FALL 2017
www.bdo.com

THE NEWSLETTER FROM THE BDO CENTER FOR HEALTHCARE EXCELLENCE & INNOVATION

BDO KNOWS HEALTHCARE

CONTENTS

PILOT PROGRAM TESTS EASING FDA REGULATORY BURDENS FOR LOWER RISK MEDICAL DEVICE PRODUCTS

by Dr. David Friend and Patrick Pilch

The healthcare industry's cries for a less burdensome approval process for new medical products have been heard and solutions are finally being tested.

In late July, Food and Drug Administration (FDA) Commissioner Scott Gottlieb announced a pilot program to explore a "pre-certification" to fast-track the approval process for medical software products. The Software Precertification (PreCert) Pilot Program, which launched on Sept. 1, is designed to more closely examine the software or digital health technology developer instead of the standard process that focuses primarily on the product.

The working theory: If the FDA has a full understanding of the company that's making the product, it could be pre-certified so that its low-risk software products could bypass parts of the traditional 510(k) premarket submission process, or potentially go straight to market.

TOP INSIGHTS FROM THE BDO KNOWS HEALTHCARE BLOG

- BLOG On Your Mark, Get Set, Collect...Data: Are Providers Ready for Oct. 2 MIPS Deadline?
- BLOG Designing a Consumer-Centric Telehealth Experience
- BLOG IRS Revokes Hospital's Tax-Exempt Status, Shedding Light on Section 501(r) Compliance Concerns
- Watch: 6 Things to Know About Healthcare's Cyber Threat Landscape
- BLOG How to Enable, Implement, Measure and Reward the "Value" in Value-Based Care

Read more and subscribe at www.bdo.com/blogs/healthcare/

Read more ▶

CONTINUED FROM PAGE 1

FDA REGULATORY BURDENS

TESTING THE THEORY

Products regulated by the Center for Devices and Radiological Health (CDRH) will be the primary focus; products can be at any phase of development. The FDA limited the pilot to nine participants that best met the following criteria:

- The company must be developing or planning to develop a software product that meets the definition of a device in section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321(h)).
- The company has an existing track record in developing, testing and maintaining software products demonstrating a culture of quality and organizational excellence measured by Key Performance Indicators (KPIs) or other similar measures.
- Companies may be traditional medical device manufacturers or non-traditional device manufacturers.

On Sept. 26, the FDA announced nine companies from more than 100 applicants would participate in the pilot program: Apple, Fitbit, Johnson & Johnson, Pear Therapeutics, Phosphorus, Roche, Samsung, Tidepool and Verily. Their collective products in development include a smartwatch to detect heart abnormalities and a contact lens that could continuously monitor the body's blood sugar.

The goal is for companies in the pilot program to work collaboratively with the FDA, sharing insights about how they perform high-quality design, testing and maintenance on their products. Participants will:

- provide access to measures and KPIs that demonstrate quality and organizational excellence
- collect real-world post-market performance data and provide it to the FDA
- be available for real-time consultations with the FDA
- be available for site visits from FDA officials and
- provide information about the firm's quality management system.

FDA'S TRANSFORMATION PROCESS

The pilot program is a key element of the FDA's Digital Health Innovation Action Plan, which lays out a vision for how CDRH will encourage digital health innovation while continuing to protect and promote public health. It acknowledges the need for a new way forward for software products that have a more iterative and fast-moving design, development and validation process than many of the hardware-based medical devices.

The move fits into the FDA's broader efforts to update its policies, processes and procedures around digital health technology. The 21st Century Cures Act (the Cures Act), signed into law in December 2016, gave the FDA the impetus and funds to make these changes, dedicating $500 million to streamline regulations that would accelerate the approval process for drugs and medical devices.

Bakul Patel, associate director for digital health at the FDA, said the goal of the PreCert program is to align with the speed and manner in which products are being developed, in addition to achieving international alignment with other regulatory bodies.

The FDA has been leading an international effort to converge regulatory principles for Software as a Medical Device (SaMD). The International Medical Device Regulators Forum (IMDRF) has already agreed on common SaMD terminology and quality management systems principles for software.

WHAT DOES THE PROGRAM MEAN FOR PROVIDERS?

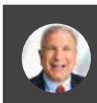
As more providers embrace the valuable data and insights they can derive from new technologies, they must carefully weigh the associated risks.

While an expedited regulatory approval process for lower-risk products can bring new innovations to market more quickly, it can also open the door for product discrepancies to slip through the cracks. Ultimately, providers are responsible for the safety of the products used inside their facilities and must implement their own internal controls to assess the quality of software and devices before using them or offering them to patients. Providers should consider mimicking the FDA's use of real-world evidence when making decisions about products and partners.

Accelerating innovation will likely introduce more unknown vendors to the healthcare marketplace and spur further investment in digital health companies, which received $4.2 billion in venture funding in 2016. The FDA's vetting process is a critical first step, but it shouldn't be the only step. Providers must still conduct their own due diligence to ensure vendors have appropriate policies, procedures and internal controls in place, and are compliant with federal and state regulations to ensure patient safety. With the influx of cyber threats against the industry, reviewing and instituting appropriate cybersecurity defenses for any new technology-related product is of the utmost importance.

Carefully mitigating the risks will be critical to delivering on the promise of improved outcomes that new technologies can deliver.

A version of this article originally ran in PM360 Online.



David Friend, MD, MBA, is chief transformation officer and managing director in The BDO Center for Healthcare Excellence & Innovation. He can be reached at dfriend@bdo.com.

Patrick Pilch, CPA, MBA, is the national co-leader of The BDO Center for Healthcare Excellence & Innovation. He can be reached at ppilch@bdo.com.

Read more ▶

CYBERSECURITY DESERVES INCREASED ATTENTION IN DEAL NEGOTIATIONS

By John Riggi and Patrick Pilch

Ascension's acquisition of Presence Health in August is just one in a series of healthcare mega-mergers announced this year.

In July, Beth Israel Deaconess Medical Center and Lahey Health signed a deal that will create Massachusetts' second-largest health system; Greenville Health System and Palmetto Health also announced plans to join forces and create South Carolina's largest health system. The medical device market has seen its share of major deals as well, including Abbott's $25 billion acquisition of St. Jude Medical and Becton Dickinson's $24 billion purchase of C.R. Bard.

As more deals unfold and the due diligence process ensues, a significant hidden risk often sits on the sidelines: cybersecurity risks. Too often in the deal-making process, cyber is viewed as a check-the-box compliance issue and given lower priority. But with the escalating impact, scale and complexities of cyber issues, companies can no longer afford to breeze over it.

THE PRICE OF INATTENTIVENESS

Research suggests that a high-profile cyber breach can have an immediate cooling effect on the prospects of a deal. In a recent survey of 276 directors and officers of public companies by Veracode and NYSE Governance Services, 22 percent said they would avoid acquiring a company that had recently suffered a high-profile data breach; 52 percent said they would consider it, but only at a significantly lower value. Not only are data breaches financially expensive, with one stolen electronic health record costing an **average $380**, but they can create significant reputational harm.

For a prime example of how cybersecurity can affect deal value, we can look outside the healthcare industry to Verizon's acquisition of Yahoo. Following revelations that more than a billion user accounts had been compromised in a massive data breach, Yahoo had to slice **$350 million** off its asking price.

Even after a deal is closed, cyber issues can rattle companies. Case in point: Abbott Laboratories landed in hot water with the Food and Drug Administration (FDA) earlier this year for failing to properly investigate and address the cybersecurity vulnerabilities of implanted heart devices that it acquired when it purchased St. Jude Medical in January. In April, the FDA issued a letter condemning St. Jude for denying claims that the external devices used to transmit and receive data from its pacemaker and defibrillator systems were vulnerable to hacking. While Abbott claimed that the issues happened before the takeover was completed and issued a security patch shortly after the deal closed, the FDA still held them responsible for not doing enough to adequately resolve the issue.

THREAT LEVELS RISE

The Abbott situation simply put a spotlight on new security vulnerabilities that are arising alongside the growing pool of interconnected devices in healthcare. Millions of medical devices have been installed in the U.S. over the past decade—many of which were created with older, less sophisticated security measures. Regardless, healthcare providers are on the line to ensure these devices are keeping both patients and their information safe. Richard Staynings, principal and cybersecurity healthcare leader at Cisco, highlighted medical device companies and healthcare providers' cyber Catch-22: Medical device vendors

Read more ▶

CONTINUED FROM PAGE 3

CYBERSECURITY

fear losing their FDA certification if they surface a security problem that requires patching their medical devices; meanwhile, healthcare facilities are reluctant to take devices like CT scanners offline to install security patches since they are used so frequently.

Hackers are increasingly targeting healthcare organizations as well. The Protenus mid-year Breach Barometer tracked 233 healthcare data breaches in the first half of 2017, impacting more than 3 million patients. There were 75 hacking incidents and 29 ransomware incidents, although experts suggest these are largely underreported right now. Experian's data breach forecast highlights ransomware as a top concern for the industry—although there have been fewer incidents, the consequences are more severe. Hackers have discovered that most healthcare organizations are willing to simply pay the ransom because the disruption is potentially catastrophic to business operations and patient safety. Experian predicts that ransomware attacks may escalate from "simply locking systems to outright stealing information to either sell or leverage for identify theft." With personal health information among the most lucrative data to steal, and healthcare IT systems largely viewed as weak, the industry is expected to remain a top target for financially motivated attacks. And with human lives at stake, it's a prime target for cyber warfare.

WHY COMPLIANCE ISN'T ENOUGH

Compliance audits and logs are frequently the default source of information to evaluate cyber risks during the due diligence process of a deal. The problem with that approach? Compliance takes a "just enough" attitude to meeting minimum standards. It doesn't provide insight into how the organization monitors, tackles and resolves cyber issues. It lacks critical security insights, such as:

- Security incident logs, which detail historical and current incidents and how they have been resolved (or not)
- What kind of access employees have to software applications and the varying levels of security
- How cybersecurity is woven into the organizational culture
- Third-party and vendor cyber policies and risks

Further, regulators can take some time to catch up to issues already happening in the industry. For example, it wasn't until July 2016 that the HHS Office of Civil Rights **issued guidance** on ransomware attacks. While companies may escape regulators' wrath if they only do the bare minimum, they can expect to take a hit in the court of public opinion—resulting in real losses in share value.

DIGGING DEEPER INTO CYBER ISSUES

Buyers and sellers alike must proceed with extra care in evaluating cyber issues when entering into any kind of transaction with another healthcare company. To effectively assess cyber risks, the following steps should be taken as part of the due diligence process:

1. **Conduct a cyber risk assessment.** Determine the current state of the target organization's cyber risk profile. Performing a cybersecurity risk assessment is far less expensive than the fines, reputational damage and regulatory issues that arise following a cyber incident. A risk assessment and gap analysis can help quickly assess current policies and operations, identify gaps and prioritize remediation initiatives.
2. **Take inventory of sensitive target company data.** The increasing frequency and severity of threats emphasizes the need for companies to implement strong information governance policies to achieve compliance and mitigate information-related risks. Understanding what kind of data an organization has, where it resides, who has access to it both inside and outside of the organization, and how it's protected is key to prioritizing and developing a mitigation strategy for the highest risks. Protecting potential new assets as part of a deal is key, but having this knowledge can also help maximize the value of the deal.
3. **Examine insurance plans to ensure adequate levels of cyber coverage.** Cyber insurance may be purchased as a stand-alone policy or included as an additional coverage under a professional liability policy. Coverage levels and terms, however, may vary greatly. Acquirers should evaluate current policies and levels of coverage, particularly if cyber coverage is added to another policy form. This may help to ensure the target organization—and subsequently the acquirer—is properly protected from losses associated with a cyber incident.
4. **Perform a thorough analysis of a target entity's IT systems and functions.** This type of analysis can help identify underperforming areas that introduce risks or optimization opportunities that can create additional value, which could serve as critical bargaining chips during deal negotiations. The process should consider policies, processes and services, facilities (data centers and other processing centers), wired and wireless networks, identity and access management, hardware and operating systems, applications and data, third-party vendor risks, business continuity and disaster recovery plans, social media and big data.

While regulatory guidance and rules are still evolving around healthcare cybersecurity measures, it's not the time to be lax. When you buy a company, you're not only buying their data; you're taking on the security risks that come with it.

John Riggi is the head of BDO's Cybersecurity and Financial Crimes practice. He can be reached at jriggi@bdo.com.

Patrick Pilch, CPA, MBA, is a national co-leader of The BDO Center for Healthcare Excellence & Innovation. He can be reached at ppilch@bdo.com.

Read more ▶

WHY ASC 606 ELEVATES RISK FOR LONG-TERM CARE PROVIDERS

by Steven Shill and Venson Wallin

The Department of Justice's largest-ever healthcare fraud enforcement action, announced in mid-July, sends a clear signal about the federal government's escalating efforts to eradicate and penalize fraud in healthcare: They're here to stay.

Attorney General Jeff Sessions said the investigation was spurred by "computer programs that identify outliers" as well as tips from affected communities, underscoring the impact of new data analytics technologies and algorithms in detecting fraud faster and more efficiently.

The long-term care (LTC) sector has been no stranger to fraud risk, whether tied to Medicaid enrollment or liability under the False Claims Act for reimbursement under Medicare or Medicaid. With many long-term care settings where providers are paid a daily rate for care, there is added risk that a provider will skimp on care to try to boost profits. Programs like New York's managed long-term care plans for dual-eligible individuals and PACE (Program for All-Inclusive Care for the Elderly) can also be exploited through fraudulent activity like incorrect enrollment, falsified enrollment information, billing for services that were provided but not medically appropriate and misreporting patients as nursing home-eligible.

Regardless of your organization's unique exposure to potential fraud, it's worth noting that the new revenue recognition standard introduced by ASC 606, *Revenue from Contracts with Customers*, adds another significant layer of complexity to the equation.

Because ASC 606 is taking effect at the same time as value-based reimbursement initiatives under Medicaid and Medicare take hold, compliance with the new revenue recognition standard can pose particular challenges to LTC providers receiving bundled payments and reimbursements tied to specific quality metrics.

One of the most significant changes between the old standard and the new is the treatment of variable consideration. Revenues under value-based arrangements are considered a variable consideration because these reimbursements may be subject to retroactive adjustment after the fact.

The new guidance stipulates that an entity should recognize revenue only to the extent that it is probable that the amount of variable consideration would not result in a significant reversal of cumulative revenue recognized when the uncertainty is subsequently resolved — a concept known as the constraint. Accurately estimating variable amounts is likely to be difficult for LTC providers as value-based reimbursement initiatives under Medicaid and Medicare take hold, as it requires visibility into the costs and quality of other providers to make a reasonable assessment. The complexity of these new considerations opens the door to unintentional accounting errors and material misstatements as well as outright fraud.

DIGGING INTO ASC 606 AND FINANCIAL REPORTING

The complexity of ASC 606 increases the risk of inadvertently presenting misleading financial information, and inappropriate

Read more ▶

CONTINUED FROM PAGE 5

ASC 606

reporting can conceal other, both intentional and unintentional, fraud and abuse situations. Healthcare organizations as a whole already struggle to use comparable revenue measures across a variety of provider types and structures, a challenge that is particularly felt by LTC providers. When trying to represent such diverse revenue streams in financial statements, LTC providers will need to be careful to include appropriate supplemental disclosures and discussions to avoid inadvertently presenting misleading information in their financial reporting.

Inappropriate reporting could result in retroactivity, which in turn results in recovery of funds from Medicare or Medicaid programs that the LTC provider was not entitled to receive. It could, in fact, hide situations where retroactive reconciliation could call for the repayment of funds to federal or state programs. The underlying complexity of ASC 606 may make fraud and abuse or pure financial fraudulent reporting situations more difficult to detect, or even cover them up entirely.

Revealing fraudulent financial reporting may, in some cases, reveal fraud and abuse situations in turn. In many cases, fraud and abuse situations are discovered by chance by external auditors examining a contract who discover inappropriate financial reporting.

For example, inappropriate revenue recognition or deferral can sometimes be used to cover up the existence of kickbacks for referrals or pressure on nursing homes to certify permanent placement. Such situations only become evident when auditors break apart the revenue streams and evaluate the contacts under financial accounting rules in accordance with Generally Accepted Accounting Principles. This sometimes goes down to the granular level of tracing debits and credits through the general ledger.

ADDED DUE DILIGENCE NEEDED DURING M&A

With consolidation in the sector predicted to accelerate during the Trump administration, LTC providers should note fraud discoveries can also be made during mergers and acquisitions during the due diligence and adjustment phase.

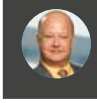
For example, consider a scenario in which an acquirer discovers financial algorithms written by the acquired company that excluded certain transactions, resulting in overpayment from the federal government under Medicare. In addition to fraudulent reporting, there's also a question of liability for the acquirer, in accordance with existing reps and warranties pursuant to the purchase agreement.

It's key for any potential acquirer to examine contracts and quality metrics that their potential target has generated during the due diligence phase, both from a data integrity as well as a clinical standpoint. Value-based reimbursement is a sea change, so buyers should prioritize ensuring the seller has the ability to effectively capture quality metrics after the deal closes. From an investment point of view, if the seller is projecting revenues or quality metrics solely based on their historical data, there's no guarantee the organization can replicate that as reimbursement continues to evolve. Under value-based reimbursement, ensuring the accuracy of quality metrics is one of the first lines of defense against inadvertent improper financial reporting as well as fraud and abuse.

The increased scrutiny of financial measurement brought on by changing revenue recognition standards coupled with a doubling-down on fraud enforcement by the Department of Justice aided by increasingly sophisticated data analytics tools, necessitate extreme caution for LTC providers.

This column was originally published in the Oct. 3 edition of McKnight's.

Steven Shill, CPA, is an assurance partner and the national co-leader of the The BDO Center for Healthcare Excellence & Innovation. He can be reached at sshill@bdo.com.



Venson Wallin, CPA, is a managing director in The BDO Center for Healthcare Excellence & Innovation. He can be reached at vwallin@bdo.com.

DID YOU KNOW...

A report from *Health Affairs* showed that admissions prices were 5 percent lower in concentrated provider and insurer markets compared to less dense markets.

A June 2017 survey from NueMD revealed that only 9 percent of providers consider themselves very familiar with MACRA, and half said they were not at all familiar.

While 80.5 percent of hospitals have in place at least a basic electronic health record system, gaps remain when it comes to advanced usage, particularly among critical access hospitals, according to a study from the *Journal of American Medical Informatics Association*.

About 3 percent of emergency room visits are unnecessary, according to a report from the *International Journal of Quality Healthcare*. Alcohol, dental and mood-related diagnoses accounted for the top three avoidable ER visits.

A recent survey from HIMSS found that 85 percent of healthcare IT leaders conduct risk assessments at least annually. This marks a change in an industry often viewed as a top target for hackers.

Read more ▶

HEALTHCARE'S CYBERSECURITY DIAGNOSIS: WHAT PRIVATE EQUITY NEEDS TO KNOW

HOW WIDESPREAD IS THE INFECTION?[1]

458
total healthcare breaches in 2016

Healthcare accounted for **15%** of last year's cyber incidents

THE X-RAYS SHOW...

64% of healthcare breaches were motivated by **financial gain**

Internal threat actors were at the root of **68%** of breaches

30% were due to **human error**

ASSESSING THE DAMAGE

About 1/3 compromised **personally identifiable information** (PII)

Almost 1/4 **weren't detected** until months after the incident

WHAT'S AT STAKE FOR PRIVATE EQUITY?

PE HAS SKIN IN THE GAME

$41.7B: Total value of U.S. PE healthcare deals in the first half of 2017[2]

THE VALUE OF FUNDS' PORTFOLIOS IS ON THE LINE

Cyberattacks cost companies an average of **$15M a year**[3]

INVESTORS ARE DEMANDING ACTION

45% of LPs will require **cybersecurity risk assessments** for portfolio companies within 3-5 years[4]

7 STEPS TO STRENGTHEN YOUR CYBER IMMUNE SYSTEM

As PE fund managers consider ways to add value, incorporate cybersecurity into the conversation:

1. **Perform cybersecurity due diligence before investing.**
2. **Take your cyber pulse.** Identify possible vulnerabilities and assess current risk management programs.
3. **Confront the human element.** Train employees to securely handle sensitive data. Simulate phishing attacks to test their cyber smarts.
4. **Implement a risk-based, threat-driven patch management program.**
5. **Update your detection, threat monitoring and analytics tools.**
6. **Get ready for damage control.** Strengthen investigative and digital forensics capabilities to assess an incident's scope and severity.
7. **Develop and proactively, regularly test an incident response plan.**

1 Verizon 2017 Data Breach Investigations Report
2 *Pitchbook* 2Q 2017 US PE Breakdown
3 *CNBC*
4 Coller Capital

BDO

Read more ▶

MARK YOUR CALENDAR...

NOVEMBER

Nov. 9
HFMA Leveraging Operational Insights and Analytics for Bundled Payment Success
Webinar

Nov. 13-15
HFMA Seminars
Omni Parker House Hotel
Boston

DECEMBER

Dec. 4-5
World Congress Physician Relations Summit
Hyatt at the Bellevue
Philadelphia

Dec. 6-8
HFMA Seminars
Swissotel Chicago
Chicago

CONTACT:

STEVEN SHILL
Partner—Healthcare, National Leader
Orange County, Calif.
714-668-7370 / sshill@bdo.com

PATRICK PILCH
Managing Director—Healthcare,
National Leader
New York, N.Y.
212-885-8006 / ppilch@bdo.com

People who know Healthcare, know BDO.

ABOUT THE BDO CENTER FOR HEALTHCARE EXCELLENCE & INNOVATION

The BDO Center for Healthcare Excellence & Innovation unites recognized industry thought leaders to provide sustainable solutions across the full spectrum of healthcare challenges facing organizations, stakeholders and communities. Leveraging deep healthcare experience in financial, clinical, data analytics and regulatory disciplines, we deliver research-based insights, innovative approaches and value-driven services to help guide efficient healthcare transformation to improve the quality and lower the cost of care. For more information, please visit https://www.bdo.com/industries/healthcare/overview.

@BDOHealth www.bdo.com/blogs/healthcare

Accountants | Advisors | Doctors

www.bdo.com/healthcare

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.