



CRITICAL FACTORS IN DIFFERENTIATING HOTLINE SERVICES

By Richard Kusserow, former DHHS Inspector General

HOTLINE CLIENTS SHOULD BE HELD BY SERVICE, NOT CONTRACT. Look at vendor contracts carefully. There are many tricks to “lock in” clients. Beware if a vendor insists on annual contracts where it cannot be easily terminated and/or termination procedures are complicated. Those vendors that “lock in” their clients with contracts and not by good services should be suspect. Insist on being able to cancel a contract at any time *without* cause with simple written notice. If the service is good, there should be no concern in granting this request. Similarly, if there is a client specific number used in the service, ensure that the number can be kept by your organization, should there be a termination of service for any reason. It is a common trick by vendors to get a client to publicize a toll free number they own, so that to cancel the contract would create a host of problems with changing to another number.

Best Practice Tip. If you want to use a phone number exclusively for your hotline, obtain your own number and forward it to your hotline vendor. In that way you will never have to be concerned about who controls the number.

ALWAYS INSIST ON A SINGLE ACCOUNT REPRESENTATIVE. Once a vendor is selected, it is important that optimum service follows. That means, there should be a single point of contact with the vendor for any and all issues, whether related to the quality of the reports, changes in protocols, or an invoice. It should not be the client that has to chase down the “right” party to get the right action. This will also have the effect of creating greater accountability on the part of the vendor.

Best Practice Tip. Include in the contract terms, designation of a single point of contact for all issues related to the service agreement.

VERIFY YOUR INFORMATION WILL BE SECURE USING LATEST FIREWALL TECHNOLOGY. The Internet was not originally designed for open access by the general public. However, the popularity and acceptance of the Internet as a means of communication is creating the demand for more and more companies to make information available from internal computer systems. For example, your company may wish to have their hotline information via the Internet, but does not want to compromise their security. It is critical that the vendor installs and maintain a security firewall on their computer network. The hotline vendor should have a professional firewall that authenticates every request for information, and provide only the information that person is authorized to have while documenting every event.

Best Practice Tip. Ask for evidence of firewall protection (for files and systems). Verify they have annual independent operational audits.

CALL INTAKE CAPACITY SHOULD ENSURE NO QUEUING OF CALLS. A caller should never get a busy signal or wait for more than five rings before a live operator answers the call. It is extremely important that your vendor has no abandonment rate due to calls going into a queue. Callers should not hang up because of wait times. Vendors should be able to provide an answering standard as to the maximum number of rings before any call will be answered.

Best Practice Tip. Have your vendor warrant in writing that no caller will have to wait more than five rings or be placed in a queue.

ENSURE VENDORS HAVE ADEQUATE SECURITY CONTROLS IN PLACE. Vendors should maintain data on servers in-house with backup and recovery data offsite. The vendor should be able to evidence a system of internal controls that ensure segregation of duties and functions. All database information should be located on a secure server that utilizes the latest in firewall technology to protect confidential client information in a private network environment. Access outside of the network should not be permitted unless all systems on the network have the most up-to-date virus definitions to protect against viruses. Employees should have access to the database through password-protected application programs located on individual workstations that are networked with the server. For security and privacy reasons, all callers should be assigned a confidential case number and a unique digit code for subsequent access to the case file. Callers should be required to provide these in order to be granted access to the record.

Best Practice Tip. Vendors should evidence a compliance audit by an outside expert to verify all the policies, procedures, protocols, and controls are being followed.