
Confidential Information policy

Employers should take the following steps to protect confidential information

1. Limit access to disclosure.

Keep the disclosure of confidential information limited to a discrete group of individuals who need the information to perform their jobs or for other legitimate business functions. Remind employees at meetings or events where confidential information will be disclosed that the information is confidential and that they have a duty to maintain confidentiality.


2. Use appropriate contractual protections.

- use confidentiality agreements and, for confidentiality agreements outside the employment relationship.
- use confidentiality policies with employees that remind employees of their duties to preserve confidentiality.
- ensure that confidentiality agreements and policies comply with HIPAA requirements; and
- use non-compete agreements where permitted by state law.

3. Establish appropriate security measures:

- be consistent in marking documents or materials as confidential information, as needed, but do not mark materials that are not truly confidential, and do not fail to designate material the company wishes to protect.
- keep sensitive information physically guarded by maintaining single entry into the building, installing security cameras, posting signs limiting general access to areas where sensitive information is stored, and using physical and/or electronic access controls.
- remove confidential information, as needed, by only authorized individuals from the employer's premises.
- use secure emails with proper encryption.
- password-protect confidential material that is stored electronically, and only authorized individuals with a need to know the information have access to these passwords.
- set up hard drive encryption, anti-virus software for employee use of company computers on/offsite.
- use AWS instances with LUKS disk encryption to secure data in rest
- use key paired SSH, SCP or SFTP for AWS instances and S3 buckets to secure data in transit.
- maintain non-electrically stored items in locked cabinets or other secure areas.
- for visitors, such as requiring that they sign acknowledgments prohibiting disclosure of information viewed or accessed during a visit and requiring that they be accompanied by employees while in locations where sensitive information might become known.

4. Train employees:

- ask employees to sign documents acknowledging receipt and understanding of confidentiality policies and training; and
 - remind employees of their obligations with respect to taking confidential or trade secret information off the premises and using company laptops remotely.
- 

- ask employees to take HIPAA training class and get certificates

5. Departing employee procedures:

- provide departing employees with copies of any confidentiality agreement they signed during their employment and the company's policy on confidential information and trade secrets.
 - remind departing employees of their continuing obligations to keep information confidential and ask departing employees to sign an acknowledgement of their continuing obligations.
 - shut off the employee's access to computer files and other information technology systems immediately on termination.
 - review the departing employee's computer activity, hard drives, email, voicemail, and other communication records for the period before the employee's termination if there is a high risk of misappropriation.
 - ensure that the departing employee surrenders all company documents, files, and other material (including electronic documents) and signs an acknowledgement of having done so;
 - ensure that the departing employee returns all company access cards, PDAs, and other electronic devices; and
 - change electronic passwords as needed.
- 