- [Home](#)
- [SF STAT!](#)
- [Current Articles](#)
- [CURRENT ISSUE](#)
- [Online Newspapers](#)
- [WEEKLY NEWSLETTERS](#)
- [Media Kit](#)
- [Calendar](#)
- [Business Directory](#)
- [Video Interviews](#)
- [Contact](#)

Select Page

Coming Soon: HITRUST Threat Catalogue to Comprehensively Address Risks to PHI

From "repeal and replace" to blocked mega-mergers, almost nothing about the healthcare industry in 2017 is guaranteed.

But there is one thing you can count on—the cyber threats healthcare organizations dealt with in 2016 are here to stay. In fact, we believe they are going to get a whole lot worse.

In the first 30 days of 2017, the Department of Health and Human Services' Office for Civil Rights disclosed 10 healthcare data breaches, affecting nearly 25,000 individuals.

Concurrently, HHS OCR has lowered its threshold for investigation of healthcare record breaches and possible enforcement action to cases involving as few as 500 records.

Healthcare has a more complex challenge than many other industries for one big reason: the Health Insurance Portability and Accountability Act (HIPAA). Cyber risk management can feel like an impossible choice between compliance and security. The challenge boils down to lack of guidance on how organizations should interpret "reasonable and appropriate safeguards" and "adequate protection," and what constitutes a valid risk analysis.

That's where a risk-based control framework comes in. The HITRUST CSF—the most widely adopted security framework in the U.S. healthcare market—integrates requirements from multiple, relevant standards and best practices to sets an industry standard of due care and baseline set of controls that, importantly, are tailored by specific organizational, system and regulatory risk factors.
In other words, it helps facilitate HIPAA compliance and cyber readiness.

The problem with any cyber framework, however, is that it's relatively static, and typically updated based on historical breach data and lessons learned instead of forward-looking information. Security controls are meant to address specific risks posed by specific threats, which are constantly changing.

To help enhance the framework's responsiveness to the dynamic threat landscape, BDO is proud to be working closely with HITRUST and other industry leaders to develop the Threat Catalogue, a comprehensive taxonomy for common threats mapped to specific CSF controls designed to counter cyber threats and protect electronic Personal Health Information (ePHI) and other types of sensitive data held by healthcare organizations such as personally identifiable information (PII), Payment Card Information (PCI) and research data. HITRUST anticipates the Threat Catalogue will be a "living document" due to the constantly changing threat environment, including planned

improvements to better facilitate risk analyses and the consumption of threat intelligence.

Governing chairs of the HITRUST CSF Threat Catalogue Working Group include: Kevin Charest, Ph.D., DSVP and CISO, Health Care Service Corporation; Bryan Cline, Ph.D., VP, Standards and Analytics, HITRUST; Roy Mellinger, VP, IT Security and CISO, Anthem, Inc.; John Riggi, Head of Cybersecurity & Financial Crimes, BDO Consulting.

HITRUST will also issue advisories to provide more granular intelligence on actual, immediate threats and corresponding security controls.

The Threat Catalogue will be available in March. For more information, check out the official announcement from HITRUST or visit https://hitrustalliance.net/threat-catalogue/.

South Florida Hospital News and Healthcare Report's number one goal is top quality healthcare journalism written and edited for the region's most successful, powerful healthcare business executives and professionals.

- [Home](#)
- [About](#)
- [CURRENT ISSUE](#)
- [Media Kit](#)
- [Video News](#)