



HIPAA Compliance Statement

Updated June 2021

The Careficient Agency Management service provided by Careficient is HIPAA compliant. Under the HIPAA privacy rules Careficient, Inc. is considered a Business Associate.

It is our policy to comply with the rules and regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Through our Service Agreement and a Business Associate Agreement (BAA) with the Covered Entity, we give contractual guarantees that we will use Protected Health Information (PHI) that we are granted access to only for the purposes for which we have been contracted. We will safeguard the information from misuse and will help the Covered Entity comply with their obligations under the HIPAA rules. If the Covered Entity does not have a BAA of their own we will provide one as an addendum to our Service Agreement (see attached BAA). If required by the Covered Entity we will make the necessary changes to our Service Agreement and/or our BAA to ensure our HIPAA compliance meets their needs.

We have taken the necessary steps to assure Careficient is compliant as follows:

Accounting of disclosures and audit trail issues:

We are appointed by and contracted to the Covered Entity to assist in the payment process and are considered part of the treatment, payment, or health care operations (TPO). A Covered Entity is not required by HIPAA regulation to keep an accounting of anyone within their own organization who has received (or had access to) medical information. The accounting provision only covers "disclosures," which are defined as the sharing of health information with someone outside of an organization that is not a part of the TPO. See Section 164.528(a) (right to accounting of disclosures) and Section 164.501 (definition of "disclosure"). The regulation specifically states that a Covered Entity does not have to keep an accounting of information disclosed to someone outside of the organization for the purposes of treatment, payment, or health care operations. See Section 164.528(a)(1)(i). The result of these exclusions are that a Covered Entity is required to account for only a narrow category of disclosures that primarily are not related to health care, such as those made to law enforcement personnel or pursuant to a request for documents in a lawsuit.

Data is protected from unauthorized viewing/usage:

Careficient access is restricted via password to only those employees that have a need to know. Servers and data storage units are in a secured SSAE 16 compliant data center with limited access. Data is received and forwarded via automated, electronic processes where no direct human intervention is required. Access or viewing of PHI is only allowed when required to provide further support to the Covered Entity. Archive and backup tapes are encrypted and stored in a secured location in a fireproof safe.

Proper disposal of data:

At the end of a Covered Entity's contract or upon cancellation of services by the provider with Careficient their data will be archived per HIPAA guidelines and deleted from the Careficient systems. No printed reports or paper copies are ever retained in our facility. If reports are ever printed to further support the Covered Entity, they are shredded immediately upon completion of the task that required the paper output.

Privacy and Security Rule(s):

To protect the privacy and security of the PHI we have implemented the following processes:

- Covered Entities must execute a Service Agreement and BAA to subscribe to our service
- All employees, contractors, sub-contractors, agents, and representatives are required to sign an agreement to abide by the HIPAA Privacy Act and a Confidentiality & Non-Disclosure agreement
- Support data encryption on all websites and all reports
- E-mail address verification
- Restricted access to PHI on a need-to-know basis (via passwords and company policy)
- Automatic expiration of passwords
- 24/7 restricted access to SOC1, SOC2 and SOC3 certified Data Centers
- Office facility is locked 24/7, requires keycard access and has monitored security system installed throughout the facility
- Automated encrypted data backups
- Encrypted data backups stored in secured safe
- Automated virus checking
- HIPAA and Security awareness training for all employees, contractors, sub-contractors, agents and representatives is mandatory
- Employee termination security procedures in place
- All retired computer hard drives are shredded

HIPAA Transaction and Code Set Rule

- HIPAA compliant EDI transactions are used when applicable
- HIPAA compliant Code Sets are used when applicable

Careficient is committed to full and complete compliance with all HIPAA rules and regulations. As necessary, we will adjust our policies to adhere governmental regulations, to our clients' needs and to adjust to any changes in the HIPAA rules. If you have any questions concerning our HIPAA compliance policies, please contact Support at <mailto:support@Careficient.com>.