ABC's of Protecting Confidential Information

All entities are at risk of security and privacy breaches.

Banking information changes for electronic transfers should never be taken over the phone.

Continuously audit the enforcement of your policies and procedures.

Dumpsters should be stored in a secure area to avoid "dumpster diving" for sensitive information.

Exterior doors should never be propped open. Keep them closed to keep intruders out.

Firewalls on computer systems should be installed and enabled.

Guidelines should be developed regarding the types of documents that must be shredded.

Have all employees log off or shutdown their computers at the end of the day.

Instruct employees to lock their computers when away from their desks.

Jotting down passwords and leaving them in open view is not a good idea.

Keep current on privacy and security risks.

Let your employees know what type of information is sensitive and confidential and what must be safeguarded.

Make sure all employees understand that IT staff have administrator privileges – they don't ask for passwords. Outsiders, posing as IT staff, ask for passwords.

Never ignore threats made by a disgruntled employee. Deal with them.

Old electronic equipment must have the hard drive/ internal memory wiped clean prior to disposal, either with special software or by physically removing and destroying the hard drive.

Passwords should be safeguarded by employees. They shouldn't be shared with anyone.

Question your employees as to ways of improving your current security procedures.

Reception should have a list of the contractors and suppliers that will be on the premises on a given date.

Staff should be regularly reminded of safety and security protocols.

Third party cleaning and building staff should be bonded.

User accounts should be terminated as soon as an employee leaves your employ.

Visitors, contractors, etc should be required to report to the receptionist and then escorted throughout the facility by a staff member.

Whistleblowers can provide you with information regarding potential security breaches. Listen to them and protect them.

X'plain to staff that privacy and security is everyone's job.

Your security measures are only as strong as your weakest link. Your weakest link is your employees.

Zero in on your weakest link.