How we ensure data security and privacy when handling sensitive employee information:

Administrative Safeguards

Segal has documented and implemented processes and procedures for obtaining authorization for staff member's access to PHI, PII and other Confidential Data. These processes and procedures are managed by Information Technology, and requests for and authorization of access are recorded in an Information Technology issue tracking and reporting system. Segal will use its "Minimum Necessary Principle", which has been established as part of Segal's Information Security Policies as the basis for the type and extent of authorized access to PHI, PII and other Confidential Data.

Data security and risk is reviewed and analyzed on an on-going basis through regular operational and compliance processes. Administrative, technical and physical and technical security compliance is audited annually via an IT controls audit performed by an external audit firm. IT systems are monitored daily through automated and operational processes. Annual compliance audits of individual client cases are performed by practice area. These internal audits include a review of physical space, network storage and transmission of data to ensure all security policies, procedures and standards are adhered to. Client needs and regulatory requirements are constantly evaluated throughout the company using industry standard malware and intrusion protection software, server and workstation security patch management, Web filters and Internet E-mail filters.

Technical Safeguards

Segal workstations are standardized with the latest patched versions of the operating systems and standard applications, and malware and intrusion protection. Additional security enhancements include complex passwords, hard disk encryption, encryption of data on removable devices, regularly scheduled system updates, monthly security updates and a regularly required reboot of all PCs.

Transmission of protected or sensitive data is accomplished through the use of industry standard encryption solutions.

Network vulnerability testing is performed on a regular basis by Segal personnel and on a periodic basis by external firms specializing in network security.

Segal desktop and laptop hard drives are encrypted. Segal has implemented a security policy stating that all data sent to third parties on removable media or via electronic transmission must be encrypted using company standard encryption methods or other IT or client or vendor secure systems. Technical controls, including e-mail and web Data Loss Prevention monitoring and filtering solutions have been implemented to detect any potential policy violations

Physical Safeguards

A combination of security guards, access cards and/or key locks control access to The Segal's facilities. In addition, physical access to any of Segal's network equipment or communications rooms is restricted by access card readers or key locks that limit access to the Information Technology Department and other authorized personnel.

Contingency Operations processes have been implemented to ensure the restoration of data as defined in The Segal Business Continuity Plan. The Segal Business Continuity Plan calls for recovery of operations at an alternate Segal facility that is subject to and is consistent with The Segal's standard security measures including security guards, access cards and/or key locks.

Company security policies dictate that laptop computers be locked to their docking stations or secured in locked cabinets when not in use. All computer hard drives are fully encrypted to prevent data loss in the event of lost or stolen computers.