VIEWS & VISIONS

A publication of Bowles Rice LLP

Fall 2017

How Well Do You Know Your Fourth-Parties?

Katie J. Stanich, CPA, Director of Audit & Compliance
The Health Plan

Katie J. Stanich serves as the Director of Audit & Compliance for The Health Plan. Her role encompasses all facets of these areas, from corporate, government and regulatory compliance to internal audits and implementation of the Model Audit Rule ("Sarbanes-Oxley for insurance companies"). Stanich is committed to continuously evaluating and refining The Health Plan's risk profile, but gets the greatest satisfaction in identifying opportunities for her organization to become more efficient and effective.

Before starting with The Health Plan, she was responsible for the internal audit function at both Gateway Health Plan and Allegheny Health Network. She also worked as a senior manager for EY, specializing in external audits of healthcare organizations.

Stanich received her undergraduate degree in finance from the University of Pittsburgh and her master's in accountancy from the University of Virginia. A certified public accountant, Stanich formerly served on the board of Pittsburgh Cares, a non-profit volunteerism group, and is actively seeking a similar board opportunity in West Virginia.

The phrase "vendor risk management" is enough to send shivers down the spines of audit and compliance professionals everywhere, particularly in the health care industry, where we constantly deal with sensitive data and a complex regulatory environment. When you exchange compensation for goods or services, your organization is assuming additional risk. The news is crowded with examples of large, sophisticated organizations who experienced significant data breaches or service disruptions which started with their vendors. (Anybody recall Target and its HVAC vendor?)

Perhaps you feel comfortable with your organization's existing monitoring of third-parties, but what, if anything, has been done with respect to "fourth-parties"? A fourth-party is a subcontractor of your vendor with whom your organization has little or no direct contact. Just think of the magnitude of processes a typical organization outsources to third-parties, and then consider that each of your vendors might also have a similar number of its own vendors.

As a result, your organization likely has more fourth-parties than third-parties!

Now that we have identified the potential problem, let's explore some strategies to effectively deal with fourth-parties.

Make sure your own house is in order. Ensure that your vendor management and monitoring processes are robust.

Do you have a comprehensive inventory of all third-parties? To underscore the importance of compiling and maintaining this inventory, consider that lists of First-Tier/Downstream/Related Entities (FDRs) and business associates, both subsets of your list of third-party vendors, are common audit requests from the Centers for Medicare and Medicaid Services (CMS) and the Health and Human Services Office for Civil Rights (OCR), respectively. Set up a process to keep your inventory current and test your process by periodically reviewing all payments made to outside entities. Don't forget to include vendors who are not paid through your accounts payable function, such as vendors paid on a percent-of-savings basis that deduct their fee from recovered amounts instead of submitting an invoice, and any joint ventures or similar arrangements.

Do you conduct periodic vendor risk assessments? This could ultimately be incorporated into your overall organizational

risk assessment process, but if it's your first time through, consider performing it as a separate exercise. Ensure that your risk assessment has enough specificity to be meaningful. The risks you have with a third-party call center are not the same as a vendor who sends nurses into the home of a member or patient. Identify these risks and prioritize accordingly.

Openly and regularly communicate with your vendors. Successful monitoring of fourth-party vendors cannot happen without an open and productive communication channel with each of your primary vendors. The level of transparency and disclosure around these fourth-parties can be indicative of the quality of your third-party's vendor risk management program. Make sure to speak to the "right" vendor contact for a comprehensive understanding of any fourth-party resources.

The account executive or relationship manager may not know how your organization's data is accessed or the physical location of all servers that house such data, including whether any data are held offshore. Ask questions, and keep asking, until you are satisfied that you have been given a complete and accurate answer – and don't forget to leverage your internal subject matter experts in IT, operations, etc. to ensure that you do! Remember, this is not a "one and done" exercise. Your vendors may enter into arrangements with new subcontractors at any time.

Think of creative strategies to mitigate risk. Review your contract language and build in language that requires your vendors to notify you in advance of any subcontractors obtaining access to your systems or data. Depending on your organization's regulatory requirements, this may be particularly important for offshore resources.

Fold a review of vendor/subcontractor system and data access into your existing IT logical access testing. What is your current process to identify vendor employees whose roles no longer require access to your systems or who have terminated employment entirely? Such processes should be mirrored for fourth-parties.

Does your vendor perform internal audits of its vendors? If so, ask for copies of those reports, or consider performing a site visit or participating in an internal audit for particularly significant subcontractors. Ask for information on any corrective action plans the vendor has required of their subcontractors. Be sure to obtain a System and Organization Controls (SOC) report, which will give you information on the subcontractor's internal controls around financial reporting (SOC 1) or security, privacy, and/or processing integrity (SOC 2).

In the event of a compliance issue, data breach or other unfortunate incident, your regulators and customers will ultimately hold your organization responsible and will care little whether the issue originated with one of your vendors, or, for that matter, your vendor's vendor. Implementing robust third- and fourth-party processes now could avoid an embarrassing front-page headline later.