Vendor credentialing: Overview, Issues and Prospects

By Karen L. Ekstein, Ph.D.

This paper provides an overview of the vendor credentialing industry – an industry that has been steadily growing in the United States and, more recently, has been making an entrance into the Canadian market. Vendor credentialing as a process is not new – health care organizations have practiced manual, in-house forms of vendor credentialing for decades. Challenges presented in the current healthcare context, contribute to the insufficiency of the more primitive approaches to vendor credentialing. A need for more formal, sophisticated methods of supporting vendor access and partnering decisions has given rise to a 'revitalized' vendor credentialing industry; this newer vendor credentialing industry largely consists of third-party firms offering vendor credentialing systems and services.

Though there is considerable debate surrounding vendor credentialing and despite that there are many Canadian organizations weighing benefits of opting into vendor credentialing programs, there does not appear to be a cohesive, objective discussion of vendor credentialing or the vendor credentialing industry to use as a foundation for dialogue, research and decision making; it is this gap that the current paper seeks to address, by beginning to synthesize existing considerations of vendor credentialing and initially contemplate its implications. The purpose of this paper is to serve as the basis for dialogue, research and decision making on and around vendor credentialing within the Canadian context.

The paper begins with a history of vendor credentialing. Focus then turns toward the current healthcare climate and duties of healthcare organizations within this climate. Attention turns to the vendor credentialing industry today, and then to a discussion of the benefits of vendor credentialing, concerns about vendor credentialing and critiques related to vendor credentialing. Finally, the future of vendor credentialing is considered as are opportunities within and related to the industry.

History of the Vendor Credentialing

Vendor credentialing originated from a historical lack of enforced controls for restricting access and preventing unauthorized access to patient files (Crans, 2010; Garner, 2012). In years past, health care organizations' had lax security (Crans, 2010; Garner, 2012). Anyone could walk halls of a health care facility without being questioned, patients` files would be kept in the open (Crans, 2010; Garner, 2012) and individuals could access patients` medical records without being questioned about their interest in the files (Garner, 2012). While there were sign-in procedures akin to earlier forms of vendor credentialing they were rarely enforced and often ignored by vendors (Crans, 2010; Garner, 2012).

The impetus to adopt vendor credentialing programs arose, at least in part, from pressures health care organizations were experiencing to increase quality of care while controlling costs of care (Douglas, 2011). Hospital security representatives increasingly put pressure on hospitals to keep a closer watch on vendors (DeJohn, 2009). The rationale for increased scrutiny of vendors

specifically was related to the idea that controlling vendor access to sensitive areas of a health care facility and health care practitioners could reduce patients' and organizations' vulnerability to various safety, security, privacy and could, therefore, reduce the health care organizations' risks of exposure (Douglas, 2011).

A need for more rigorous, sophisticated and robust vendor credentialing programs, combined with recognition that agents of health care facilities were having challenges implementing vendor checks and restricting vendor access in-house, led to healthcare organizations' interest in having others take on vendor credentialing responsibilities (DeJohn, 2009). In a natural progression, the earlier providers of vendor credentialing services to health care facilities on a contract basis were security experts (DeJohn, 2009).

The Current Health Care Climate

The current health care climate has become more complex, sensitive and political, resulting in much greater concern for patient protection and reduction of business risks. Among the general contextual factors that shape the current health care climate are the following:

- *Increased privacy and confidentiality concerns.* Organizations are faced with increasing responsibility to ensure privacy and confidentiality of their patients', customers', clients', employees', etc. information, particularly in an electronic environment. Such concerns extend to not only who should access this information, but also whether it should be stored and how portable it should be. In health care, privacy and confidentiality concerns are taken especially seriously and protection of health records is a statutory requirement as per PHIPA (Personal Health Information Protection Act, 2004). While certainly the use of technology and electronic records makes communication about a patient across a health care system much more effective, it also increases concerns about the vulnerability of that information.

- *Increased security concerns.* In society in general, there is a heightened sensitivity toward security concerns. Concerns range from terrorism and bioterrorism concerns, gun control and bullying concerns, protection from theft, identity theft and hacking. In the health care context, security includes alertness to all of the aforementioned threats to ensure patients – their person, possession and files – are protected while in the health care facility.

- *Increased health concerns (and concern for spread of health risks)*. In society in general there is a heightened sensitivity around risks of the spread of infection and communicable diseases; this is likely partly fallout from SARS, exacerbated by the publicity surrounding the pandemic and H1N1. In the health care context, the concerns for spread are especially heightened; this is not only because infections are, obviously, more rampant in a health care facility, but also because of the ease of transmission of infection in such facility and the vulnerability of those in the care of such a facility.

- ➔ *Increased speed of information transmission.* The progression of communications and of internet technology has permitted the transmission of information at extraordinarily high speeds and to far distances. While this can be helpful to businesses (and individuals) in a wide range of ways, it can be difficult for organizations to rein in the chatter in delicate or crisis situations. In short, while good news travels fast, bad news travels faster; this is in part due to a public fascination with and craving for dramatic stories, and the modern approach to news casting, which focuses on breaking news, significant repetition, and live updates to unfolding stories. In today's society, organizational problems can be made public in a matter of seconds. If these problems have victims, and there is a desire to hold someone accountable, speculation, criticism and blame is immediate. Whether merited or not, this speculation, criticism and blame can temporarily if not permanently ruin an organization's reputation.

- ➔ *Increased concern for accountability in the health care environment*. In general, there is an increased effort by organizations to create accountability frameworks in tandem with detailed risk management programs. Accountability frameworks make significant sense in light of Sarbanes-Oxley (to which many organizations subscribe despite that it is an American statute) and increasingly complex business circumstances. In the healthcare environment, there is particular concern for avoiding negative publicity and / or litigation. In the case something goes wrong or challenges arise, defending an organization is more possible when it is possible to demonstrate that steps were taken to foster accountability.

In addition to general trends that affect most organizations, including health care organizations, there is a series of trends that are specific to healthcare; these include:

- ➔ *Increasing complexity of health care systems*. Health care institutions may have several locations, and health care systems (i.e. like LHINs) are becoming more predominant. The result is that there are a number of access points into a system or that certain departments (like purchasing) are not on-site (Herman, 2007). The result is greater concern for controlling access to a health care facility and clarifying and increasing accountability across the system.

- ➔ *Greater control over the healthcare supply chain*. There is increasing interest in avoiding scenarios in which health care practitioners are apt to make unilateral decisions around purchase of equipment, devices or medication due to persuasion, pressure, or favoritism. As part of larger accountability frameworks (discussed in the previous section), managers of health care organizations are increasingly concerned with demonstrating contracting, prescribing and purchasing decisions are made equitably, fairly and in the utmost interest of protecting the organization and its patients. Greater control over the supply chain, for example through vendor credentialing, controls vendor access to health care practitioners by ensuring new equipment and drugs are introduced to health care practitioners through proper channels (i.e. such that it shows up on the radar of the purchasing department) (Herman, 2007).

Health Care Organizations: Duties to Protect

Management of health care institutions and parties funding these institutions (governmental, private donors, etc.) are concerned with: offering (and improving) quality patient care, ensuring patient safety and security, and guarding patients' rights to privacy and confidentiality. Within today's health care context pressure on managers of health care organizations to be concerned with protection of patients, *as well as* the health care institution, is mounting (Garner, 2012).

Protecting the health care institution is partly accomplished through protecting patients (i.e. by providing quality care and by preserving their safety, security, privacy and confidentiality); this, of course, can help a health care institution to avoid litigation, distrust, illness and infection. In essence, one way to protect the health care institution demands that management takes steps to avoid risks to the continuity and reputability of the organization.

Protecting a health care institution extends beyond understanding details about representatives working for vendors to determining which vendors to do business with; this, presumably, will assist in reducing a variety of business risks. Protecting a business requires managers of health care institutions to understand who they are entering into business and partnerships with – what is the quality of products or services provided by a vendor and is the vendor reliable, trustworthy and stable, etc.?

Experiences at Montreal hospitals underline that business risks also involve loss prevention – protection of equipment and assets of a health care facility. Derfel (2011) reports on the robbery of thousands of dollars worth of specialized surgical tools in Montreal hospitals over a six-month period. While it was not certain who was accountable for the thefts, there was fair suggestion it was an 'inside job' made possible by lax standards in and around the hospital and its operating rooms. In particular, several sources claimed a wide variety of individuals could gain access to hospital equipment without having to explain what they needed it for. There was speculation the equipment would be desirable for resale in alternative markets. In another case an American sales representative was caught stealing equipment from the operating room of a hospital; it was found that the equipment stolen was that which he usually sold, and that he had hoped that the hospital would re-purchase the equipment from him (and boost sales) following the robbery (Amstutz, 2012).

Orenstein (2012) reports on another case, in which old x-ray film was stolen from the radiology departments of hospitals in Canada and in the United States, presumably to extract the silver in the film. The case points to the vulnerability of radiology departments to theft of x-ray film as well as to issues associated with the privacy of images themselves and increasing vulnerability of imaging departments to infiltration physically or electronically.

In short, examples highlight the value of health care equipment and supplies to would-be thieves who may or may not have authorized access to the health care organization.

➔ *Patient Protection and Risk Management*

In any organization, risk management involves identifying the reasonable risks that may come to fruition in the course of business. In a typical organization, there are two 'clusters' of risks – a generic cluster consisting of risks faced by most businesses, regardless of industry, and a more specific cluster of risks, particular to an industry, organization, department or team (Ekstein, 2008). Further, organizations will typically be faced by various *categories* of risks, some which are more likely and foreseeable and some which are not. In regards to more anticipatable risks, pre-emptive routines are put in place to minimize the likelihood the risk will come to fruition (Ekstein, 2008).

In the health care context, there are numerous 'foreseeable' risks to quality of patient care, patient safety, security, privacy and confidentiality (Ekstein, 2008). For instance, among more common risks are: likelihood of infection, breaches of security and concern for patient privacy, hand-washing routines, information desks or security checkpoints and record-handling processes. Pre-emptive measures are often complemented by reactive routines for containing or minimizing the impact of a foreseeable risk should it be realized. Such routines include the protocols and the procedures for handling infections, in the case that there is a breach in security, etc. (Ekstein, 2008). As well, at least rudimentary interventions are considered for less standard (but possible) risks so as to at least allow for the initiation of a response (Ekstein, 2008). For example, health care organizations may reasonably be faced with unknown infections for which there is no clear containment or treatment protocol; in these cases, there are loose guidelines or starting points the organization may use to move forward in trying to solve the unstructured problem faced (Ekstein, 2008). Further, in some organizations, particularly within the healthcare setting, an embedded structure may be in place to support responses to more complicated, unstructured, but impactful risks (Ekstein, 2008).

Clearly, a complete risk management program contains both offensive and defensive measures to afford the organization the protection required. And often, the more offensive measures will arise from the experience of less foreseeable events. For example, Grissinger (2012) highlights two cases in which pharmaceutical sales representatives contribute to realization of risks in the health care setting and recommends a general framework for engagement with pharmaceutical representatives that would offset those risks. While the obvious intention of risk management is the prevention of risks (i.e. the offensive facet of risk management), there is also an orientation towards the containment and swift resolution of problems if and when they arise. The ability for an organization to demonstrate due diligence and show measures to minimize and avoid risks were in place is critical for an organization to defend itself.

➔ *Vendor-Associated Risks*

A key question that arises in relationship to vendor credentialing is why vendors are singled out and are subjected to intense scrutiny. Some have likened vendor credentialing to a 'witch hunt' and question why other parties entering a health care facility, like a patients` family, are not subject to the same scrutiny (Douglas, 2011).Vendors perceive that they offer specialized expertise and training that would be otherwise difficult for health care institutions to acquire and that should be valued (Thill, 2007). Furthermore, particularly the representative from medical

devices vendors suggest they have a level of scholarship that equips them to be present in and positive contributors to sensitive environments like the operating room (McGinnity, 2005)

Others maintain, however, that to do their jobs some vendors require significant access to restricted areas of health care facilities, patients or patient records. In the name of patient protection, the contact with restricted areas of a health care facility, patients and patient records at least justifies scrutinizing the credentials of vendors; this, is especially true if a vendor needs specialized knowledge to do his or her job (Garner, 2012) or if a vendor is required to be presenting or training in front of a patient (Cross, 2009). Concerns about vendor representatives being persuasive, if not aggressive, to encourage sales is also a concern. McGinnity (2005) highlights that the boundaries between the informational and sales roles of medical devices sales representatives can be grey, and that this can create conflicts of interest.

A Clinical Alert (2007) prepared by the Maryland Department of Health and Mental Hygiene indicates vendors in the operating room help practitioners to remain current; however, they also create risks to the patients because they are effectively trying to make a sale and risks to the hospital by opening up potential for liability. The alert reports on instances in which the presence of vendor representatives' in the operating room violated a patient, and suggests representatives can neither be assumed to have sufficient specialized scientific or medical knowledge nor be assumed to have adequate in-depth knowledge of the equipment they are selling. To note, the clinical alert does not explain away responsibility of hospital staff such as physicians, nurses to asking the questions that can minimize risks to patients. Ultimately, however, the alert comes out in strong support of vendor credentialing as a method of verifying a vendors' skills and knowledge and of creating accountability in the operating room. DeJohn (2009) echoes that part of the benefit of the credentialing program is to clarify what role a vendor has within the context of the health care facility and particularly the operating room. Ensuring that a vendor does not bring new and unauthorized machinery into the operating room is paramount for avoiding hospital liability in the case something goes wrong.

Another issue that is raised is conflicts of interest that *can* develop as hospital representatives and vendors form relationships. Physicians reported relationships with vendors can keep them current in the knowledge and equipment of their profession (Clinical Alert, 2007). The Clinical Alert (2007) clarified relationships with vendors' representatives would allow doctors to access equipment in operating rooms without having to either purchase it or go through legitimate and formal channels to acquire it. In this sense vendor credentialing offers a health care organization the recourse to address situations in which a vendor is seen to be in the way or overstepping his or her boundaries (DeJohn, 2009). For many of these health care organizations, avoiding conflicts of interest is critical for governance (and compliance with Sarbanes-Oxley), to avoid potential litigation, and to control costs by avoiding unnecessary purchases (McGinnity, 2005).

The University of Ottawa Faculty of Medicine (2011) also has a very specific policy for avoiding conflicts of interest that arise through interactions between physicians and vendor such as pharmaceutical, biotechnology, medical device and hospital and research equipment and supplies industries. AHRMM (2008) specifically focuses on ethical responsibilities of physicians,

particularly when they receive gifts from pharmaceutical representatives; this article also highlights a more general need to attend to conflicts of interest that arise in relationships between physicians and pharmaceutical representatives. Grissinger (2012) highlights that some medical schools and their affiliated hospitals are moving to limit interactions between institutions and pharmaceutical representatives and are putting stricter guidelines in place for managing the relationships with such representatives. The College of Registered Nurses of British Columbia (1996) also highlights guidelines for avoiding conflicts of interest; these include the expected conduct around accepting gifts from suppliers.

In short, it is believed that collecting data on vendors and their representatives is part of the due diligence process for a health care institution. As in any business context, it is routine to gather data in order to make decisions about who to contract or partner with to minimize the potential of organizational harm in the transaction (i.e. bad decisions or charges of unethical behaviours or unfair practices). For a health care facility in particular, given the number of representatives that enter into the institution to do work, and given the proximity to unauthorized areas, patients and patient files, the process of controlling vendor access to a health care facility also helps control risks of vendor (and vendor representative) initiated harm (i.e. infections, breaches of privacy, security and confidentiality, inadequate skills or knowledge).

The Vendor Credentialing Industry Today

➔ *Overview*

The vendor credentialing industry is currently a multi-million dollar industry in the United States, and is showing strong signs of growth in the United States and internationally. Vendor credentialing arises out of health care organizations' administrators' needs to take proactive steps towards protecting patients and protecting the health care organization. In this sense, vendor credentialing is one aspect of a health care organizations' overall risk management plan

In particular, vendor credentialing helps to minimize healthcare organization's exposure to risk by providing decision support to agents of the healthcare organization, particularly around access and contracting decisions. To some "access" is a misnomer, and vendor credentialing is about the creation of an accountability framework (DeJohn, 2009). Regardless, vendor credentialing is ultimately intended to avoid harms that can result from bad partnering decisions and from uncontrolled vendor access to a healthcare organization, its staff and its patients.

➔ *Players*

There are a number of players in the vendor credentialing industry – vendors (and their representatives), health care organizations and vendor credentialing companies (VCCs).

***Vendors*:**

In the health care setting many services are contracted out to third parties – "vendors." Those vendors with which health care institutions typically do business include (but are not limited to) pharmaceutical, medical devices and facilities management, food service providers, engineers and clinical services. These vendors provide service to and on behalf of a health care institution,

and as such effectiveness, reliability and reputation of vendors matters for the quality of service offered by the health care institution.

Employees of vendors, referred to as "representatives" often work in a health care institution, and may do so on a periodic, temporary or full-time basis. While vendors and representatives of vendors are not employees of a health care institution, they often require access (and at times considerable access) to the health care institution to fulfill contracts and to do their jobs.

***Health care organizations*:**
Health care organizations include a wide range of organizational types, such as hospitals, long-term care facilities, group purchasing organizations, IDNs, etc.

***Vendor Credentialing Companies (VCCs)*:**
Vendor credentialing was historically managed in-house by health care organizations' staff. Increasingly, health care organizations are finding it more efficient and cost-effective to hire third-party vendor credentialing companies to provide vendor credentialing services on their behalf. In fact, industry members suggest that a third-party is necessary to 'incent' vendors to provide the information that health-care organizations need to make access and partnering decisions (Repertoire, 2010). It is suggested that by commissioning third-party credentialing companies, processes of and associated with vendor credentialing are streamlined (JHC, 2010).

Vendor credentialing companies have access to databases that are used to collect data on vendors and vendor representatives. First, it involves developing a profile on a vendor; this might involve understanding a business and its owners, its track record, longevity, performance, reputation, quality, etc. Secondly, vendor credentialing involves processes of gathering data on representatives who will require access to a health care institution; this will involve validating a representative's credentials, determining the status of a representative's vaccinations or immunizations, and gathering information on an individual's police or criminal record. Data that comprises a vendor record depends on a number of factors, including the demands of a particular healthcare organization, the jurisdiction of a healthcare organization, government regulations, the requirements of a vendor credentialing company and the demands of particular vendor roles.

In addition to the ability to collate and track vendor and representative data, vendor credentialing companies' make that data available to agents of a health care facility using proprietary, secure information technology solutions. An end user (in this case, an agent of a health care organization) can access the database on the client side, search for and retrieve credentialing data. Ultimately, this data is used as the basis of internal decisions about vendor access and partnering.

➔ *Vendor Credentialing in the Healthcare Industry*

Vendor credentialing services facilitate vendor access to health care organizations and, thus, affect the supply chain and logistics functions, and affect procurement and purchasing functions (Cross, 2009). In other words, vendor credentialing controls vendor access to areas of the organization, employees of the organization and patients within the organization. While some vendors see vendor credentialing as a barrier to access, the intention is to control access in an

effort to protect the patients of a health care organization and the organization itself. Controlling access involves checking to ensure a vendor and / or vendor representatives conforms to a set of standards and requirements; in this vein compliance is a minimum requirement for participating in the health care supply chain.

➔ *Parameters of the Vendor Credentialing Industry*

There are some limits to the definition of the vendor credentialing industry at present. Examples of responsibilities that fall outside of *outside* of the purview of vendor credentialing companies follow:

➔ *Vendor credentialing companies do not determine access*. Vendor credentialing companies provide data to use for and support access decisions. Access decisions are made by agents of a health care organization based on their own judgement and organizational policy.

➔ *Vendor credentialing companies do not determine frequency of credentialing.* The frequency of that data review is determined by the health care organizations and/or by government regulation. Existing standards include the following: worker's compensation is reviewed every 90 days, general insurance liability is updated annually and criminal checks are done once a year. In the United States, criminal checks include sex offender registries, while in Canada the public does not have access to the National Sex Offender Registry. If and when employment involves contact with vulnerable populations the RCMP will conduct a Vulnerable Sector Screening.

➔ *Vendor credentialing companies do not provide risk assessment*. Vendor credentialing companies provide data for a health care organization to use in determining their own risk scores and risk comparisons.

➔ *Vendor credentialing companies have limited responsibility for implementing vendor credentialing*. There are limits to the involvement of a vendor credentialing company in regards to implementation of a vendor credentialing program. That is, while a vendor credentialing company may have responsibility for the program itself and the training that surrounds it, the vendor credentialing company is typically not responsible for managing the internal, organizational cultural, operational and policy changes that surround vendor credentialing.

Benefits of Vendor Credentialing

Certainly, vendor credentialing is not the be all and end all and does not address every risk on the radar of a health care organization. At the same time, it does provide health care institutions with some measure of protection from risks that can be introduced by third parties contracted to work with and for a health care facility. Frequently, vendor credentialing programs request data on vendors that is seen as reasonable not only because of hyper-sensitivity around the health care industry or because of the nature and duties of a health care organization, but rather because of

the risks vendors realistically can present the health care organization and its patients (Barlow, 2009). As Repertoire (2010) underlines, it is only responsible for health care organizations to ensure vendors entering into a facility are free of communicable diseases, are insured and are not criminals. Vendor credentialing represents a step towards protecting patients of a health care institution and an institution itself, but is only one aspect of the health care organization's overall risk management plan. Among the benefits of vendor credentialing are the following:

- ➔ *Addresses privacy and confidentiality concerns.* Vendor credentialing is about providing a healthcare organization with data as a foundation for access and partnering decisions. In this way, healthcare organizations have tools for making more informed decisions about who should be given access to a healthcare facility and who should be awarded contracts.

- ➔ *Addresses some safety concerns.* Vendor credentialing provides data on representatives' criminal and health history. Vendor credentialing helps agents of health care organizations to make access decisions. In particular, the data provided through vendor credentialing can help control who will be allowed into more sensitive areas of a health care facility (DeJohn, 2009; Clinical Alert, 2007). If a vendor is admitted to sensitive areas of a health care organization, such as an operating room, a need to ensure he or she is trained properly, has knowledge of cleanliness and privacy, and will not overstep his boundaries. Vendor credentialing confirms that a representative has accreditation and training that is relevant to work that he or she does and that merits his or her access.

- ➔ *Addresses some security concerns.* Part of the vendor credentialing program involves screening a vendor and its representatives. In regards to a vendor, this might involve collating information on the financials of the business and its track record; this data can be used to inform decision making on the reliability and motives of a vendor. On the representative level, individuals' credentials, accreditations and police records are checked. A vendor representative lacking necessary credentials or with a police record will be flagged in a vendor credentialing system and can be used to inform access decision making by agents of a health care organization.

- ➔ *Increased health concerns (and concern for spread of health risks)*. Vendor representatives are screened to ensure vaccinations and immunizations are up to date. Further, credentialing files will include data on the health status of a particular representative. In the case that there is a particular health concern involving a vendor representative, this will be flagged in a vendor credentialing system and can be used to inform access decision making by agents of a health care organization.

- ➔ *Greater control over the organizational supply chain*. Vendor credentialing offers greater control over a health care organization's supply chain. Particularly given the increasing complexity of health care organizations, partnerships and systems, the ability to quickly determine who should access what areas of a health care organization is valuable (Thill, 2009). By controlling vendors' unsolicited access to practitioners in the health care

organization, vendor credentialing is also said to curtail conflicts of interest. It also provides legitimacy to health care organization staff trying to rein-in overly aggressive vendor representatives (DeJohn, 2009).

Vendor credentialing helps to ensure the most suitable purchases are made by the health care organization (Thill, 2009). Control over the supply chain permits an organization to track purchases made in the organization and protect against untoward behaviour by vendor representatives (see McGinnity, 2005) that can open the organization to various forms of litigation. As well, it can reduce redundancies created by disaggregated purchasing of the same equipment (Repertoire, 2010). Control over the supply chain is critical when it comes to new equipment. While a sales representative from a vendor company may wish to demonstrate a particular machine, doing so 'off-board' and without the knowledge of appropriate departments in the health care facility can create a number of issues. For one, the hospital can be held liable if something goes wrong with the machinery and a patient is harmed or dies (DeJohn, 2009).

Streamlines and reduces costs associated with the request for proposal (RFP) process. If standardized, vendor credentialing can result in cost-savings for the vendors, the health care facilities and the health care system. By being credentialed, vendors have the ability to use that as a selling point to potential clients without needing to incur costs at the time of a bid. For example, a typical check that vendor credentialing includes is monthly Dun and Bradstreet corporate verification. Corporate verification provides health care organizations with a more complete picture of risks and opportunities in their business relationships with vendors. Health care organizations will also save costs associated with reviewing RFPs; this is because credentials, which they have access to, will automatically confer credibility on a vendor, its representatives and on the products and services offered and the representatives.

- *Demonstrates proactive efforts to avoid vendor-related problems*. In the case that problems do arise, a health care organization is in a better position to defend itself if a vendor credentialing system is in place. In particular, agents of an organization will at least be able to demonstrate reasonable pre-emptive steps were taken to screen vendors with whom business partnerships and contracts were created and representatives who were given access to an organization in the case of criticism or litigation. Naturally, a great deal will also come down to internal policies and decision making surrounding contracting relationships and access permission.

- *Updated, arm`s length validation and updating of current credentials*. A health care facility may accept a vendor`s attestation that representatives have had checks, for example criminal checks, at stated intervals (for example, yearly, bi-annually or upon hire). Since certain credentials expire after a period of time and managers of health care facilities want to ensure credentials (including criminal checks) are current there is often a preference for third-party vendor credentialing companies to perform such checks. Not only does this ensure current credentials, but also prevents a `fox guarding the henhouse`

dynamic, in which vendor companies watch over the very representatives who sell on their behalf.

➔ *Rapid communication infrastructure*. The databases that third-party vendor credentialing companies offer health care facilities is a vast improvement on traditional methods used by health care organizations used to manage vendor data. In particular, not only do these companies offer unique data, but they also store, organize and compile the data in order to support decision making. These databases represent an infrastructure to promote the rapid communication of risks. For example, if there is a pandemic communication to the vendors can occur rapidly. Or, if there is a recall notice, vendors can communicate with health care facilities rapidly and directly.

In addition, it is suggested that while there have been concerns raised about the legitimacy and fairness of requests for vendor and representative data, data gathered is not unreasonable given the nature of the health care climate and the duties of a health care organization (Barlow, 2009).

Concerns About Vendor Credentialing

In response to Canadian health care organizations' increasing interest in vendor credentialing, MEDEC (2012) prepared a document outlining considerations for a health care organization to make if they are considering introducing a vendor credentialing program. The document highlights some central critiques of vendor credentialing:

- Requirements and procedures of vendor credentialing can duplicate those already required as part of a vendor / representative's other training / accreditation;
- Demands of vendor credentialing may be unnecessary or excessive given the role or job a vendor / representative is contracted to do and the access required to fulfill that role or do that job;
- Vendor credentialing potentially compromises the privacy of a vendor / representatives;
- Vendors incur costs of vendor credentialing

While vendors may understand the necessity of having some form of credentialing (Thill, 2007), which can protect all, their main objection seems to be to its current form. The following discussion expands on critiques of vendor credentialing programs and summarizes additional critiques of vendor credentialing programs as they appear in the literature.

➔ *Vendor Credentialing is costly for vendors:* In addition to costs of participation noted by MEDEC, vendors report a need to pay for credentialing of each and every representative and for updating credentials over time. In particular, credentialing can create an enormous upfront expense when hiring representatives into a company (Douglas, 2011). Compliance will also result in costs over time, particular for companies with enormous numbers of representatives (Thill, 2007; Repertoire, 2008); this is particularly the case as additional requirements (rather than just updates) are added to credentialing (Douglas, 2011; Repertoire, 2008). In some instances, it is suggested that costs of credentialing are

excessive and constitute a 'cash-grab' by health care facilities and vendor credentialing companies (Barlow, 2009). Ultimately, vendors are rebelling that the costs associated with credentialing create an unnecessary burden on them (DeJohn, 2009).

While larger companies are coming out against vendor credentialing (Thill, 2007), it is smaller companies that have more to lose (Crans, 2010; Repertoire, 2008). Because of their specialized products and services, smaller providers are unsure that they will be able to keep up with costs of credentialing, let alone remaining competitive (Douglas, 2011; Thill, 2007). In some cases, smaller players may have to pick and choose which customers to serve because of the costs involved in participating in the vendor credentialing programs (Crans, 2010). Particularly, this is the case if larger companies can use scale to negotiate for deals on vendor credentialing fees (Burnell, 2008). Furthermore, because different credentialing companies will charge different prices based on different considerations, understanding the nuances of the different products offered by vendor credentialing companies is an additional source of confusion (Douglas, 2011). And ultimately, all of these costs will need to be passed on to the patients (Crans, 2010).

➔ *Vendor credentialing is difficult for vendors to manage*. There are concerns for dollar costs as well as costs of time and effort. At present, there is concern about overlaps between credentialing processes used by vendor credentialing companies and those implemented by vendors in their own businesses (Repertoire, 2008). As well, costs associated with processing and fulfilling the credentialing requests for large companies can be enormous (Thill, 2007). As well, vendors may need to deal with multiple credentialing companies in addition to health care organizations, which can complicate their situation further (Douglas, 2011). And, for some companies, managing credentialing of thousands representatives and hundreds in accordance with the requirements of hundreds of health care facilities through multiple vendor credentialing companies creates an enormous burden (Thill, 2007; Repertoire, 2008; Repertoire, 2010).

In fact, the consistent need to stay abreast of vendor credentialing requirements can be cumbersome for various parties, beyond the vendor. Efforts need to be undertaken by a vendor credentialing company to update vendors and / or vendor representatives about the updates to their credentials that are required (Thill, 2007). While there is a mechanism in place to make sure updates are monitored, tracked and reported, or additional notifications about required updates are given. The burden is on a vendor and / or representative to update credentials. If a representative is not updating his or her credentials, a vendor may need to intervene in the process, which can create a whole variety of issues.

New requirements may be added into a vendor credentialing process; this would require additions to the existing records of vendors' and their representatives' records. Among vendors, there is some concern that new credentialing requirements will be continuously added, effectively raising the hurdle each time it is met by vendors; this can increase

costs for vendors especially in the case that new accreditation or certification is required (Douglas, 2011).

While immunizations work, inconsistent policies and recommendations across provinces, states and jurisdictions as well as the consistent need to update vaccination recommendations can become confusing (Halperin & Pianosi, 2010). For example, suggested and required vaccinations may be announced by governmental departments and agencies, health care institutions, agencies and associations can result in additional vaccination requirements. Some hospitals were so concerned about the spread of H1N1 by vendors that they demanded vendors be vaccinated against H1N1 prior to gaining entry into the hospital (Healthcare Purchasing News, 2010).

Douglas (2011) reports that despite costs associated with vendor credentialing, vendors typically do a fairly poor job of tracking and managing their costs. Others imply that they prefer not to divulge those costs (Rooney, 2008b). It is even suggested that vendors do take a closer look at tracking costs to understand how much the vendor credentialing program is really costing them (Barlow, 2009).

➔ *Vendor credentialing privileges patients' rights over those of vendors and their representatives*. A vendor company will need to justify the right of a health care institution to collect personal information from a vendor. Ultimately, while there is greater likelihood that rights of a patient will be protected by implementing vendor credentialing, this may be done at the risk of protecting a vendor's statutory right to privacy. In particular, collecting private information from a vendor demands that he or she understands why information is being collected and what it will be used for and agrees to provide information for those purposes (MEDEC, 2012). Further, only information that is relevant to the vendor's role can be collected and only for the purpose suggested (MEDEC, 2012).

In some instances, creative means of justifying and getting information about compliance with credentials is becoming a necessity, as vendors cannot force employees to comply (Repertoire, 2009). Imaginably, a representative may legitimately feel he or she must provide personal information beyond his or her comfort level to keep his or her job; this, ultimately, puts a patients' rights to privacy is privileged above the rights of a vendor representative. As suggested in Repertoire (2009), a vendor cannot force an employee to undergo a drug test.

Yet, there are additional concerns about implications of such checks. It is ultimately the responsibility and right of the hospital to determine access based on credentialing. As Douglas (2011) highlights, this unleashes a torrent of questions about whether or not a vendor representative can hope for a career in health care with a criminal record. And, it leads to questions about which criminal records may be 'forgivable' and which will not. As such, it is recognized that there is a greater need for consideration of these checks and how they will be used to determine access in a way that is fair and equitable to all of the

parties involved (Repertoire, 2010). And there are all sorts of concerns that there will be a movement beyond checking credentials to consistently monitoring representatives (Repertoire, 2009). Increasingly, critics of vendor credentialing are questioning where credentialing data is stored and whether it is secure (Repertoire, 2009). The HSCN (2012) white paper specifically recommends that: "all data collected by third party Vendor Credentialing Companies must be stored in Canada by a Canadian based storage company. Further, all VCCs should follow the Canadian Standards Association's Model Code for the Protection of Personal Information, ensure that they are in compliance of PIPEDA (Personal Information Protection and Electronic Documents Act (Canada) and comply with all applicable provincial and federal privacy laws" (p. 2).

➔ *Vendor credentialing is unnecessary for some representatives.* Some vendors suggest participation in vendor credentialing programs is not necessary for all representatives. For some representatives, participating in vendor credentialing represents a waste of resources, such as time and money; in these cases, credentialing is seen as irrelevant and inappropriate to the role and work of some representatives (Rooney, 2008a). One vendor representative suggests not only do detailed requirements for credentialing vary across health care organizations and vendor credentialing organizations, but they are also more realistic for an organizational employee than for a contractor (Repertoire, 2010).

Some vendors are less opposed to credentialing, per se, than how such programs are implemented by health care institutions; in these cases, they believe that credentialing processes should be matched with a vendor's access needs (Rooney, 2008a). In other words, some agreement needs to be created around what credentials are actually needed for what access levels (Thill, 2007). Herman (2007) describes that vendors who require the most credentialing are those that require the greatest access to patients and authorized patient care areas (e.g. operating rooms); these, he suggests, are the most likely vendors to introduced more experimental technology to the organization.

➔ *Vendor credentialing treats vendors and vendor representatives with undue suspicion and undermines their value in the health care industry*. Vendor credentialing can be seen to treat vendors with suspicion. As communicated in the article by Thill (2007), vendors recognize a need for a form of credentialing, but resent how it is being done. Some vendors want validation that they provide services to health care facilities that add value (Thill, 2007; Repertoire, 2009), rather than being treated like an enemy. While there is concern that vendors can instigate conflicts of interest by being able to access health care practitioners directly, it is also worthwhile recognizing controlling access can prevent practitioners from staying current in their fields (Barlow, 2009; Clinical Alert, 2007). In this view, vendors provide practitioners with access to new ideas and technologies which they would otherwise potentially not gain access (Barlow, 2009). And, the medical device sales representatives often have specialized information that is required to operate devices that are specialized and often have a short lifespan (JHC, 2010). In some cases, vendors suggest that the value of their contribution to quality of health care cannot be

assessed adequately by someone in supply chain management, product or purchasing department; this value can only be established on the basis of direct relationships between clinicians and vendors.

Redundancies introduced by vendor credentialing processes are resented as well (Medec, 2011, 2012) from a trust perspective. Vendors report that it is as though the credentialing they do in-house is distrusted and needs to be duplicated on their time and at their cost (Repertoire, 2010). As well, there are redundancies in the credentials themselves. A representative of one vendor company explains, it is redundant to require a vendor's representative to understand proper hand-cleansing techniques and then to delineate a horde of policies around hand-washing (Repertoire, 2010).

In the worst case, some industry representatives suggest vendor credentialing programs can undermine the value of vendors by stifling innovation (Repertoire, 2009). By restricting access to health care practitioners and by increasing costs of access, the ability for such vendors to continuously innovate suffers. Burrell (2008) reports restrictions of access to practitioners can affect clinical trials. Prada (2011) highlights that the Canadian health care system is not doing a fantastic job of ensuring health care innovations are brought into the system; this, it is suggested, might be related to the pressures health care administrators face to invest in innovations that can contribute to quality care and to keep costs low (Prada, 2011).. Adding expensive credentialing requirements for participating vendors can further impede progress towards achieving innovation in health care, by increasing vendors' cost structures.

Aggravating the trust issue is that vendors question why they are required to complete all sorts of requirements staff of a health care institution may not be required to complete (Barlow, 2009; Douglas, 2011). Some vendors also wonder why visitors do not have to be credentialed (Barlow, 2009); this is perhaps indicative of a deeper debate regarding whether vendor representatives are visitors to a health care facility or an agent of that facility? Does the motive of a vendor (to get sales information and leads) affect their role? What about if the vendor provides information – by leaving pamphlets or a poster or offering advice to patients?

Further, vendors are concerned that the data will be used to bar their access to health care facilities and wonder whether it will lead to them being watched all the time (Repertoire, 2009).

Critiques *Related to* Vendor Credentialing

Like most new and developing industries, the vendor credentialing industry is encountering some resistance and growing pains. As well, related industries have had to adopt new mindsets and to find their centre of balance in light of new industry realities and expectations. There are several areas in which these growing pains are being felt in and by health care institutions, as considered below.

➔ *Inconsistent Implementation of Vendor Credentialing.* The implementation of vendor credentialing within health care institutions and regions is a definite area of criticism. There are critiques that while vendor credentialing processes are somewhat consistent across health care institutions, policies related to credentialing are institution-specific (Rooney, 2008a). Procedures a vendor is expected to follow upon arriving at a health care institution may vary considerably (Rooney, 2008a; Thill, 2007). And the actual credentials that are verified may vary from institution to institution, system to system and vendor credentialing company to vendor credentialing company (Hermann, 2007; Repertoire, 2008). As a result, vendors bear the burden of keeping track of, understand and abide by requirements of each and every institution with which they do business; this can be very burdensome when a company has thousands of employees (Thill, 2007; Repertoire, 2008) and lead to confusion (Rooney, 2008a; Thill, 2007). As well, if there are differences not only in procedures, but also in fee structures (Douglas, 2011), this can further aggravate the existing confusion. Some document vendor credentialing is creating inefficiencies that merit a closer look and justify development of a standard (Rooney, 2008b).

The confusion surrounding vendor credentialing moves beyond inconsistent access procedures across the institutions. Also inconsistent across health care organizations are policies surrounding decision making on the basis of vendor credentialing data. As a result, in one institution a vendor representative may not be permitted access whereas in another institution, that same vendor representative will be permitted access (Douglas, 2011). Crans (2010) shares an anecdote. For a meeting on-site at a health care facility, he was required to go through credentialing processes. After the meeting, security told him and his colleagues to throw out their badges. The following morning, only one of the three was contacted to notify him that he had contravened the organization's vendor credentialing protocol.

➔ *Inconsistent Messaging Around Vendor Credentialing.* While not a rampant concern, there seems to be some confusion among vendors about reasons for vendor credentialing. As Burrell (2008) highlights, some health care organizations show interest in vendor credentialing for the purposes of protecting the privacy and confidentiality of patients. Others, it seems, adopt vendor credentialing with the seeming intention of restricting the ability for vendors to access practitioners.

➔ *Education Surrounding Vendor Credentialing.* Related to the implementation of vendor credentialing programs is also the issue of education within the institutions. The process of vendor credentialing is a hurdle that vendors and representatives must jump if they are to be given access permission. Permission, however, does not necessarily equate with access. Although vendors may willingly participate in the vendor credentialing process, there are variations in the acceptance and interpretation of credentials across health care institutions. For example, vendors report that the access permitted by their badges – which are used to indicate a vendors permitted level of access to the health care institution – are understood differently across health care institutions (Rooney, 2008a).

As a result, ensuring employees of the health care organization itself are familiar with credentialing processes is absolutely necessary, particularly given the sizable investment that vendors make into participating in a vendor credentialing program. To date, though vendors follow vendor credentialing guidelines, and in some case wear badges as an indication of their participation in vendor credentialing programs, staff of the health care institutions may not understand what vendor credentialing means, what it entails or what a badge signifies.

➔ *Too Consistent Implementation of Vendor Credentialing.* Ironically, another area of criticism regarding implementation of vendor credentialing is that it is too consistent. In particular, though it is suggested that all vendors and representatives need to be screened in the same way and go through the same processes and procedures, not all vendors and representatives need commensurate access to the facility. In other words, while vendors do not necessarily resist participation in a vendor credentialing process, they feel the process is too invasive given the level of access that they actually require to the institution.

The Future of Vendor Credentialing

Vendor credentialing has the potential to assist health care organizations to minimize exposure to a set of manageable risks. In the same way health care organizations institute protocols and procedures for dealing with spreads of infections or outbreaks, there is no reason why protocols and procedures should not be in place for determining access to a facility and patients and data held within it. In short, it does not make sense for a health care organization to expose patients and managers to risks that are created by the vendors and representatives to which the health care

organization contracts its business. Especially given sensitivity around privacy and security, health care organizations' management have a duty to do what is necessary to protect patients. It also makes sense for health care organizations to avoid harming to patients, uphold ideals of patient protection and minimize the possibility of litigation or protect itself in the case of criticism or litigation.

At the same time, there is significant outcry from vendors about costs incurred by participation in vendor credentialing processes and by the potential invasion of rights presented by such vendor credentialing programs. Further, vendor credentialing creates an enormous barrier for vendors to enter into the industry; this is because of costs that a vendor will incur by getting credentialed. As well, credit checks associated with credentialing on companies that lack a track record will suggest such companies are riskier than they actually are. In effects, costs of credentialing can be quite large, contributing to reduced innovation.

Vendor credentialing is most definitely in an upswing and is projected to grow; however, what it looks like and how it changes over time is obviously unclear at present. It might be suggested that a number of developments around vendor credentialing are likely to occur going forward.

- ➔ *Clarification of roles and responsibilities of the vendor credentialing companies and the health care institutions*. For example, at its essence, vendor credentialing involves information search and assembly more than enforcement. Do vendor credentialing companies provide information reports to the health care institution? Do vendor credentialing companies provide advice or risk assessment of vendors or representatives? Do vendor credentialing companies create policies or advise on the creation of vendor permission policies? What guidelines or standards should a vendor credentialing company recommend?

- ➔ *Greater concern for consistency of vendor credentialing protocols across health care institutions*. At present, confusion among vendors and representatives about vendor credentialing procedures in and across institutions is evident (Rooney, 2008a; Thill, 2007). Terminology referring to the various types of vendors may be different across organizations and may need to be agreed upon (Repertoire, 2009). For example, in discussions around creating standards, there was need to agree on what a `clinical rep` meant and what type of insurance such a representative would be required to carry (Repertoire, 2009). Affiliated health care institutions may not enforce protocols consistently. Even in an organization, protocols may be enforced differently at different times (Rooney, 2008a; Thill, 2007). In this vein, further coordination and standardization across the facilities within a healthcare system will increasingly be required (see Repertoire, 2010) and will likely need to be the responsibility of a health care organization. Training internally will also help to increase other organizational employees' awareness of and comfort with vendor credentialing programs and procedures (see Repertoire, 2010). If requirements are dramatically different across health care institutions, this is an additional source of confusion and consternation. The question that arises is who should be responsible for making sure that there is consistency

and/or how to make it easier for vendors and their representatives in the case that there is inconsistency? Efforts are underway to increase consistency in vendor credentialing requirements across institutions in the form of a 'passport' (Repertoire, 2008) which will presumably contain a range of information that is required commonly across most, if not all, health care organizations. Presumably, over time a body will be created to regulate the vendor credentialing industry.

- *Creation of levels of access permissions*. The question of whether access should be standardized across all vendors and their representatives or whether there should be gradations depending on the required level of access will need to be considered sooner or later (DeJohn, 2009). Vendors are not necessarily rebelling against the concept of vendor credentialing in its entirety, but to some degree vendors who do not need carte blanche are asking why they need to participate in a full-fledged vendor credentialing processes if it is not commensurate with their required level of access and/or is not necessary given their job and role. As noted several times in this paper, there seems to be particular concern around medical device sales representatives who not only have access to operating rooms, but who also stand alongside surgeons as they perform surgeries (even demonstrating equipment) and pharmaceutical sales representatives who influence prescription decisions. At present, it appears that the Joint Commission guidelines seem to be best for all vendors as they require proof of product training, patient privacy, criminal background checks and vaccinations.

- *Exceptions*. While there is a definite push towards standardization and simplification of vendor credentialing requirements and implementation, there is also a need to ensure wiggle room to deal with exceptions and emergencies that might arise. JHC (2010) highlights a case in which a surgeon is using a device with which he or she is unfamiliar in a middle of the night surgery. The question is whether that surgeon should be able to call on an uncredentialed vendors` representative (from whom he or she likely got the device? Or, should vendor credentialing be a minimum requirement? Is it enough to credential the company and not the representative? As Medical Device Licenses are given by Health Canada to ensure safe devices are imported into the market, many players in the health care industry would submit that there should be more rigorous efforts to ensure that vendor representatives are also safe.

- *Development of credentialing standards*. While development of credentialing standards is probably at least somewhat related to the previous three points, it is also a separate point. At present, there a number of moves intended to create standards across industry though questions persist about who will be involved in and / or spearhead such initiatives (DeJohn, 2009). There is commitment from MEDEC to support creation of such standards (MEDEC, 2011) as well as a whole range of other Canadian and American agencies and associations, including the Canadian Healthcare Supply Chain Network (HSCN). In fact, in September 2012, the HSCN revealed their recommended standards, which varied from those of the Ontario Hospital Association.

At the same time, the efforts remain fragmented. Some industry representatives suggest that while it is likely that there will be differences in credentialing needs across parties in the industry, there are also areas for standardization that need more exploration (Repertoire, 2010). Rooney (2008), for example, suggests that efforts are underway to gather the costs associated with credentialing to move toward the development of vendor credentialing standards. To some, it is not only about creating standards, but also about ensuring there is collaboration and common understanding of expectations of a vendor's behaviour and perhaps some guidelines for them to abide by (DeJohn, 2009). Repertoire (2009) notes various organizations, agencies and industry associations are interested in understanding issues around vendor credentialing and participating in the development of credentialing standards; these organizations appear to be borrowing ideas from each other in the development of guidelines and standards.

➔ *Developing trusting partnerships with vendors*. While there is an adjustment period when new standards and requirements are introduced into the industry, there is also significant room for animosity and anger. As shown, there are a number of reasons why vendor credentialing makes sense in the context of health care organizations, particularly within the current health care climate. Yet, in the case of vendor credentialing, vendors may feel distrusted by health care institutions, and this is a relationship that should be managed. In addition to feeling that they are being scrutinized (Repertoire, 2009), vendors also feel distrusted because vendor credentialing processes overlap with and / or duplicate their own efforts (Cross, 2009). In many instances, vendors feel singled out, and wonder why hospital employees and visitors do not have to go through the same procedures that they do (Thill, 2007; Barlow, 2009). Future efforts will need to be placed on determining an appropriate division of labour between vendor credentialing companies and vendors to avoid duplication of efforts. As well, efforts will have to be made to ensure the suspicion with which vendors are treated is minimized. Also, consideration might be given to how the parties can work together to create standards or guidelines that are meaningful, useful and not overly ambitious, invasive or unnecessary (DeJohn, 2009).

In the articles about vendor credentialing, there is a visible pattern – the loudest voices are coming against vendor credentialing are medical devices vendors. On one hand, as noted throughout this discussion paper, medical devices vendors offer various benefits to health care organizations and health care in general; they provide practitioners with access to current technology, helping to keep them up to date, they contribute to overall innovation in the health care industry, they have specialized knowledge and training that permits them to assist in critical care environments, they contribute overall to the quality of patient care. However, there are also risks associated with medical devices vendors in particular; their purpose is to sell product and their access puts them in a position to breach all duties of a health care organization (safety, security, privacy, etc.).

Ultimately, developing collaborative relationships with vendors is essential for both health care facilities as well as the vendors (Thill, 2009). Health care organizations also may take a more active role in monitoring the credentials of vendors and helping them negotiate the vendor credentialing requirements (see Repertoire, 2010).

- *Credentials a minimum requirement for industry participation*. The introduction of standards in an industry has a fairly predictable trajectory. Over time, the standards themselves become a key expectation of doing business within the industry; it acts as an admission ticket. In effect, it may be that vendors are wary of vendor credentialing, and clearly details need to be ironed out among all industry players, but participation in vendor credentialing programs will be necessary for those vendors interested in continuing to do business with health care institutions.

- *Industry exit by players with shallower pockets and less supplier power*. There is no doubt there is need for extensive negotiation across vendor credentialing companies, health care institutions and vendors about the areas that are perceived as particularly challenging or limiting for vendors. At the same time, it is likely companies who cannot afford demands of vendor credentialing will leave the industry. The concern will come to companies that provide specialized services to the health care industry. Thill (2007) describes the smaller players are fearful of costs associated with vendor credentialing. However, it is precisely these parties that have the power to negotiate more suitable vendor credentialing requirements.

- *Changes in selection and hiring procedures among vendors*. Given the costs associated with the process of credentialing, it is likely having and maintaining credentials will become a condition of employment and will become the responsibility of employees. Representatives will, effectively, become personally responsible for costs associated with vendor credentialing. As well, this can create shortages of skilled professionals in the market. By putting control for the process of credentialing in the representatives` court, this also alleviates some privacy concerns for the vendor companies

- *Streamlining processes for updating vendor credentials*. Presumably, over time there will be a need to manage updates to vendor credentials in a more streamlined process. There are two ways in which credentials will need updating. First, there will need to be updates to certifications and memberships, vaccinations and inoculations. In order to make these updates, action must be taken on the part of a vendor or vendor representatives. Thus, a notification and tracking system will be necessary, as will a reminder system. Further, recognizing the limits of responsibility for a vendor and vendor representative will be necessary. In the case that it is required, issues surrounding who pays for credential upgrading may be necessary.

  Second, there will need to be responses to new requirements for credentialing. Similar efforts manage and track responsiveness to new vaccination and immunization, tests and

certification requirements will be necessary as they come down the pipeline. As Healthcare Purchasing News (2010) reported, vendors were suddenly faced with the need to take proper precautions to gain access to the hospitals they worked for as H1N1 arose.

For some vendor firms, this may require the hiring of an additional staff member to deal with the credentialing requests. As a reported in Repertoire (2010) one firm was finding that the onslaught of e-mails being sent to representatives from credentialing companies was being ignored, and that subsequently representatives were not being given access to health care organizations. As a result, a staff member was hired to deal with the credentialing requests.

➔ *Concerns about privacy*. It is expected vendors will continue to rebel against strict requirements of vendor credentialing and to do so, will raise additional concerns about privacy and storage of their data. As a result, vendor credentialing companies will need to pay much more concern to the security and training around their databases. If health care organizations are investing in vendor credentialing as a method of reducing risk, they will also need reassurance that their risk is being protected on all sides.

➔ *Technological concerns*. Going forward, vendor credentialing systems are going to have to be interoperable and easy to use. Web-based systems are likelier to be appreciated because it will reduce the potential for technological glitches that come with system upgrades. Ease of use will be increasingly important as health care organizations' personnel deal with multiple vendor credentialing companies and don't have the patience to learn multiple systems. Going forward, it is also the technology that creates the temporary competitive edge credentialing companies will depend upon.

Going forward it will be increasingly important for vendors and vendor representatives to also be able to share their credentials if and when it is required. As such, if a vendor deals with a health care organization that does not have a vendor credentialing system, the vendor might forward their credentials to that organization. By so doing, the primary vendor credentialing company is essentially attesting to the records that are being submitted by the vendor to other health care organizations to vendor credentialing companies. The result is greater sharing of records across vendor credentialing companies which not only will foster greater consistency in the records of all credentialing companies and health care organizations, but which will also reduce the costs of verification and make vendor credentialing processes it far more seamless for vendors.

➔ *Sidestepping vendor credentialing processes*. There are questions of whether or not the vendor credentialing programs will effectively deter vendors' representatives from finding other ways to get to the physicians who they hope to sell to and influence. As Crans (2010) highlights, there is nothing preventing vendor's representative from meeting a physician outside of the hospital setting. Of course, another question in this

vein is how much vendors can rebel against the vendor credentialing requirements. It is possible that over time, vendors will seek to take control over the vendor credentialing process to avoid the inherent duplication of effort and costs. Thus, rather than allowing the health care organization to control credentialing, vendors can take control of the processes in a way that would be deemed legitimate by all parties. Finally, of course, there is a good potential for vendors to lobby against these vendor credentialing demands.

A central issue that presents itself is related to the power dynamics of vendors versus the health care organizations that they want to access. If vendors were to take control over their own credentialing, it is likely that over time corners will be cut to save costs. Also, leaving vendors with responsibility to credential themselves and those who work for them represents a conflict of interest. It may be that the situation will come full circle, with the health care organizations coming to distrust the self-credentialing process of vendors, causing them to look for alternatives with more stringent measures. What is also possible, however, is that inequities may be created. Vendors may eventually chose when to get credentialed, and following the 80-20 rule, will be likelier to get credentialed for higher yield contracts. As a result, smaller facilities will lose out as vendors defect when faced with the prospect of rigorous credentialing requirements.

➔ *Evidencing positive impacts of vendor credentialing*. There is no doubt that vendor credentialing offers a foundation for health care organizations to prevent and minimize certain categories of risks (when used in conjunction with internal guiding policies). Yet, the data to demonstrate these effects and the conditions that foster them is hard to come by. To be clear, a fear of negative publicity or worse creates a shroud of silence around the vendor-related risks health care organizations face and have faced; this makes it difficult for the vendor credentialing companies to access comparative data before and after adopting vendor credentialing programs and standards which could allow them to establish applications of vendor credentialing data that contributed to (or detracted from) successful risk avoidance, mitigation or management.

➔ *Vendor credentialing is limited*. Vendor credentialing has been targeted by critics, but a vendor credentialing company is not accountable for decision making by organizations that use their services. Rather, vendor credentialing companies provide data to support the decision making of other organizations' decision making as based on internally created or adopted guidelines. Going forward, vendor credentialing companies will need to pay greater attention to delineating the limits of their responsibility and accountability for healthcare decision making. For instance, if a vendor's representative is given access to an organization in spite of having a positive TB test as per the vendor credentialing company's profile, this is not a problem that can be blamed on a vendor credentialing company. In the case a mistake is made in a vendor credentialing profile a different story might come to the fore.

Opportunities Surrounding Vendor Credentialing

Based on the overview of the vendor credentialing industry provided, a range of opportunities can be identified.

- ➔ *Vendor credentialing literacy consulting* – despite claims about the inconsistencies across vendor credentialing requirements, standardization is not likely to occur any time soon. In fact, the likelier scenario is that only certain vendor requirements will be standardizable across institutions, while others will be customizable. As well, if more access levels are added to the vendor credentialing process, this is apt to cause even more confusion in a vendor company. It is likely vendors will need help interpreting and administering all of the credentialing requirements on an employee by employee, facility by facility, VCC by VCC basis. An opportunity is, therefore, presented to consult to these vendors. Or, as an alternative, there is an opportunity to train internal employees, on behalf of vendors, to manage the vendor credentialing requirements for the vendor.

- ➔ *Delineating vendor-managed credentialing*. Going forward, it is likely that agreements will be made about the aspects of vendor credentialing that vendors can manage on their own versus those that will need to be managed by a third-party. Part of the issue in terms of vendor credentialing appears to be that vendors resent having rules pushed down their throats that treat them with suspicion, cost them money, increase their workload and prevent them from doing their jobs. To remain conciliatory with these vendor companies, it will be increasingly necessary for some agreement to be found and some autonomy to be given back to the vendors.

- ➔ *Decision support and risk management*. As noted, access and partnering decisions are made on the health care organization level. While health care organizations have a wide variety of expertise about risk, they may need additional support to make access decisions and assess risks. In particular, there may be some room to assist representatives of health care institutions in comparing vendors' risk profiles.

- ➔ *Providing credentialing pre-training as a condition of future employment*. As the costs of credentialing increase and present a burden to vendors, it is expected vendors will start to demand that their representatives receive certain credentials as a condition of being hired. As a result, vendors will not have to pay for credentialing beyond any specific credentials required by their specific workplace. Alternatively, vendors may wash their hands of credentialing and make it a requirement for representatives to independently manage as a minimum requirement for employment in an industry. Further, as would be the case with other health care practitioners (namely physicians), recruiters would be likelier to not only look at a vendor representative's competencies (i.e. experience), but also their eligibility (i.e. their credentials).

➔ *Shared service organization management of vendor access*. Increasingly, health care organizations are making use of centralized procurement options. Typically, these centralized procurement organizations will facilitate bulk purchasing of all sorts of hospital equipment and supplies on behalf of a collective of hospitals. Looking into the future, it is viable for such shared service organizations to procure vendor credentialing on behalf of member health care organizations; this would facilitate consistency and standardization across the member health care organizations, streamline vendor credentialing processes considerably.

If shared service organizations are to procure vendor credentialing on behalf of the member health care facilities, this would reinforce previously made points about vendor credentialing being an expectation, minimum requirement and admission ticket for participating in the health care industry. As well, it is anticipated that the centralization will also result in sharing of information about application of vendor credentialing that will lead to greater consistency in policies and procedures around vendor and vendor representatives' access. Ultimately, these effects will help move the industry forward and will result in greater differentiation across vendor credentialing companies and the products and services they offer.

➔ *Movement beyond healthcare*. Justifications for vendor credentialing within the health care industry are very strong, but risk management is increasingly important for all types of businesses. Over time, vendor credentialing will move to other industries with similar structures and concerns and in which contracted and sub-contracted employees are able to access customers or clients in a way that could compromise their safety, security and health. As well, it is expected that vendor credentialing will also be extended to other professionals, such as physicians, who work within the health care organizations presently.

Conclusion

All in all, vendor credentialing is a promising industry, and its progress and development will be very interesting to watch. While vendor credentialing makes sense, helps cushion health care organizations from risks, and therefore seems to be a necessity for health care organizations that are trying to protect their patients and their organizations, it is proving to be the topic of active political debate and to be disturbing to the health care supply chain. Currently, concern around vendor credentialing is especially communicated by vendors and vendor representatives, who are worried about costs of participation in terms of money and time and implications for their access to health care facilities and health care practitioners.

Over the next few years it is likely that a considerable amount will change in regards to vendor credentialing, as competition among vendor credentialing companies increases, as new third-party providers enter the market, as work towards development of credentialing standards accelerates and as organizations get more and more into the groove of administering vendor

credentialing programs. Further, it is expected that over time, businesses and industries will grow out of vendor credentialing and that vendor credentialing companies will need to expand and differentiate their services and the industries they serve as part of their market positioning.

Despite debates surrounding vendor credentialing, it is becoming an essential aspect of the health care supply chain. The urgency that managers of health care organizations feel to take proactive measures to avoid threats to their patients and their institutions strengthens the rationale for including vendor credentialing within the larger risk management program of health care organizations. In short, vendor credentialing is undoubtedly here to stay in some form.

References:

AHRMM (Association for Healthcare Resource and Materials Management) (2008). Issues & legislative committee reports. Available: http://www.ahrmm.org/ahrmm/news_and_issues/issues_and_initiatives/issues_legislative_committee_reports/archives/02_14_08_report.jsp. Accessed: November 2, 2012.

Amstutz, L. (2012, June 11). Munson catches sales rep stealing from operating rooms. Available: http://www.upnorthlive.com/news/story.aspx?id=764425#.UJFy89ewWSp. Accessed: October 1, 2012.

Barlow, R.D. (2009). Checks for balance: vendor credentialing efforts strive to thwart red ink, red tape, risk exposure. Available: http://www.hpnonline.com/inside/2009-02/PS-VendorCred.html. Accessed: July 20, 2012.

Burnell, S. (2008). Industry pushes for standardization of vendor credentialing. Available: http://www.mddionline.com/article/industry-pushes-standardization-vendor-credentialing. Accessed: July 20, 2012.

Clinical Alert (2007). An unnecessary distraction: Vendors in the operating room. Clinical Alert, 4(3),

College of Registered Nurses of British Columbia (2006). Practice standard for registered nurses and nurse practitioners: Conflict of interest. Available: www.crnbc.ca, Pub. No. 439.

Crans, F. (2010). Vendor credentialing: What the dog saw...Available: http://www.repertoiremag.com/Article.asp?Id=3408. Accessed: July 20, 2012.

Cross, D. (2009). Vendor credentialing – GPO perspective. GPS Newsletter. Available: http://www.nci-cg.com/blog/post/Vendor-Credentialing-GPO-Perspective-Dee-Ann-Cross.aspx. Accessed: October 1, 2012.

DeJohn, P. (2009). Rules for O.R. reps. Available: http://www.hhnmag.com/hhnmag_app/jsp/articledisplay.jsp?dcrpath=MATMANMAG/Article/data/09SEP2009/0909MMH_Coverstory&domain=MATMANMAG. Accessed: July 20, 2012.

Derfel, A. (2011, May 26). Surgical tools stolen from Montreal hospitals. Gazette. Available: http://www.montrealgazette.com/Surgical+tools+stolen+from+Montreal+hospitals/4839949/story.html. Accessed: July 20, 2012.

Douglas, K. R. (2011, May 16). Limited access. Available: http://www.labx.com/article.cfm?articleId=2245. Accessed: July 20, 2012.

Ekstein, K. (2008). Organizational responsiveness as a strategic core competence in dynamic and complex environments: An exploratory developmental framework. (Doctoral dissertation). AMICUS No. 34645519

Garner, G. (2012). Top 5 reasons for vendor credentialing. Available: http://ezinearticles.com/?Top-5-Reasons-for-Vendor-Credentialing&id=7058449. Accessed: 20/07/2012.

Grissinger, M. (2012). Managing visits from pharmaceutical sales representatives. *P T. 37(5)*, 261, 263.

Halperin, S.A. and Pianosi, K. (2010). Immunization in Canada: a 6-year update. *Journal of the Canadian Chiropractic Association*, *54(2)*, 85-91.

Healthcare Purchasing News (2010). H1N1 fears offer vendor access hurdle. Available: http://www.readperiodicals.com/201002/1966442051.html. Accessed: July 20, 2012.

Herman, D. (2007). Vendor representative credentialing: The growing challenge. Journal of Healthcare Contracting. Available: http://www.hpnonline.com/inside/2007-10/0710-cbs.html. Accessed: July 31, 2012.

Jaeger, J. (2011, January 25). Survey: companies unhappy with vendor risk assessments. Compliance Week. Available: http://www.complianceweek.com/pages/login.aspx?returl=/survey-companies-unhappy-with-vendor-risk-assessments/article/194663/&pagetypeid=28&articleid=194663&accesslevel=2&expireddays=0&accessAndPrice=0. Accessed: July 20, 2012.

JHC (2010). Vendor credentialing still an issue. Available: http://www.jhconline.com/vendor-credentialing-still-an-issue.html. Accessed: July 20, 2012.

McGinnity, E. (2005). Sales versus scholarship in medical device procurement. Healthcare purchasing news. Available: http://www.hpnonline.com/inside/August%2005/0508ClinicalBusiness.html. Accessed: August 2, 2012.

MEDEC (2011). Medical technology industry representative credentialing. Available: http://www.medec.org/webfm_send/1362. Accessed: July 20, 2012.

MEDEC (2012). Hospital vendor access control. Available: http://www.medec.org/webfm_send/1818. Accessed: July 20, 2012.

Repertoire (2008). Boiling point. Available: http://www.repertoiremag.com/Article.asp?Id=2847. Accessed: July 20, 2012.

Orenstein, B. (2012). Securing films and files – privacy protection and x-rays. Radiology Today, 13(7), 20.

Prada, G. (2011). Innovation procurement in health care: A compelling opportunity for Canada. The Conference Board of Canada: Ottawa.

PRlog (2010). Medical vendor credentialing takes a turn for the better. Available: http://www.prlog.org/11178945-medical-vendor-credentialing-takes-turn-for-the-better.html. Accessed: July 20, 2012.

Repertoire (2009). All together now. Available: http://www.repertoiremag.com/Article.asp?Id=3148. Accessed: July 20, 2012.

Repertoire (2010). Vendor credentialing still a thorny issue. Available: http://www.repertoiremag.com/Article.asp?Id=3612. Accessed: July 20, 2012.

Rooney, C. (2008a). A fight's brewing over vendor credentialing. Available: http://www.hisci-net.org/Portals/0/Press%20Room/CurtisRooney-JHC-MarApr08.pdf. Accessed: July 20, 2012.

Rooney, C. (2008b). Mandate for change. *The Journal for Healthcare Contracting*, November / December, 8.

Thill, M. (2007). Observation deck: The vendor credentialing mess. *Journal of Healthcare Contracting*. Available: http://www.jhconline.com/observation-deck-the-vendor-credentialing-mess.html. Accessed: July 31, 2012.

Thill, L. (2009). Best in class. Available: http://www.repertoiremag.com/Article.asp?Id=3224. Accessed: July 20, 2012.

University of Ottawa Faculty of Medicine (2011). University of Ottawa Faculty of Medicine policy. Available: http://med.uottawa.ca/assets/documents/policies_procedures/Policy_Interacting_Industry_Septembre2008.pdf. Accessed: July 31, 2012.