Corporate Privacy Policy

BenefitHelp

1. Purpose for Policy

BenefitHelp places a high value on the privacy of its clients ("Clients") and the expectation that information regarding Clients remains confidential and is made available only to persons who have a legitimate right to know. BenefitHelp recognizes that all employees and temporary workers ("Employees"), as well as outside contractors, have an ethical and legal obligation to keep certain information about Clients confidential and to protect and safeguard this information against tampering and unauthorized use or disclosure.

2. Overview

This privacy policy concerns "protected client information" ("PCI"). PCI, as defined herein means; any individually identifiable health, financial or personal information of a Client, including, but not limited to: social security number, name, address, birth date, age, telephone number, subscriber number, policy number, e-mail address, fax number, and medical records.

PCI is not confined to written materials, facsimiles, or hard copy, but also includes information derived from any source, including, but not limited to: E-mail, computer data, data stored on electronic media, disks, or personal digital assistants (PDA), verbal communications or recordings, and visual observation.

3. Procedures

The following section outlines the basic procedures necessary to comply with this policy.

Disclosure of Information

- An Employee may access, discuss, use, and disclose PCI only for BenefitHelp business as it relates to that employee's specific job functions and/or responsibilities.
- Employees may disclose PCI only to those who have a legitimate, BenefitHelp-related business need to know or who have prior written authorization. PCI about a Client may only be shared for purposes of claims payment or healthcare operations or other business authorized by the Client.
- PCI must never be the subject of casual conversation either inside or outside of the workplace. PCI must not be discussed in lobbies, stairwells, elevators, restrooms, hallways, or any other public area where conversation could be easily overheard by visitors and Employees who do not have a need to know.
- Only "Minimally Necessary" PCI may be disclosed. "Minimally Necessary" means only that amount of PCI necessary to accomplish the intended purpose of the use or disclosure.

Access to Information

- PCI may only be accessed if related to specific job functions and responsibilities.

- Casual reading of PCI is not permitted.
- Employees with legitimate access to PCI will protect this information from casual or unauthorized access.

Security of PCI

- Employees may remove PCI from the facility only as it relates to specific job functions and/or responsibilities. It is the responsibility of each Employee to protect and safeguard all such information.
- Copies of PCI are to be destroyed after use by placing them in a covered recycling bin for destruction.
- Employees are encouraged to review PCI in a secure area and are responsible for records that are checked out to them. It is the responsibility of the Employee to protect and safeguard all records that are removed from the secure areas.

Breach of Confidentiality

- Any Employee who believes he/she has observed a breach of confidentiality is encouraged to address the person directly. If this is not an option, the Chief Privacy Officer should be notified.
- Employees found to be in violation of this policy may be subject to disciplinary action, up to, and including termination and/or legal action. PCI is protected by federal and state laws and regulations that define civil and criminal penalties for violations of confidentiality.
- BenefitHelp will periodically conduct unscheduled audits to ensure compliance with this policy.

Safeguarding PCI

- In order to maintain confidentiality, any item containing PCI must be discarded according to the standards identified below:

Item	Examples	Where/How Discarded
Paper	Medical records, applications, census files, or any other paper-based document containing PCI	Original hardcopies should be placed in a sealed recycle bin for destruction. Electronic copies stored in the BenefitHelp Document Management System will be password protected using encryption procedures.

- Employees must not leave any PCI on fax machines, printers, or copies.
- Employees are to clean their workspace of PCI at the end of their work day.
- Employees must exercise caution and discretion when leaving voicemail messages containing PCI.
- Employees are to escort visitors through work areas.

- Employees must exercise caution and discretion when E-mailing PCI internally within BenefitHelp.
- Employees must not store PCI on PDAs.
- Employees must secure all hardcopy mail containing PCI.
- Employee workstations will be programmed to auto-lock after 30 minutes of inactivity.

Employees should refrain from loading PCI on pooled laptops. Information stored on laptops will be routinely purged.

_____ _____

Signature Date

Employee Signature & Acknowledgement of receipt and understanding of BenefitHelp privacy policy

Corporate Privacy Policy