PRESENTED BY HealthData Management | SourceMedia

Demystifying Third-Party Vendor Risk Management for Healthcare Organizations

Outsourcing is a fact of life for healthcare organizations, from routine functions such as food services and laundry to regulatory compliance and clinical activities. Large numbers of vendors must be properly managed in order to reduce clinical, financial and regulatory risk. This paper discusses how to reduce complexity in third-party vendor risk management, and how to turn uncertainty and confusion into efficiency and confidence.

SPONSOR CONTENT FROM PREVALENT®

It is fairly typical for even a mid-sized hospital or healthcare organization to be doing business with dozens, or even hundreds, of vendors.

Healthcare organizations face a wide range of potential challenges, many of which require tight relationships with third-party vendors.

Take regulatory compliance. By now, the entire industry knows about the Business Associate Agreements (BAA) section of HIPAA and the responsibilities of all parties in adhering to the regulatory guidelines. The penalties for violations by BAs are substantial and unyielding, with little to no leeway for healthcare organizations contracting the offending parties. It's worth noting that nearly half of the respondents to a highly respected industry study said ineffective BAAs increased security vulnerabilities for patient information.[1]

The focus on BAs, of course, goes far beyond compliance. In fact, the healthcare industry is one of the most active and strategic users of outsourcing partners across the economic spectrum. That trend is driven by a number of factors, such as financial tradeoffs, the desire to focus on core competencies and the need for specialized skills.

Outsourcing fairly routine and tactical support functions such as food services, laundry and facilities security and access has been commonplace for decades. More recently, services deemed closer to the delivery of critical services such as billing services, medical staffing, pharmacy management, clinical documentation, HIPAA compliance, claims processing, malpractice insurance, litigation and information technology have been added to the outsourcing checklist. And, more clinical activities now have been outsourced, including radiology, dialysis and psychiatric services.

As a result, it is fairly typical for even a mid-sized hospital or healthcare organization to be doing business with dozens, or even hundreds, of vendors. This makes vendor risk management a complex challenge.

THE PROBLEMS AND IMPLICATIONS OF THIRD-PARTY VENDOR RISK IN HEALTHCARE

The most fundamental questions about outsourcing in healthcare—should we outsource and, if so, which functions should we outsource—have been answered. Outsourcing is widely deployed in healthcare for a wide range of business and operational requirements.

The financial and operational benefits of outsourcing have opened the eyes of many hospital administrators and medical executives, and now even highly specialized and strategic clinical functions are being outsourced for many of the same reasons. Functions traditionally handled exclusively or primarily with in-house resources, such

[1] "State of Cybersecurity in Healthcare Organizations in 2016," Ponemon Institute, February 2016

Few, if any, organizations have a full and up-to-date inventory of their third-party relationships.

as medical imaging, are increasingly being outsourced to Business Associates. And fast-growing, newer applications such as telemedicine have a strong outsourcing orientation.

But as the number of third parties doing business with healthcare organizations continues to expand, there is mounting pressure on those organizations to get a better handle on the risk exposure they are facing. That risk includes such factors as how protected health information is handled, how systems are accessed and the availability of services by Business Associates.
Beyond compliance, there are very real legal, clinical, operational and financial risks that go along with managing so many different vendors for so many different services. To start, few, if any, organizations have a full and up-to-date inventory of all third-party relationships and an accurate and relevant index of services provided and associated risks.

DEMYSTIFYING THIRD-PARTY VENDOR RISK MANAGEMENT: GETTING STARTED

The good news: Many—maybe even most—healthcare organizations—understand that their swiftly escalating number of third-party vendors has added complexity and risk. The bad news: Few of them actually have a plan in place to address those challenges, and many of them lack a firm idea of where to start. This is certainly true as more and more new vendors are added to the mix. However, it is particularly problematic to identify and analyze risk potential for the huge number of legacy vendors that have been doing business with the organization for year.

Getting a firm handle on third-party vendor risk management is essential, but it need not paralyze the organization. In fact, there are some clear steps organizations can and should take in order to identity, manage and reduce risks associated with working across a diverse number and type of third-party vendors.

- **Build a complete, accurate and up-to-date inventory of third-party vendors.** Some organizations' accounts payable and contracts departments can help with this, but don't be surprised if they are missing documents or have less formal relationships with suppliers. This is why having a diverse team of stakeholders from different parts of the organization is important; doing so increases the chance "rogue" vendor will be spotted and added to the inventory.
- **Have a system for categorizing the types of services those vendors provide.** This is vital in order to determine what unique risks are inherent within each group, so that a third-party vendor risk management plan accounts for the specific risk exposure of each type of service provided.

40 Technology Drive • Warren, NJ 07059
info@prevalent.net • Toll Free: (877) PREVALENT

Solutions exist today that help healthcare organizations continue to use outsourcing as a strategic tool to improve efficiency and competitiveness.

- **Analyze the financial cost and business impact of what diminished, delayed or total lack of availability of a service means to the organization.** This will be important to know as you put together a new system for risk mitigation, because not all organizations will have the resources to tackle everything simultaneously.
- **Keep in mind that even if your organization is doing periodic assessments of third-party risk, those assessments have limited value going forward.** Most vendor assessments are static, "point in time" analyses. Just like regulatory compliance, not all vendor risk is properly managed at all points in time unless there is a comprehensive, automated, ongoing solution.

CONCLUSION

Third-party vendor risk management has become significantly more challenging as healthcare entities increase their outsourcing of a wider number and range of critical business and clinical activities. This has led to an increased awareness of the scale and scope of the problem, as well as a commitment to finding solutions.

While many healthcare organizations still struggle with the best way to get started on identifying and implementing solutions, it is encouraging that new, flexible and efficient technology-based options are available. Solutions exist today that help healthcare organizations continue to use outsourcing as a strategic tool to improve efficiency and competitiveness, while also identifying and dampening potential risk sources that expose the organization to potential regulatory violations and loss of patient trust.

For more information on how Prevalent helps healthcare organizations reduce and manage risks associated with third-party vendors, please visit www.prevalent.net.

40 Technology Drive • Warren, NJ 07059
info@prevalent.net • Toll Free: (877) PREVALENT

ABOUT PREVALENT

Clearly, finding a way to manage the risks of all these third-party relationships can no longer be done with a few in-house employees using manual processes. Identifying, categorizing and assigning risk factors to several hundreds or several thousand vendors and Business Associates (as well as the constant stream of new Business Associates) requires a technology-based solution built on a foundation of discovery, automation, policy management, accuracy and cost reduction.

Prevalent has a long history of success in helping healthcare companies minimize the burden of controls, data collection and distribution, workflow management, risk scoring and problem remediation. Its Synapse platform is a purpose-built, cloud-based SaaS solution designed for high availability, robust security and easy scalability as more and more third-party vendors are added to the mix.

Synapse is ideal for small networks, as well as large, diversified health care organizations. It prioritizes efficient data collection and security controls sharing. Prevalent has been selected by the National Health Information Sharing and Analysis Center (NH-ISAC) as a foundation element in CYBERFIT™, a third-party shared-risk assessment tool that provides automated evidence collection and risk assessments for healthcare industry third-party vendors.

40 Technology Drive • Warren, NJ 07059
info@prevalent.net • Toll Free: (877) PREVALENT