HIPAA Privacy Policy For

Business Associate

Contents

HIPAA Privacy Policy

A. Introduction

Medskinessentials performs services for Covered Entities that on occasion involve the use or disclosure of Protected Health Information. Medskinessentials is considered to be a business associate under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Protected health information (PHI) means information created, received, or maintained by Medskinessentials from or on behalf of the Covered Entity that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living, or persons deceased for less than 50 years.

Medskinessentials shall make every effort to comply in good faith with the terms of the business associate agreements that it enters into with Covered Entities. To that end, all members of Medskinessentials workforce must comply with this Privacy Policy.

No third-party rights are intended to be created by this Policy. Medskinessentials reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or any business associate agreement, the Policy shall be aspirational and shall not be binding upon Medskinessentials. This Policy does not address requirements under other federal laws or under state laws.

B. Medskinessentials Responsibilities as Business Associate

I. Privacy Official and Contact Person

[Insert person's name or title] will be the Privacy Official for Medskinessentials. The Privacy Official will be responsible for overseeing the business associate agreements entered into by Medskinessentials with Covered Entities. In addition, the Privacy Official shall be responsible for monitoring Medskinessentials compliance with the terms of those business associate agreements.

II. Workforce Training
The Privacy Official is responsible for ensuring that all workforce members receive the training necessary and appropriate to comply with the terms of the HIPAA business associate agreements.

III. Safeguards and Firewall
Medskinessentials will establish appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. Technical safeguards include limiting access to information. Physical safeguards include locking doors or filing cabinets.

IV. Complaints
The Privacy Official will be the contact person for receiving complaints. Any individual who believes that this Policy or the terms of a business associate agreement have been violated shall report such violation to the Privacy Official.

V. Sanctions for Violations of Privacy Policy
Sanctions for using or disclosing PHI in violation of this Policy or a business associate agreement shall be addressed by Medskinessentials. Sanctions may include reprimand, suspension, or termination of employment.

VI. Mitigation of Inadvertent Disclosures of PHI
Medskinessentials shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of PHI in violation of this Policy or a business associate agreement. As a result, if an individual becomes aware of an unauthorized use or disclosure of PHI, the individual must immediately contact the Privacy Official so that appropriate steps to mitigate harm can be taken.

VII. No Intimidating or Retaliatory Acts
No individual may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

VIII. Documentation
Medskinessentials privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with

changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

C. Policies on Use and Disclosure of Protected Health Information

I. Permitted Uses and Disclosures on Covered Entity's Behalf

Medskinessentials is permitted to use and disclose PHI that it creates or receives on Covered Entity's behalf or receives from Covered Entity (or another business associate of Covered Entity) and to request PHI on Covered Entity's behalf (collectively, "Covered Entity's PHI") to perform services for the Covered Entity.

II. Permitted Uses and Disclosures for [Insert Business Associate Name] Operations

Medskinessentials is permitted to use the Covered Entity's PHI for proper management and administration or to carry out legal responsibilities, provided that, with respect to disclosure of Covered Entity's PHI, either: (A) the disclosure is Required by Law; or (B) Medskinessentials obtains reasonable assurance from any person or entity to which Medskinessentials will disclose Covered Entity's PHI that the person or entity will:

- Hold Covered Entity's PHI in confidence.
- Use or further disclose Covered Entity's PHI only for the purpose for which Business Associate disclosed Covered Entity's PHI to the person or entity or as Required by Law.
- Promptly notify Medskinessentials (who will in turn notify Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of Covered Entity's PHI was breached.

III. Complying With the "Minimum-Necessary" Standard

Medskinessentials will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of Covered Entity's PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Medskinessentials will not be obligated to comply with this minimum-necessary limitation if neither Medskinessentials nor the Covered Entity is required to limit its use, disclosure or request to the minimum necessary. The phrase "minimum necessary" shall be interpreted in accordance with HIPAA and its implementing regulations.

IV. Disclosures of PHI to Subcontractors and Agents

Medskinessentials will require any of its subcontractors and agents to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to Covered Entity's PHI and/or Electronic PHI that are applicable to Medskinessentials.

V. Privacy or Security Breach

Medskinessentials will report to the Covered Entity any use or disclosure of Covered Entity's PHI which is not permitted under the business associate agreement along with any Breach of Covered Entity's Unsecured PHI. Medskinessentials will treat the Breach as being discovered in accordance with 45 CFR § 164.410. Medskinessentials will make the report to Covered Entity's Privacy Official not more than 30 calendar days after the Medskinessentials learns of such non-permitted use or disclosure. If a delay is requested by a law-enforcement official in accordance with 45 CFR § 164.412, Medskinessentials may delay notifying the Covered Entity for the applicable time period. Medskinessentials report will at least:

- Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach.
- Identify Covered Entity's PHI that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual basis.
- Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure.
- Identify what corrective or investigational action Medskinessentials took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches.
- Identify what steps the individuals who were subject to a Breach should take to protect themselves.
- Provide such other information, including a written report, as Covered Entity may reasonably request.

VI. Security Incidents

Medskinessentials will report to the Covered Entity any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's Electronic PHI or (B) interference with Medskinessentials system operations in the information systems, of which Medskinessentials becomes aware.

VII. Prohibition on Unauthorized Use or Disclosure

Medskinessentials will neither use nor disclose Covered Entity's PHI, except as permitted or required by a business associate agreement or in writing by the Covered Entity or as Required by Law. Medskinessentials may

not use or disclose Covered Entity's PHI in a manner that will violate the Privacy Rule if done by the Covered Entity.

D. Policies on Individual Rights

I. Access to PHI and Requests for Amendment

Medskinessentials will, within 20 calendar days following Covered Entity's request, make available to the Covered Entity or, at Covered Entity's direction, to an individual (or the individual's personal representative) for inspection and to obtain copies of Covered Entity's PHI about the individual that is in Medskinessentials custody or control, so that the Covered Entity may meet its access obligations under 45 CFR § 164.524. Effective as of the date specified by HHS, if the PHI is held in an Electronic Health Record, then the individual shall have a right to obtain from Medskinessentials a copy of such information in an electronic format. Medskinessentials shall provide such a copy to the Covered Entity or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously, and specifically made by the individual or Covered Entity.

II. Accounting

Medskinessentials shall assist Covered Entities in satisfying its disclosure accounting obligations under 45 CFR § 164.528:

- **Disclosures Subject to Accounting.** Medskinessentials will record the information specified below ("Disclosure Information") for each disclosure of Covered Entity's PHI, not excepted from disclosure accounting as specified below, that Medskinessentials makes to the Covered Entity or to a third party.
- **Disclosures Not Subject to Accounting.** Medskinessentials will not be obligated to record Disclosure Information or otherwise account for disclosures of Covered Entity's PHI if Covered Entity need not account for such disclosures.
- **Disclosure Information.** With respect to any disclosure by Medskinessentials of Covered Entity's PHI that is not excepted from disclosure accounting, Medskinessentials will record the following Disclosure Information as applicable to the type of accountable disclosure made:
    - **Disclosure Information Generally.** Except for repetitive disclosures of Covered Entity's PHI as specified below, the Disclosure Information Medskinessentials must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) the address of the entity to which Medskinessentials made the disclosure, (iii) a brief description of Covered Entity's PHI disclosed, and (iv) a brief statement of the purpose of the disclosure.
    - **Disclosure Information for Repetitive Disclosures.** For repetitive disclosures of Covered Entity's PHI that Medskinessentials makes for a single purpose to the same person or entity (including Covered Entity), the Disclosure Information that Medskinessentials must record is

either the Disclosure Information specified above for each accountable disclosure, or (i) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (ii) the frequency, periodicity, or number of repetitive accountable disclosures; and (iii) the date of the last repetitive accountable disclosures.

- **Availability of Disclosure Information.** Medskinessentials will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates (3 years for disclosures related to an Electronic Health Record, starting with the date specified by HHS). Medskinessentials will make the Disclosure Information available to Covered Entity within 30 calendar days following Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. Effective as of the date specified by HHS, with respect to disclosures related to an Electronic Health Record, Medskinessentials shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual.

III. Requests for Restrictions on Use and Disclosure of Protected Health Information

Medskinessentials will comply with any agreement that the Covered Entity makes that either (i) restricts use or disclosure of Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(a), or (ii) requires confidential communication about Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(b), provided that Covered Entity notifies Medskinessentials in writing of the restriction or confidential communication obligations that Medskinessentials must follow. A Covered Entity will promptly notify Medskinessentials in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Medskinessentials whether any of Covered Entity's PHI will remain subject to the terms of the restriction agreement.