with other common frameworks, the HITRUST CSF represents an "assess once, report many" assurance model. Such a model offers the potential to streamline the effort associated with responding to multiple customer inquiries and audits, reducing audit fatigue and resource drain.

Some customers demand third party assurance, and recognize that Service Organization Controls (SOC) 2 might not be completely relevant for the services provided by a vendor. In this case, the HITRUST Alliance can provide an independent, third party assessment of how well the vendor has implemented the HITRUST CSF and adheres to its control requirements. The HITRUST Alliance issues official HITRUST certifications to those organizations that meet the requirements.

HITRUST is the only CSF that integrates all healthcare standards and regulations

The eight most common regulation and control frameworks covered by HITRUST



Third party assurance options for healthcare customers

Options for providing third party assurance to healthcare customers

A **standalone HITRUST certification** is just one of two tools available to vendors that need to protect PHI and provide third party assurance. Depending on what their customers require, it's possible that an American Institute of Certified Public Accountants (AICPA) **SOC 2 report with an embedded HITRUST opinion** will suffice. Familiar to most organizations, SOC 2 is a framework built on AICPA principles and criteria that provides an independent, standardized analysis of vendor operations. This examination may be based on a unique set of management's controls. Healthcare vendors seeking to provide assurance over PHI may use the HITRUST CSF as the basis for this examination.

Given these two tools, organizations that face a HITRUST mandate or are generally asked to provide assurance may do so in one of three ways:

SOC 2 with a HITRUST opinion.

Some customers will accept a SOC 2 report using the HITRUST CSF controls with an opinion embedded within the report over the HITRUST CSF. (Obtaining the HITRUST option requires that the organization implement the HITRUST CSF.)

Standalone HITRUST certification.

Other customers recognize that a SOC 2 report may not be relevant for the services being provided and instead will require a standalone HITRUST certification.

Options 1 and 2 combined.

A handful of customers will require certain vendors to supply both a SOC 2 report with an embedded HITRUST opinion and a standalone HITRUST certification.

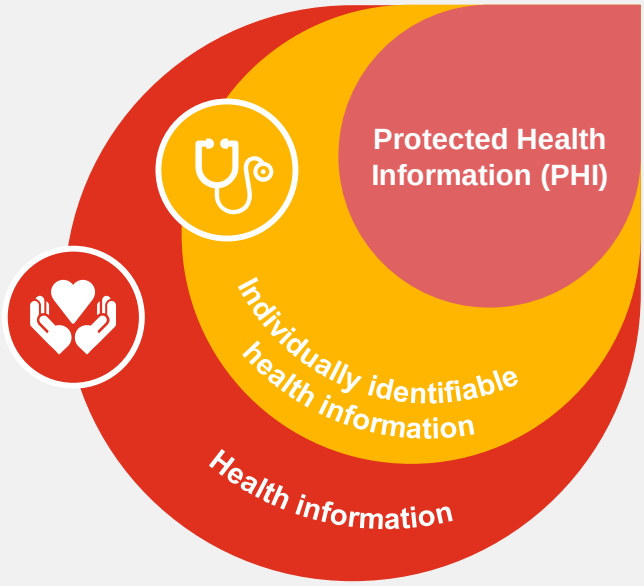
In the coming months, all healthcare vendors will need to evaluate their compliance activities to determine what's expected of them and how to provide the needed level of third party assurance that is fast becoming the marketplace norm. Vendors not currently facing a HITRUST mandate should think carefully about the direction in which the industry is headed and weigh the costs and benefits of adopting the framework sooner rather than later.

What is considered Protected Health Information ("PHI")?

Many organizations will have to start their assessment process by getting a handle on exactly what constitutes PHI—and the definition is more narrow than one might think. PHI is information that relates to:

- The physical or mental health condition of an individual;
- The provision of healthcare to an individual; or
- The payment for the provision of healthcare to an individual.

In addition, that information must be individually identifiable, meaning that it either identifies an individual or can reasonably be used to identify an individual.



Determining if HITRUST is the right fit

Determining whether HITRUST is the right fit

Many companies that have served or want to serve healthcare customers are already mired in a swamp of regulatory- and assurance-related processes and reporting. They devote considerable resources to meeting industry requirements, and many wonder, “If we're already doing all this, why must we do HITRUST?”

In a handful of cases, the answer is: You don’t. If your customer has randomly assigned a business associate designation to you and you know that your company will never have even the potential to come into contact with PHI, you should think about challenging the designation. Everyone else should consider that the HITRUST certification requirements may be partially addressed by what they are already doing with regard to third party assurance. There are areas where SOC 2 and HITRUST overlap, for instance. By consolidating existing initiatives, some organizations might eliminate redundancy associated with using multiple control frameworks.

Before deciding whether or not HITRUST is right for your organization—and whether you want to take a CSF-only approach or obtain a HITRUST certification—work to thoroughly understand what your stakeholders are asking for and why they’re asking for it. It might be that a SOC 2 report combined with the HITRUST CSF would sufficiently address their demands. On the other hand, some traditional healthcare companies have declared that every single organization with which it does business must be HITRUST certified, with no exceptions, even if they produce a SOC 2 report.

It is also possible that a HITRUST certification alone will not be enough for all parties. In particular, large healthcare vendors will likely have to continue to produce HIPAA risk assessments, traditional SOC 1 reports, and SOC 2 reports in addition to a HITRUST certification. Of course, by using a common control framework an organization can assess once and produce multiple types of third party assurance, meeting the numerous, varying needs of multiple stakeholders in the marketplace. For example, say a customer requests a SOC 2+ of an associate that is already HITRUST–certified. It is not strictly necessary to produce two separate reports. There is a new option where—thanks to a collaborative effort between HITRUST and AICPA—it is possible to obtain an opinion over the CSF framework that addresses both HITRUST and SOC 2 and in a single report.

This report can meet the requirements of both HITRUST and SOC 2, as long as an organization can meet the requirements of the HITRUST CSF. The HITRUST requirements are, as a general rule, more granular than those in the SOC 2 Trust Service Principles and Criteria. So vendors should take great care and confirm that they have fully met both the requirements of the HITRUST CSF and all relevant criteria under the SOC 2 Trust Service Principles and Criteria.

HITRUST can work for any covered entity, in any industry

Case example: How one company implemented HITRUST

In the coming months, several organizations that traditionally operate outside healthcare, but that serve or aspire to serve the healthcare industry, will have to determine whether to implement the HITRUST CSF and obtain the certification. For some, an investment in HITRUST will be worthwhile. One of several large, US-based personal publishing services, for example, wanted to capitalize on its strengths in producing custom-printed marketing materials and expand its business-development reach into other industries, particularly in the corporate space. A clever marketing executive uncovered an opportunity to work with health plans to print targeted, health-related materials with the goal of helping covered individuals obtain preventative care and stay healthy. For instance, if John Doe visits his general practitioner and is deemed to be at an elevated risk for heart attack, two weeks later John might get a brochure in the mail with a list of things he can do to lower that risk and maintain a healthy lifestyle.

Of course, the advice contained in the printed materials is based on data obtained from John's physical examination—and is therefore PHI. This publishing company—which had no previous exposure to or experience with the healthcare industry—pitched the idea to a prospective healthcare customer who loved it but required that the publishing service be in compliance with the HITRUST CSF. Moreover, the publishing service had to be compliant before any PHI could be handed over and work could be done.

The publishing service, which was already in the midst of completing a SOC 2 report, charted a path forward. It immediately began a HIPAA risk assessment, which also acted as a readiness analysis for a HITRUST certification. It mapped its current SOC 2 report against the HITRUST CSF to uncover multiple synergies between the two and avoid redundant work. It set up a recurring assessment against the CSF, the results of which support a SOC 2 opinion-based report as well as a HITRUST opinion-based report, the combination of which will meet their foreseeable needs.

In less than one year, this company went from knowing nothing about PHI security and controls to being in a position to obtain a HITRUST certification. The certification resulted in increased confidence and trust, both internally and externally, in the vendor's ability to thoroughly address information security and privacy challenges. It also provided the vendor with a more coordinated and efficient way to assess compliance with other information security and privacy requirements. In addition, the organization's improved understanding of compliance requirements boosted employees' ability to apply safeguards and spot and report issues. All of this led to decreased risk and lower expenses associated with information security and privacy assessments. In this particular case, HITRUST was well worth the investment.

Organizations that want to do business or that are already doing business within the healthcare industry need to implement a control framework for protecting PHI. Because the HITRUST framework is built specifically for those serving healthcare organizations, in many cases it is the best option.

An outlay of resources is, of course, required to implement the HITRUST CSF. But the investment can be worthwhile—particularly considering that the HITRUST CSF presents an opportunity for organizations to reengineer their overall approach to third party assurance and improve their program management process. The HITRUST "assess once, report many" assurance model can be implemented across an enterprise, potentially saving substantial amounts of resources. Companies can even use the framework to standardize the evaluation of and set the bar for its own business associates and vendors. It is important for business associates and vendors to think about their own vendors, or "sub-business associates" and what controls and safeguards they have in place, in addition to what types of third party assurance they should provide.

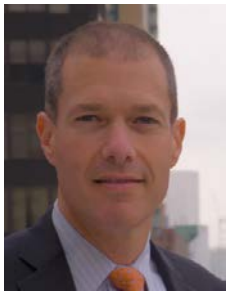
Along with the measurable benefits and cost savings associated with using the HITRUST CSF, obtaining a HITRUST certification may create goodwill by demonstrating commitment in customer relationships and perhaps showing the OCR that your organization is making every possible good-faith effort to identify and mitigate problems before they occur. Implementing the HITRUST CSF creates a virtuous cycle that benefits those involved, from hospitals and insurers to IT companies, banks, and even waste management companies, all the way down to Jane and Joe patient whose personal health data are more secure as a result of your efforts.

www.pwc.com/us/buildingtrust

Our services

PwC's Trust and Transparency Solutions practice takes an integrated approach to building and maintaining mutual trust; helping identify weaknesses and interconnected risks; building better protections across your business network; and providing the assurance your company, customers, suppliers, investors, and regulators need. By bringing together industry-specific skills in technology, regulatory compliance, financial and accounting, and other business processes, the PwC Trust and Transparency Solutions teams can help you assess your third-party risk management program, with a focus on controlling costs, mitigating risk, and enhancing trust and transparency.

To have a deeper conversation about PwC's HITRUST Services and increasing trust and transparency through third party assurance, please contact:



Todd Bialick

Trust and Transparency Solutions Leader

973-236-4902

todd.bialick@pwc.com

Connect with Todd

Kevin O'Connell

HITRUST Services Leader

617-530-7785

kevin.w.oconnell@pwc.com

Connect with Kevin