Berkeley Research Group, LLC
Name: HIPAA PRIVACY POLICY

Effective Date: January 2017

A. Introduction

Berkeley Research Group LLC ("BRG") is an independent expert testimony, strategic advisory services, and data analytics firm (the Firm). Members of the Firm's workforce may have access to individually identifiable health information on behalf of (1) the Firm itself; or (2) its clients.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations restrict the Firm's ability to use and disclose protected health information ("PHI"). The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients certain rights with respect to that information. Consistent with these patient rights, the HIPPA Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Protected Health Information. PHI is identifiable information about the past, present, or future physical or mental health or condition (including the provision of his/her health care, insurance, payment status, etc.) of an individual obtained or managed by a health care provider or other health-related entity "Covered Entity". PHI may be information that is recorded electronically, on paper or orally. PHI must be protected from unauthorized use or disclosure by the Covered Entity under HIPAA regulations.

It is the Firm's policy to comply fully with HIPAA's requirements. To that end, all members of the Firm's workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Firm's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, independent contractors, volunteers, trainees, and other persons whose work performance is under the direct control of the Firm, whether or not they are paid by the Firm. The term "employee" includes all of these types of workers.

No third party rights are intended to be created by this Policy. The Firm 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 HIPPA, the Policy shall be aspiring and shall not be binding upon the Firm. This Policy does not address requirements under other federal or state laws.

I. Privacy Official and Contact Person

Kate Koppenhoeffer will be the "Privacy Official" for the Firm. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Firm's use and disclosure procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

II. Workforce Training

It is Firm's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions.

III. Technical and Physical Safeguards and Firewall

The Firm will establish appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls and implementing password and encryption procedures to limit access to PHI ("Security Procedures"). Physical safeguards include locking doors or filing cabinets where access to PHI can occur.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for authorized employees to perform their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Practices

The Privacy Official is responsible for developing and maintaining a notice of the Firm's privacy practices that describes:

- Uses and disclosures of PHI;
- Individual's rights; and
- The Firm's legal duties with respect to the PHI.

The privacy notice will inform employees that the Firm will have access to PHI in connection with the performance of services to its clients.

V. Complaints

Kate Koppenhoeffer will be the Firm's contact person for receiving complaints ("Privacy Official"). The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Firm's privacy procedures, or violations of those procedures, and for creating a system for handling such complaints. Complaints will be handled in a confidential manner with only those with a need to know involved in the resolution of the complaints. Complaints can be directed to the Privacy Official at 312-429-7920 or kkoppenhoeffer@thinkbrg.com, to the Firm's General Counsel, Eric Miller at 202-585-1487 or emiller@thinkbrg.com or to the Firm's designated e-mail at privacyofficial@thinkbrg.com.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with BRG's corrective action policy, up to and including termination which is addressed in the Firm's Policy Employee Handbook.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

BRG shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a potentially inappropriate disclosure of PHI that is not in compliance with this Policy they should immediately contact the Privacy Official so that the appropriate steps to mitigate the potential harmful effects can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee 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.

IX. Firm Requirements

The Firm policy shall include provisions to describe the permitted and required uses and disclosures of PHI by the Firm. Specifically, the Firm shall require its employees and agents to:

- Not use or further disclose PHI other than as permitted by the Firm or as required by law;
- Ensure that any agents or subcontractors to whom it provides PHI received from the Firm or its clients agree to the same restrictions and conditions that apply to the Firm;
- Report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Make the Firm's internal practices and records relating to the use and disclosure of PHI received from the Firm's clients available to applicable regulatory bodies upon request; and
- If feasible, return or destroy all PHI received from the Firm's clients in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

X. Documentation

The Firm's privacy policies and procedures shall be documented and maintained for at least six years. 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.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The Firm shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to the use and disclosure of PHI. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The documentation must be maintained for at least six years.

B. Use and Disclosure of PHI

I. Use and Disclosure Defined

The Firm will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for the Firm or its agents.

- *Disclosure.* For information that is protected health information, disclosure means any

release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by the Firm.

II. Workforce Must Comply With Firm's Policy and Procedures

All members of the Firm's workforce who have access to PHI (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and with the Firm's use and disclosure procedures.

III. Access to PHI Is Limited to Certain Employees

Access to PHI will be limited to individuals assigned to work on specific client engagements and will be defined at the commencement of the project. PHI related to Firm employees will be accessed by human resources and management personnel on a need to know basis.

IV. Mandatory Disclosures of PHI: to Individual and DHHS

PHI must be disclosed as required by HIPAA in two situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows); and
- The disclosure is made to DHHS for purposes of enforcing of HIPAA.

V. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Labor;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making *disclosures* of PHI to any Business Associate or providers for claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from Business Associates, providers or Plan Participants for purposes of claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

VI. Disclosures of PHI to Business Associates

Employees may disclose PHI to business associates and allow the business associates to create or receive PHI on its behalf. However, prior to doing so, we must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

A *Business Associate* is an entity that:

The Firm frequently executes business associate agreements with its clients and subcontractors to:

- Perform or assist in performing a function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- Provide legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services.

VII. Disclosures of De-Identified Information

The Firm may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a Covered Entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers. Contact the Privacy Official before disclosing any information that might be considered de-identified information.