Please provide current contact information for our records:

Date: June 15, 2022

Business Name: Benefit Insurance Marketing (Bim Group)

Mailing Address: 1151 Red Mile Rd Lexington KY 40504

Telephone: 859-255-9455

Fax: n/a

Website URL: www.bimgroup.us

First Contact	Second Contact
Full Name: Dustin Stacy	**Full Name: Heather Taylor**
Title: President	**Title: Sr. Director of Operations**
Mailing Address: 1151 Red Mile Rd	**Mailing Address: 1151 Red Mile Rd**
City / State / ZIP: Lexington KY 40504	**City / State / ZIP: Lexington KY 40504**
Telephone: 859-255-9455	**Telephone:859-255-9455**
Fax:	**Fax:**
Email: dustin@bimgroup.us	**Email: heather@bimgroup.us**

In regard to PMC's protected health information (PHI), does your organization:

(Check all that apply. If none, mark as "n/a".)

Create	**n/a**
Receive	**Yes**
Transmit	**Yes**
Maintain / Store	**Yes**

HIPAA Compliance Status Questionnaire

Part I. Business Associate:

Company name:

Part II. Business Associate Information:

What type(s) of service do you provide to Pikeville Medical Center (PMC)?	Bim Group provides insurance consulting services for PMC's employee benefit Health & Welfare Plan. This can include analysis of health and ancillary benefit plans, renewal benefit plan marketing activities, and claims reporting/budgeting/forecasting. A copy of our executed BAA with PMC is included here. Bim Group also assists as needed with claims resolution for members of the Plan. When engaged to assist with claims resolution, our team will obtain a signed release direction from the PMC employee to allow us to work on their behalf. A sample agreement is attached.
What type of PHI do you access?	Member demographic information to include names, SS number, DOB, health plan elections. Member medical and pharmacy claims information for analytics, marketing, and claims resolution purposes.
What quantity of PHI do you access?	Bim Group accesses PHI explicitly for the purposes of insurance services to include data for benefits eligible employees and dependents. This information is updated monthly for the purposes of claims analytics and can be used annually for marketing purposes with benefit carriers. An annual Data Use Agreement (DUA) would be obtained in advance of marketing the benefit plans. Because of current arrangements in place for PMC, we have not had to obtain a recent DUA for marketing activities. A sample DUA is attached for reference.
How do you access PHI?	Bim Group maintains a Microsoft SQL database containing member and service level claim detail for both medical and pharmacy. This database is updated monthly with a file provided by Aspirant, Inc. (formerly ARC Administrators), PMC's Plan Third Party Administrator to include the most recent claims and contains data back to January 2016.
How do you store PHI?	Our attached HIPAA Policy describes our protocols for storing and access to physical

	PHI. Our quantity of physical PHI documentation is extremely limited at this point as most PHI is stored electronically. ePHI is encrypted at rest and in motion, access is tracked via unique username and password with multi-factor authentication. Physical equipment containing ePHI is in an offsite data center with controls restricting access to hardware.
When did you complete your last HIPAA Risk Assessment?	The results of our latest HIPAA Security Risk Assessment in June 2022 utilizing the HHS Reference Tool, are provided as an attachment in our response.
If you use PHI off-site from PMC, do you access PHI through electronic means? If so, what safeguards are in place to protect the PHI?	Yes, PHI is accessed electronically. ePHI is stored encrypted while at rest and in transit. Access to data is allowed through restricted permissions and using a unique username and password with multi-factor authentication. Our Information Security Policy and Security Program Intent documents are attached.
Is any PHI maintained on portable media (flash drives or external hard-drives)?	No, Bim's policy prohibits the use of flash drives or external hard-drives.
How many employees do you have who have access to or use of PMC PHI?	The Bim service team includes 7 employees who would access and use PMC's PHI to deploy the services mentioned above.
Does your company use the PHI for purposes other than those for which you are a Business Associate? If yes, list the purposes for which data is being used or disclosed outside the purposes of the Business Associate Agreement.	No
Do you engage in any marketing activities in which PHI is used or disclosed in any manner?	Typically, our annual renewal marketing activities would include our team obtaining an annual Data Use Agreement (DUA) from PMC in order for us to market the benefit plan(s) for renewal and to obtain alternate options. We also obtain a signed Privacy Agreement (sample attached) for any subcontractors we engage in Health & Welfare planning on behalf of our clients.
Do you engage in any research activities in which PHI of PMC is used or disclosed? If yes, do you have a chain-of-custody agreement or other written agreement that requires the subcontractor to meet the requirements of HIPAA?	No, PMC's data is not utilized for research activities.
Are any of the services you perform done outside of the jurisdiction of the United	No

States? If yes, please list all other jurisdictions in which services are performed for PMC.	
Do you/your employees have direct contact with patients of PMC?	No
Has your company or any of your employees or subcontractors ever been involved in a data breach involving PMC's PHI? If yes, how many breaches and how many patients were affected?	No
What steps were taken to mitigate the consequences and notify the affected patients and PMC of the breach?	N/A

Part III. HIPAA Compliance Checklist

Does your Program include separate policies on Privacy and Security pursuant to the HITECH statute and Rules?	Yes, see our most updated HIPAA Privacy and Security Manual and Notice of Privacy Practices attached.
Have you completed vulnerability assessments of your network? If yes, have you created a Contingency Plan? [If the answer is yes, please respond to the following 6 questions. If no, skip to Part IV.]	Ad hoc vulnerability assessments are performed based on need or in the event of a security incident or suspicion. A Business Continuity Plan is in place including information on disaster recovery and incident response. Polices are attached.
Have you conducted an Application & Data Criticality Analysis?	Yes, systems and data critical to operation are prioritized for restoration.
Have you created a Disaster Recovery Plan?	Yes, the attached Business Continuity Plan covers disaster recovery scenarios and defines key needs and responses.
Have you created a Data Backup Plan?	Yes, this is included in the attached Information Security Policy. Data is backed up and stored offsite nightly, encrypted and tested for integrity.
Have you created an Emergency Mode of Operations Plan?	Yes, the emergency mode of operations plan is part of the business continuity plan and covers multiple scenarios of disaster.
Have you created testing and revision procedures?	Yes, business continuity and disaster recovery procedures and response are tested and policies revised when needed as the operations change
Are all employees of your organization, including Executive Officers/Board of Directors provided basic HIPAA training? If so, how often?	Yes, all employees including Executives are required to take annual HIPAA training most recently completed in May 2022.

Part IV. Compliance Officer or Department

Does your company have a HIPAA Compliance Officer/Compliance Department?	We currently employ a Compliance Consultant to coordinate our compliance

	initiatives and projects. Bim Group also engages an ERISA attorney to author / update internal agreements and policies related to HIPAA.
If so, please provide the name, title, and email address for the HIPAA Compliance Officer.	Lauren Johnson, Compliance Consultant, (lauren@bimgroup.us)
Has your company appointed a privacy and/or security officer?	Yes
If so, please provide the Privacy officer's name and email address.	Heather Taylor, Sr. Director of Operations (heather@bimgroup.us)
Is the privacy officer an employee of your organization?	Yes
If not an employee, is there a written contract between your Company and the Privacy officer regarding his/her duties and responsibilities?	N/A

*Please provide copies of your Compliance Program, last risk assessment and other documentation regarding your HIPAA Compliance Program, policies and procedures.

Please see following attachments:

- ***PMC / Bim Group BAA***
- ***Auth Form for Claims Assistance***
- ***Sample Data Use Agreement (DUA)***
- ***HIPAA Privacy and Security Manual 2022***
- ***Notice of Privacy Practices***
- ***Information Security Policy and Appendices:***
  - ***Appendix A ISP Acknowledgment Form***
  - ***Appendix B Business Continuity Procedure***
  - ***Appendix C Security Incident Handling***
  - ***Appendix D Definition and Guidelines for transmitting ePHI***
  - ***Security Program Policy / Intent***
- ***Sample Privacy Agreement (subcontractors)***
- ***HIPAA Security Risk Assessment***

By signing this document, you agree that you have answered all questions honestly and to the best of your knowledge.

Part V. Verification

Prepared and submitted by: Heather Taylor

Name and Title: Heather Taylor Sr. Director of Operations

Date: June 15, 2022