Compliance with financial reporting requirements, government regulations and environmental laws is becoming increasingly challenging for enterprises across numerous sectors of the economy in the digital era.

But no other industry faces greater risks for failure to meet compliance requirements than healthcare. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required modernization of electronic healthcare records and standards for electronic healthcare transactions.

HIPAA rules and requirements are designed in large part to protect patient privacy and prevent healthcare fraud and abuse. The penalties for failure to comply are steep, including civil fines of up to $1.5 million per year and a prison sentence of up to five years upon criminal conviction.

Make no mistake: The federal government is aggressively coming down on healthcare providers that are not in compliance. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required modernization of electronic healthcare records and standards for electronic healthcare transactions.

OCR’s investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections,” HHS said. “Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI.”

• In May 2014, New York and Presbyterian Hospital (NYP) and Columbia University (CP) paid a combined $4.8 million in penalties after releasing health information for 6,800 patients on the Internet. According to HHS, the breach was caused “when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI.”

“OCR’s investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections,” HHS said. “Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI.”

• In April 2014, Concentra Health Services agreed to pay $1,725,220 to settle potential HIPAA violations. Cause of the breach? An unencrypted laptop containing patient health information was stolen from a physical therapy center in Missouri.

• Adult & Pediatric Dermatology, P.C., of Concord, Mass., agreed in December 2013 to pay HHS $150,000 after “an unencrypted thumb drive containing the electronic protected health information of approximately 2,200 individuals was stolen from a vehicle of one its staff members.”

A doctor fooling around with a computer, a stolen laptop and a stolen thumb drive: Those are what cost four organizations nearly $7 million for failing to meet HIPAA compliance.
New operating rules enacted this year under the Affordable Care Act (ACA) add even more complexity to HIPAA, requiring health plans to certify compliance with operating rules and standards and obtain HPIDs (Health Plan Identifiers), among other changes.

As the ACA continues to roll out—and as structural changes reshape the U.S. healthcare system—healthcare providers must ensure that the compliance software and systems they use are specifically suited for HIPAA and other healthcare compliance and regulatory requirements. Off-the-shelf solutions simply won’t due when the stakes are so high for both healthcare providers and patients.

Healthcare IT professionals should choose a compliance software and services vendor that can provide solutions and support tailored to HIPAA requirements as well as their own enterprise. Anything less would be unhealthy.