

The Bigger Picture: From Vendor Credentialing to Vendor Management

By John Harper

Executive Summary

Vendor credentialing, a fast-growing trend in healthcare operations, is driven by a confluence of patient activism, regulatory oversight, and economic concern. At its core, vendor credentialing in healthcare is simply the process of ensuring that the individuals and entities that sell goods and services meet the standards and requirements of the purchasing healthcare providers. Confusion arises because standards and requirements are set by a complex web of interested parties both inside and outside the provider organization. This article identifies some of the risks and areas for internal auditors to look into.

Vendors Touch the Entire Hospital

Within healthcare provider organizations like hospitals, many functions interact with vendors in distinct as well as overlapping ways. Clinicians are interested in the efficacy of the service or product. Materials management is concerned about supplier pricing and performance. Compliance organizations are on alert for sanctioned vendors and improprieties. Legal wants to ensure appropriate terms and indemnifications are included in contracts. Additionally, each function has its own set of standards, or credentials, that apply to the vendor selection and ongoing vendor performance.

Primarily two forces have driven the recent rise in vendor credentialing activity.

Primarily two forces have driven the recent rise in vendor credentialing activity. First, delivering quality patient care with 'quality' defined by several organizations. Second, controlling

medical costs and improving the return on medical dollars.

Patient care guidance has come from medical associations, such as the American College of Surgeons (ACS) and The Association of Peri-Operative Registered Nurses (AORN), which have voiced concerns about vendor influence and transparency in patient care. The Joint Commission, the leading accrediting organization for hospitals themselves, also has become interested in the role and documentation of any person in a procedural area, including healthcare industry representatives. The Centers for Disease Control (CDC) has made statements regarding immunizations in the interest of patient safety and potential pandemic management.

Financial concerns come directly from the payers, both private and public. For example, the significant expenditures by Medicare/Medicaid on US healthcare has led those government agencies to look twice at the transparency and appropriateness of vendor activities and payments to prevent fraud and waste.

Starting with Patient Access

Vendor credentialing is frequently simplified to focus on the 'rep in the hall,' that is, the vendor representative in

procedural areas. In 2000, the American College of Surgeons issued a *Statement on Healthcare Industry Representatives in the Operating Room*. This statement, revised in 2005, defined the appropriate role of industry representatives in the OR with a focus on patient safety and privacy, and corraling any appearance that a rep may influence medical care. Specifically, the statement suggests:

- A time-limited approval and appropriate identification (to be worn at all times) for the Health Care Industry Representative (HCIR)
- Ensure orientation to the facility is provided
- Verify the documentation that certifies the HCIR has had education and training in:
 1. HIPAA compliance and all matters related to patients rights and confidentiality
 2. Appropriate conduct and attire in the OR environment
 3. Aseptic principles and sterile techniques



4. Infectious disease and blood borne pathogens
5. Occupational Safety: bio-hazardous waste, fire, electrical, radiation and other safety protocols
6. Other applicable practices that may be related to the operation:
 - Should not engage in the practice of surgery, nursing or medical decision making.
 - Should not scrub or be involved in direct patient contact.
 - Should have his or her activities monitored and supported by the surgeon (or, at the surgeon's discretion) by the peri-operative nurse responsible for the patient's care .

Other groups, such as AORN, have issued similar statements:

"It is important that the health care industry representative understands how to safely work in the operating room to assist the peri-operative team in maintaining the patient's safety, right to privacy, and confidentiality when a health care industry representative is present during a surgical procedure."

(<http://www.aorn.org/PracticeResources/AORNPositionStatements/>)

While the Joint Commission has actively announced it doesn't have requirements specifically for vendor representatives because no national standards exist, it does point to areas of its requirements that could apply "to any individual that enters a healthcare organization who directly impacts the quality and safety of patient care." (http://www.jointcommission.org/AccreditationPrograms/LongTermCare/Standards/09_FAQs/HR/hc_industry_vendor_representatives.htm) These standards include managing facility access, patient confidentiality awareness, verified education, training, orientation, health status, and other items.

In practice, Joint Commission tracers have expressed interest in vendor representatives. Hospitals have been asked to show how they record and control access to the OR, how they distinguish vendors from staff, and what records they have about the immunizations and training of vendor representatives on site.

Clinical departments faced with these requirements have created their own in-department responses. Reps are asked to sign in and out at the department reception desk. Bans on detailing with promotional items and food have become commonplace. Hospital staff at each department independently review the reps' copies of immunization and training records

Hospital Administration Gets Involved

Simultaneously, interest in managing vendors more closely is increasing at the administrative end of the hospital. Vendor-influence publicity, government involvement, and rising costs cause administrators to take a closer look at vendor selection.

Providers have an affirmative duty to check the Medicare program exclusion status of individuals and entities.

Critics, inside and outside the hospital, became increasingly vocal about the role and influence of vendors in Continuing Medical Education (CME) over 20 years ago. New policies designed to limit vendor influence and to increase the transparency of vendor-provider relationships have emerged. For example, many hospitals have policies that state any product sampling or trial is to be considered a gift and not subject for reimbursement. Product evaluation procedures prohibit vendors from introducing new products directly to clinical staff. But without any tracking or significant controls in place, these policies are difficult to enforce.

Non-payment and threats of fines from government entities for doing business improperly are increasingly strong and create concerns that a major revenue source could be jeopardized by even unintentional actions. A prime example is the Department of Health and Human Services Office of Inspector General (HHS/OIG) prohibition against payments to anyone who employs or contracts with an excluded party and any hospital or other provider where an excluded person provides items or services. Hospitals, therefore, are potentially exposed by

both direct employment or contracting with an excluded party or by allowing an excluded party to provide goods or services.

The categories of who can be excluded and for what reasons are broad. For example, the *Exclusion of Certain Individuals and Entities from Participation in Medicare and State Health Care Programs* includes not only individuals and companies, but even *entities with a controlling interest held by an excluded individual*. (http://www.ssa.gov/OP_Home/ssact/title11/1128.htm)

The OIG goes even further by assigning providers an affirmative duty to check the Medicare program exclusion status of individuals and entities or run the risk of Civil Monetary Penalties if they

fail to do so. While the OIG provides this information through the List of Excluded Individuals and Entities (LEIE), the list includes over 40,000 entries and is updated monthly. Civil Monetary Penalties can be significant, up to \$10,000 for each item or service furnished by the excluded party as well as up to three times the amount claimed. (<http://oig.hhs.gov/fraud/exclusions.asp>)

Cost and expense management has been addressed by the materials management function in hospitals. These departments typically have on-boarding processes that encompass financial due diligence and statements of liability insurance at the time of the initial contract. Going a step further, value analysis teams bring together supply chain, clinicians, and others in order to control costs by systematically selecting suppliers that best fit every department's standards and enabling volume contracts and terms.

For many hospitals, this financial due diligence occurs only at contract review. Yet, the rising rate of bankruptcies in the current economic climate creates continual concern about the stability of a supply chain to the point that a one-time credit check at contract signing is no longer sufficient.

Vendor Management: Tying It Together

Healthcare systems looking for a way to streamline the capturing, credentialing, and monitoring of one or more of these requirements has fueled the growth of the vendor credential service community. Today, approximately one third of the US hospitals have turned to third-party vendor credentialing providers for support with that number expected to rise to one half by the end of 2010 (based on Vendormate internal estimates).

No matter whether the hospitals decide to handle this internally or with an outsourcer, hospitals initiating a vendor credentialing program quickly face two dilemmas. First, which department sets the requirements? Second, who needs to meet these requirements?

In practice, department-level vendor credentialing creates significant gaps in meeting the true needs. Without a cross-functional view as to whether or not a vendor met the system's standards, vendor participation is inconsistent. Policy acknowledgments in one facility are not accessible by another facility. Details about which vendors are approved to provide which products aren't on hand in clinical areas when a rep comes to call. Reps are repeatedly asked for the same documents by multiple areas of the same system. Expired immunizations and training documents are easily overlooked when stored in a hard copy file in only one location.

Also, multiple definitions of who exactly is a 'vendor' must be reconciled. While

clinical concerns about vendors are primarily focused on the behaviors and status of an individual rep, many administrative concerns relate to the vendor as an entity. When the hospital contracts with a supplier, the contract is between two entities. The vendor representative in the facility has little impact on these issues. Ultimately, failures in vendor performance, whether by the company or the individual, are resolved between the entities.

“Department-level vendor credentialing creates significant gaps in meeting the true needs.”

In reality, there is a matrix of compliance and operational information required from both vendor reps and vendor entities.

Robust vendor management programs continually make the connection across all these functional lines—linking individual reps to their employer and the assessment of one department to the assessments of others.

Oakwood (MI) Healthcare System is an example of one healthcare provider that understands the interrelationship among patient safety, business practices, vendor reps and vendor entities. Oakwood ties the records in its vendor management system to its purchasing accounts payable system through unique vendor IDs.

“Patient safety is number one. So tracking the vendor rep is important, but that has to be tied to the vendor company as well,” said Jerry Derowski,

Director Supply Chain, R&D for Oakwood Healthcare System. “We use our vendor management system as the central place to manage our conflict of interest policy, to make sure vendors are financially sound, and to ensure that vendors are authorized before cutting POs.”

Internal auditors have the independence and expertise to help their hospitals identify the connections. Auditors

typically view an organization with a risk management point of view. Third-party risk management is well understood in the financial community, and healthcare can easily borrow a page from a Federal Deposit Insurance Corporation (FDIC) playbook. FDIC's guidance to managing third party risk in the financial community can help shape a framework of vendor risk that is equally applicable here. (FDIC FIL-44-2008 <http://www.fdic.gov/news/news/financial/2008/fil08044a.html>). Consider these risk parallels.

1. Compliance risk—Per the FDIC, this is the risk arising from violations of laws, rules, or regulations, or from noncompliance with internal policies or procedures or with the institution's business standards. Compliance risk is exacerbated when an institution has inadequate oversight, monitoring or audit functions.

In a healthcare practice, this could be:

- The ability of the third party to maintain patient privacy, i.e., HIPAA .
- Ability to identify sanctioned vendor companies, principals, and individuals before payments to guard against CMS fines, etc.
- Identification and response to potential Stark law and conflict of interest situations.
- Alignment with Joint Commission, CDC, AORN, ACS, and other recommendations to maintain accreditations.

Table 1

	Vendor Rep	Vendor Entity
Compliance Information	Joint Commission CDC AORN/ACS HIPAA Training Immunizations Ethics Federal/State Sanctions	Ethics HIPAA Federal/State Sanctions HHS/OIG OFAC Deficit Reduction Act/CMS Gift policies
Operational Information	Contact Details Access Sign In/Out Authorized Appointments Other Policies	Financial Health Legal Status Liability Insurance Status Product sampling policies Other Policies Contract

continued on page 49

Guidelines and Regulations Affecting Healthcare Vendors

Patient Care

American Council of Surgeons (ACS) Statement on Health Care Industry Representatives in the Operating Room—Supplier must wear a time sensitive means of identification at all times in the OR, be oriented to the particular healthcare facility, should be trained in HIPAA compliance and appropriate OR conduct and attire, and must receive education concerning infectious disease, blood borne pathogens, occupational safety, aseptic technique, and other applicable practices relating to the operation. (www.facs.org)

The Association of Peri-Operative Registered Nurses (AORN) The Role of the Health Care Industry Representative in the Perioperative/Invasive Procedure Setting—It is important that the health care industry representative understands how to safely work in the operating room to assist the perioperative team in maintaining the patient's safety, right to privacy, and confidentiality when a health care industry representative is present during a surgical procedure. (<http://www.aorn.org/PracticeResources/AORNPositionStatements/>)

The Joint Commission "The standards in the human resource chapter apply to direct, contract, and volunteer personnel providing patient care and/or services on behalf of an organization, regardless of whether the contracted organization is accredited." These standards include verified education, training, orientation, health status, and other items. (http://www.jointcommission.org/AccreditationPrograms/Hospital/Standards/09_FAQs/HR/Human_Resource_Standards.htm)

Centers for Disease Control Immunization of Health-Care Workers—These recommendations outline a variety of immunization guidelines for health care workers ranging from physicians to volunteers. (<http://www.cdc.gov/mmwr/preview/mmwrhtml/00050577.htm>) ©2009 Vendormate, Inc.

Business Practices

Department of Health and Human Services Office of Inspector General (HHS/OIG) List of Excluded Individuals and Entities (42 U.S.C. 1320a–7a) Establishes categories of parties excluded from payment by any Federal health care program for any items or services from an excluded individual or entity. This payment prohibition applies to the excluded person, anyone who employs or contracts with the excluded person, any hospital or other provider where the excluded person provides services, and anyone else. Providers have an affirmative duty to check the program exclusion status of individuals and entities (List of Excluded Individuals and Entities (LEIE)) prior to entering into employment or contractual relationships or run the risk of Civil Monetary Penalties if they fail to do so. The list includes over 40,000 entries and is updated monthly. CMPs are delineated as up to \$10,000 for each item or service furnished by the excluded party as well as up to three times the amount claimed. (<http://oig.hhs.gov/fraud/exclusions.asp>)

Federal False Claims Act (31 U.S.C. ss3729 et seq.) Prohibits conspiring to defraud the government by getting a false claim paid, presenting a false claim for payment or approval, or using a false record to avoid or decrease any obligation to pay the Government. Allows for penalties of \$5,500 to \$11,000 per claim, treble damages and costs of civil action brought to recover.

State False Claim Laws Deficit Reduction Act of 2005 Section 6031 and Section 1909 of the Social Security Act creates financial incentives for states to enact state Medicaid false claims acts similar to the Federal False Claims Act. States receive 10% of recoveries. States with FCA laws: California, Florida, Hawaii, Illinois, Indiana, Louisiana, Massachusetts, Michigan, Nevada, New York, Tennessee, Texas and Virginia.

Federal Anti-kickback Statute (section 1128B(b) of the Social Security Act) Civil and criminal penalties for an individual or entity that knowingly and willfully requests, solicits, gives or pays any remuneration, overtly or covertly, to induce a referral, purchase or lease of any good or service which may be paid under a Federal health care program, including Medicare. Safe harbor protection requires strict compliance with all applicable conditions set out in the relevant safe harbor. Criminal fines up to \$25,000 per offense and/or 5 years imprisonment, Administrative fines, exclusion from Medicare/Medicaid programs, and civil penalties up to \$50,000 plus treble damages. (http://www.ssa.gov/OP_Home/ssact/title11/1128B.htm)

Physician Self-Referral/Stark Law (section 1877 of the Social Security Act) Prohibits hospitals from submitting—and Medicare from paying—any claim for a "designated health service" (DHS) if the referral of the DHS comes from a physician with whom the hospital has a prohibited financial relationship. This is true even if the prohibited financial relationship is the result of inadvertence or error. In addition, hospitals and physicians that *knowingly* violate the statute may be subject to CMPs and exclusion from Federal health care programs. A knowing violation of the Stark law may also give rise to liability under the False Claims Act. (<http://oig.hhs.gov/fraud/complianceguidance.asp>)

Incentive for Self-Reporting Where the hospital discovers evidence of misconduct, the hospital should promptly report the existence of misconduct to the appropriate Federal and State authorities. Prompt reporting will be considered a mitigating factor by the OIG in determining administrative sanctions, if appropriate. (<http://oig.hhs.gov/fraud/complianceguidance.asp>)

General Services Administration (GSA) Excluded Party List Those excluded from Federal procurement and reciprocal programs. Any penalties or liability for doing business with an excluded party depends on the violation that led to ineligibility. (<http://www.epls.gov/>)

Department of Treasury Office of Foreign Asset Control (OFAC): Prohibits any transaction with persons on the specially designated nationals list. Maximum civil penalty is the greater of \$250,000 or an amount that is twice the amount of the transaction that is the basis of the violation. (<http://www.treas.gov/offices/enforcement/ofac/programs/terror/terror.shtml> and http://www.treas.gov/offices/enforcement/ofac/civpen/penalties/interim_pol_11272007.pdf)

©2009 Vendormate, Inc.

2. Operational risk—the inability to deliver services due to the actions or failure of the third party.

- What is the impact to the hospital or health system if a vendor is unable or unwilling to deliver products and services according to specifications or in a timely manner?
- How will this affect patient care?
- Are alternative providers easily identified and on-boarded?
- Vendors that are essential to the supply chain require additional monitoring.

3. Credit risk—the risk that a third party is unable to meet the terms of the contractual arrangements because of its own financial condition.

- What is the potential expense to the hospital from an insolvent supplier?
- How well does the hospital monitor the financial health of its key vendors?

4. Reputation risk—the risk of negative public opinion resulting from the actions of the third party. For better or worse, the behaviors of the third party are assigned to the healthcare system. When the actions of a rep in a procedural area result in damages, the hospital will carry the blame from the media and the public.

Summary

With a framework of risk in mind, vendor credentialing quickly evolves into vendor management, and internal

auditors can play an essential role in identifying gaps among policies, procedures, and enforcement. The vendor credentialing process can provide internal auditors tools to manage and monitor a variety of business processes and risks. This movement is an opportunity to institutionalize a vendor risk management point of view. The key is looking at vendor credentialing from a larger perspective than a compliance requirement. **NP**

John Harper is Director of Marketing for VendorMate, a provider of technology and compliance monitoring services in their relationships with vendors. John directs the company's brand management and marketing communication. His 20-year career spans Fortune 500 firms and small businesses. He may be reached by email at: john.harper@vendormate.com, or by phone at 404-920-3148.

Reprinted with permission from New Perspectives, Journal of the Association of Healthcare Internal Auditors, Inc. Volume 28 #4.

HIPAA enforcement is here.

Feel ready?
It's time for a *CheckUp*™

CheckUp™: CMS HIPAA Security Readiness Audit

CYNERGISTEK

Securing the mission of care.

IT Security | Compliance | eDiscovery
IT Audit | Data Protection | BC/DR
Risk Assessment

www.cynergistek.com