INTERNAL CONTROL SELF ASSESSMENT
IT Controls

Yes	No		
		1.	Is there a written policy or set of standards defining what the practice considers unacceptable or unauthorized use of networks, applications, hardware & software?
		2.	Is access to computer systems restricted so users have access only to those elements necessary to complete their work?
		3.	Are passwords required to be changed at least quarterly in accordance with a written policy?
		4.	Are passwords required to be at least 8 characters consisting of letters, numbers and other characters? Are employees required to maintain confidentiality of their passwords?
		5.	Are confidentiality and PCI compliance standards adhered to for all credit card information?
		6.	Are network servers and other communications hardware physically secure (in a locked room) with access restricted only to those who require it.
		7.	Are system administrator passwords restricted to one or two individuals not involved in the accounting process? Does a board member or owner have access to them (e.g., in a sealed, signed envelope) in the event the custodian(s) of the password are terminated or otherwise unavailable in an emergency?
		8.	Is intrusion detection hardware and software in place for network and communication resources?
		9.	Are exception reports and violation reports/logs reviewed regularly by appropriate personnel?
		10.	Does the practice have a back up policy that includes off site storage of backups? Is the back up restore process tested periodically?