

To help prevent a data breach:

- **Lock up sensitive data.**
File storage such as cabinets, file rooms or other areas that store files containing private data about customers, clients, patients, accounts, employees, etc., should be locked.
- **Restrict access to data.**
electronic, should only be accessible to those who have a “need to know.” Put written procedures in place defining who has access to restricted information. Set up computer networks permitting only designated people to have access to specific areas or files on the computer network. Remember to limit network access on computer stations located in public spaces, such as the reception area. Most employees do not need unfettered access to the entire company network.
- **Determine what information is necessary.**
Don’t collect and keep data that is not absolutely necessary. Collecting excessive personal information, like Social Security numbers, can be more of a liability than an asset. What’s more, storing sensitive information longer than necessary or legally required, exposes companies to unwanted risks. Put a retention policy in place and be sure to destroy outdated information in a secure manner.
- **Put security systems in place.**
Install an alarm system that alerts law enforcement if you have a break-in on your premises. Install video surveillance equipment and motion sensitive cameras on premises to monitor activities, if feasible. In addition, random or roving security patrols add an extra layer of security.
- **Require sign-in for non-employee visitors.**
Prior to being allowed on company premises, all visitors should show identification and sign in. This includes vendors, customers and prospective employees. Severely restrict or prohibit visitor access to areas containing files or other sensitive information.
- **Screen all employees.**
Implement hiring practices for all employees, especially those with access to sensitive information. Use criminal and background screening companies. All employees that have access to sensitive information—including cleaning crews, technicians, administrative assistance, temporary employees—should sign a confidentiality and security document.
- **Record and regularly review data practices.**
Distribute and explain data protection protocols to all employees. Review and revise these practices on a regular basis, at least once a year. Retrain staff when protocol changes are made.
- **Conduct routine audits.**
Put best practices and policies in place. Routinely audit them, by making sure: (a) sensitive files are locked up when not in use; (b) only authorized users can access confidential information; (c) sign-in logs are being maintained; and sensitive documents are being properly destroyed.



(over)

Tips for preventing a data breach when dealing with technology:

- **Limit the use of portable technology.**
Restrict the transfer of sensitive information from on-premises computers to portable devices such as cell phones, PDAs, laptops, USB flash drives and removable hard drives. If it is necessary to put confidential data on these devices, make sure information is encrypted and password protected.
- **Don't use wireless networks.**
Even when properly secured, off-the-shelf wireless networks *do not* provide adequate enterprise level security to safeguard confidential data. As a standard rule, refrain from using wireless networking technology (Wi-Fi) to access systems storing sensitive personal information.
- **Utilize password protection and encryption.**
Always encrypt sensitive information. Inexpensive or even free encryption technologies are readily available. All system users should be assigned unique user names and passwords, changed quarterly.
- **Install antivirus, anti-spyware and firewalls.**
To prevent the loss or mining of sensitive information by worms, Trojan Horses, viruses, etc., run all systems with the most recent enterprise level antivirus, anti-spyware, and anti-malware applications. Use firewalls to lock out hackers.
- **Regularly update all systems and software.**
To maintain the most up-to-date protection, download recently issued system "patches," antivirus and anti-malware registries containing the newest forms of viruses, Trojans Horses and other malicious software.
- **Evaluate contractor access to information.**
Review and consider any and all access that outside contractors or vendors have to sensitive data and determine the need for such access. For example, access to employee personally identifiable information should only be for payroll or benefit purposes. Be sure that relevant vendor agreements provide adequate safeguards and that vendors agree to: (a) abide by reasonable industry safeguards; (b) cover the costs and handling of any misuse or loss of sensitive data; and (c) have the financial capability, whether through a bond or insurance coverage, to pay for any required remediation in the case of a loss of information.
- **Properly dispose of technology tools.**
Implement policies on how to destroy old computers, disks, tapes, CDs, memory devices and any other equipment that may contain sensitive information. Often these devices can provide access to sensitive information, even if the information is deleted. Do not rely on the "delete" or trash function to remove files containing sensitive information. It is often best to physically destroy the devices when they are no longer needed.

