

Data Confidentiality Compliance Policy

Effective Date: 05/02/2008

BACKGROUND

Allegiance provides web, paper, automated phone, and personal phone services to organizations located throughout the world. Allegiance is committed to protecting the privacy and data of its clients and their employees. Allegiance shall govern strictly the disclosure of any information to anyone other than as authorized under the contract Allegiance has with the client. Access to data requires login credentials, and all reports sent directly to our Allegiance clients are done via secure electronic systems, and unless legally mandated, are never shared with an outside party. Allegiance further agrees to adhere to the Safe Harbor privacy principles of the U. S. Department of Commerce's Safe Harbor Program.

PURPOSE

The purpose of this policy is to provide written guidance ensuring that all confidential, proprietary and privacy related information is handled properly.

POLICY

1. Any employee who engages in unauthorized disclosure of any information concerning a client, their employees, proprietary information, financial data, or otherwise sensitive information not related to their work related activities may be subject to immediate termination.
2. Employees are not to discuss or release any private, confidential, financial, or proprietary information outside the official business of Allegiance and in conformance with client engagement contracts.
3. Employees are not to discuss or release any client proprietary or privacy information in an external or internal environment (e.g. common area) where an unauthorized person might overhear what is being said.
4. If asked about confidential information by anyone not involved in the performance of official Allegiance business or data owner, no disclosure of such information will be allowed without specific approval by an authorized supervisor, Chief Operating Officer (COO), or Chief Technology Officer (CTO).
5. No one is to have access to client data records or call records or other client information unless they are involved in the performance of service on behalf of that client as described in the engagement contract, or as part of their work related activities.
6. All information submitted through Allegiance via web, paper, automated phone, or through personal phone call shall be secured and protected from external sources, unless legally obligated.

7. No remote access to customer data will be provided unless it is required as part of the employees job requirement, and with executive approval.
8. No customer information is to leave Allegiance or its data center without formal written or customer approval. Customer data sent to the same customer does not apply. Data that leaves Allegiance must be kept secure. Digital data must be encrypted and/or password protected.
9. Doors should remain closed and locked during all hours, with the exception of the door to the reception area which remains open during normal office business hours.
10. No customer data is to be emailed, mailed, or sent in any form outside of Allegiance or customer unless prior approval is received from the customer administrator, or by legal obligation.
11. All employees with access to customer information must lock access to their Operating System when leaving their desk.
12. All changes to employee security must be approved by a security approval board. This board currently consists of the Office Manager, CTO, HR representative, and VP of Technology.

PROCEDURES

1. Anyone who believes this policy is being violated should report it to an appropriate Compliance Policy Manager (privacycompliance@allegiance.com) or executive staff member.
2. The Compliance Policy manager or executive staff is responsible for investigating all allegations received concerning alleged violations of this policy.

Please sign and return to current Office Manager

Employee Signature: _____ Date: _____

Print Name: _____

Reviewed and validated

Compliance manager: _____ Date: _____

Print Name: _____