



---

5204 Fairmount Avenue, Suite 208, Downers Grove, IL 60515 • 866-IMDA-YES (463-2937) • Fax: 630-493-0798

## Recommended Credential Verification Organization (CVO) Attributes

After a thorough review of numerous CVO business practices and their attributes, and with the objective of creating a document that will assist stakeholders in understanding a rapidly changing and expanding CVO marketplace, the following criteria and rationales are offered for consideration when contracting with a CVO for Health Care Industry Representatives (HCIR) credentialing purposes.

### Universal Membership

IMDA has investigated several business models in the marketplace. The universal membership model, defined as a single annual fee good for all installations of the same branded service solution, whereby an HCIR's membership grants it access to unlimited hospitals for one fee, is by far the preferred model.

We have concluded that a price per hospital per vendor business model per year would cost healthcare as an industry **over \$1.7 billion annually**. This specific model is extremely dangerous to the very existence of an independent manufacturer because many sales organizations have reps that cover a vast geography with multiple hospitals. If they must pay a new fee each time they enter into a hospital that simply is not feasible and participation is not possible.

### Dedicated field sales and service organization

Due to the type of information being collected, a credentialing company has access to significant data beyond just credentials. This data also includes sales activity of vendors including who they visit and what is being discussed. There are documented cases where the sales force of some of the third party credentialing services employ independent reps that also sell competing products to other vendors that they credential, giving them access to private sales activity data that would give them an unfair competitive advantage.

### Neutral stance on recommended credentials

We do not believe the third party credentialing company has the authority to, or should, dictate the hospitals' credential requirements. It should be the sole responsibility of the hospitals to select their own requirements to avoid any conflict of interest.

### Minimum of SAS70 LEVEL II Data Security process and procedures

It has become apparent that all third party companies do some sort of data encryption but we feel that this is inadequate when considering the nature of the information being stored by the CVO. We believe that at a minimum any service provider in this space should offer [SAS70 LEVEL II](#) or its equivalent around its database and servers. (see Figure 1)



## **Separation of and distinction between 'credentialing' and 'hospital due diligence'**

Some third party credentialing services are charging HCIRs fees so that they can perform financial, legal, and other "due diligence" research on their employers. This is unacceptable because:

- there should be no fee charged for free, public information
- GPOs are already completing this function for their member hospitals
- the value of this service lies solely with the hospital--it should pay for these services.
- Compliant vendors are forced to pay a fee that could ultimately lead them to being banned from the hospital due to subjective interpretations of their data.

## **Zero tolerance of Anti-Kick Back infractions**

Payment of fees to a third party vendor credentialing company that directly or indirectly results in any form of revenue share with the hospitals is questionable and may be violative of the anti-kick back statutes. As such, and at a minimum, a signed affidavit should be available to all from the company website and updated at least annually restating its commitment to anti-kickback statutes. From our perspective, this insures that the fees collected are for the sole purpose to administer the credentialing service, and do not reflect an "access fee".

## **No fees associated with general access to a hospital, or its orientation materials**

It is never appropriate to charge the HCIR for receipt of required documents on orientation, hospital procedures, etc. published by the hospital.

IMDA members feel that should the hospital desire to request their vendors to comply with the content in these materials, the distribution and administration of such material should be at the sole cost (if any) to the hospital.

## **National footprint with GPO endorsements**

IMDA believes that the best way to keep costs to a minimum is by engaging CVOs with GPO support and/or national installation capability. This will enable our members to amortize the annual cost of the membership over the largest number of possibilities.

## **Strict Privacy Policy**

IMDA categorically refuses to support any credentialing company that collects or requests Social Security Numbers or Drivers License numbers for any reason whatsoever. Background check attestations from the HCIR's employer should serve as ample proof that HCIR is free of criminal background. In addition, the credentialing company should have a clearly defined privacy policy to address the misuse or potential sale of information it collects for itself or on behalf of its clients.

## **Financial security and resources to ensure a continued level of service over the long term**

New entrants are populating the CVO landscape at an alarming rate. The challenge that these new entrants present pertains to the data collected while they are in operation and what becomes of this data when they choose/have to exit the business. IMDA is very uncomfortable with the additional and unbalanced risk that its members are exposed to when a financially unstable company cannot continue ongoing business operations.



As such, we strongly prefer to see a minimum of three years in business in the healthcare industry with the opportunity to review the CVO's financial health upon request. Preferably, the financials will be audited by

independent third parties and certified to meet generally accepted accounting standards, as well as to ensure anti-kickback adherence.

**Recognition that the HCIR is the customer and should be treated accordingly**

In our experience, the interests of patients are not advanced by the types of credentialing policies and methodologies that request Personal HCIR Identification Information, including social security, driver's license, passport numbers, job performance reviews, credit checks and resumes. This is an inefficient and ineffective way to protect patient safety and it unnecessarily invades the privacy of HCIRs.

**IMDA is a non-profit organization and has received no financial incentive to author this open letter to those involved in health care.**

**While this document represents a consensus of IMDA members, each member is free to approach all matters involved in vendor credentialing as it feels appropriate.**