Ensuring Consumer/Student/Patient/Member Privacy & Safeguarding Client Proprietary Information

Client information is always kept confidential and is proprietary to the client. File backups are maintained indefinitely and can be made available at your request. In addition, our live contact center network is a closed platform preventing unauthorized intrusion from external sources. Internally, all client databases, lists and payment processing information are only available to management at a central and controlled facility. These procedures are designed to prevent the unauthorized release, sale or use of client data such as customer lists and financial information.

Our platform is designed to support applications for major financial institutions, educational institutions, governmental agencies, multinational corporations, healthcare organizations, major non-profit organizations and large retail customers. As such, significant security mechanisms are in place to fully track all system activity/data utilization and prevent any unauthorized use or disclosure of confidential donor information.

All data captured on the behalf of our clients is confidential, proprietary and the sole property of that client. All data is centrally warehoused at Ansafone Contact Centers' headquarters in Orange County, California, on a closed network with back-up data stored as required at undisclosed locations. Additionally, existing PCI/HIPAA/HITRUST compliant customer CRM systems are utilized over secure connections when available so that consumer data is not stored in our systems.

While data records are available to appropriate personnel in a controlled format (readable only) for the purposes of assisting client constituents, it is only possible for senior management personnel to duplicate, remove, purge, manipulate or query any data. All data is treated by all staff and management as highly confidential work product. Further, all system usage is tracked using systems like Active Directory, AlienVault and Sophos.

Physical access to all of our facilities is controlled via hardened-facility access control with access to certain service areas and technical equipment restricted only to appropriate personnel. Access to systems and databases are all controlled by unique login and rotating passwords along with encryption keys. Finally, facilities are monitored via digital closed-circuit camera systems.

Automatic safeguards, on-going system checks, informal quality assurance/controls, and formal audits ensure full safeguard of client proprietary information.

Ansafone Contact Centers complies with relevant state and federal regulations as they pertain to privacy including but not limited to the Family Educational Rights and Privacy Act, Fair Credit Reporting Act (FCRA), Gramm Leach Billey Act, the Federal Do Not Call Registry (DNC), Telemarketing Sales Rule (TSR), the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry security standard (PCI). Ansafone Contact Centers is PCI compliant and adheres to generally accepted security standards of NIST and CIS as they relate to payment processing, storage of financial information, and the safeguarding of proprietary information. Ansafone maintains a PCI Certified status from Trustwave/Trustkeeper and can furnish our PCI certificate and other documentation upon requests. Ansafone also maintains a SOC2 Type II compliance via A-Lign.

Revised 1/17/2020 Jared Mendez, CTO

For additional information regarding Ansafone Contact Centers' privacy standards or for any personal data requests please contact us at (866)222-7298 or compliance@ansafone.com.

Revised 1/17/2020 Jared Mendez, CTO