Protect Paper-based Information

Sensitive information requires diligence regardless of the media on which it is stored. **Confidential** information is treated with some level of sensitivity, but there may not be legal consequences to unauthorized access or disclosure of it. **Protected** information is highly sensitive information protected by law or regulation and requires the highest level of access control and protection while in storage or transit. Unlike confidential information, protected information has defined legal consequences to not securing the information appropriately.

Examples of Protected Information

PII - Personally Identifying Information

PHI - Protected Health Information

PCI – Payment Card Industry data

Protected information requires special consideration as mandated by various federal and state regulations, such as HIPAA, and applies to information in all formats, including paper. A key characteristic of protected information is often a requirement to notify specific agencies in the event of a data breach, when protected information is inadvertently disclosed.

Best Practices - Protect Paper-based Information

Follow these best practices to avoid security breaches when working with paper-based sensitive data:

* Only distribute documents to those who have a business need for the information. Know who is receiving protected information and how the recipients plan to use the information. When sharing paper-based protected information, consider using a watermark or other tool that provides notice that the information included is protected and should be treated with the utmost sensitivity.
* Be aware of leaving printed documents unsecured in open work areas where they can be easily accessed by other people who don’t require access to the information. This includes shared or open workstations, unsecured conference rooms, library areas, or even printer trays. To guard against unauthorized access to protected data, avoid leaving documents unattended in these types of open or unsecured areas.
* Paper documents containing protected information should be stored in secure locations, such as locked filing cabinets or in locked rooms. Avoid leaving documents containing protected information such as PII or PHI in unsecured locations such as a desktop, a car, or even at home. Further, avoid transporting documents containing protected data in folders, briefcases, or bags that cannot be locked.
* Familiarize yourself with firm policies and procedures that outline how to report the loss of or unauthorized access to protected data.
* Familiarize yourself with firm policies and procedures related to document storage and destruction to ensure the security of sensitive data.