DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (212) 264-3313, (800) 368-1019
TDD - (212) 264-2355
(FAX) - (212) 264-3039
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region II
Jacob Javits Federal Building
26 Federal Plaza, Suite 3312
New York, NY 10278

MAY 17 2019

Via U.S. Mail and email to [redacted]

[redacted]

OCR Reference Number: [redacted]

Dear [redacted]

On March 26, 2018, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received your complaint alleging that Cohen, Bergman & Klepper, M.D.'s P.C. (CBK) is not in compliance with the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D). Specifically, you allege that, from July 2015 to March 19, 2018, CBK had more than 42,000 patients' electronic protected health information (ePHI) available to access by unauthorized individuals online. You also allege that, although CBK was informed of this issue on February 12, 2018, the entity did not secure the ePHI until March 19, 2018. These allegations could reflect a violation of 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(4), 164.308(a)(5), 164.308(a)(6)(ii), 164.308(a)(8), 164.312(a), 164.312(b), 164.312(d), 164.312(e), 164.404, 164.406, 164.408, 164.502(a), 164.530(b), 164.530(c), 164.530(e), and 164.530(f), respectively.

OCR enforces federal civil rights laws which prohibit discrimination in the delivery of health and human services based on race, color, national origin, disability, age, sex, religion, and the exercise of conscience, and also enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules.

Please note that a covered entity may not use or disclose an individual's protected health information (PHI) without an authorization unless permitted or required by the Privacy Rule. Also, a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. In addition, prior to disclosing PHI to a business associate, a covered entity must enter into written contracts or other arrangements with the business associate to obtain satisfactory assurances that the business associate will appropriately safeguard the PHI. Additionally, a covered entity must: 1) ensure the confidentiality, integrity, and availability of all electronic PHI (ePHI)

the covered entity creates, receives, maintains, or transmits; 2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; 3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and 4) ensure compliance with the Security Rule by its workforce.

OCR is pleased that CBK has taken the following steps toward coming into compliance with HIPAA:

1) Upon learning of this incident, CBK conducted an investigation of the incident in consultation with an outside IT vendor and a forensic analysis firm. The investigation determined that a third party configuration of the CBK backup system left a port open on its firewall that allowed unauthorized access to the CBK's backup storage by an internet security researcher (the Researcher).

2) CBK closed the Rsync port thus terminating potential access to its ePHI by unauthorized individuals, and updated its firewall to add additional security measures.

3) CBK conducted a breach risk assessment of the four factors required by the Breach Notification Rule and determined that this incident did not constitute a breach as defined by the Breach Notification Rule because (a) the Researcher was the only individual who impermissibly accessed CBK's ePHI; (b) the Researcher was the only individual who impermissibly acquired CBK's ePHI; (c) the Researcher provided an affidavit stating that he securely deleted all of the CBK data in his possession, he retained no copies of the CBK data and did not share it with anyone else and did not use it for any purpose other than notifying CBK of this incident. OCR confirmed these details by reviewing the forensic analysis report of this incident and the Researcher's affidavit.

4) Subsequent to this incident, CBK implemented new HIPAA privacy, security, and breach notification policies and procedures, and trained its workforce members with respect to their requirements.

OCR has determined that the following corrective actions are needed to bring CBK into compliance with HIPAA:

1) Conduct an accurate and thorough Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Your Risk Analysis must take into account Administrative Safeguards, Physical Safeguards and Technical Safeguards and include your system wide IT infrastructure that creates, maintains, receives, and transmits ePHI including, but not limited to applications, software, databases, servers, workstations, mobile devices, medical devices, media, network administration and security devices, and associated business processes. Please note, an accurate and thorough risk analysis should be dated and performed periodically, as required under 45 C.F.R. §164.308(a)(1)(ii)(A) of the HIPAA Security Rule.

2) Based on CBK' review of its Risk Analysis, CBK will develop and implement a Risk Management Plan that addresses the process for managing and reducing the risks identified in the Risk Analysis to a reasonable and appropriate level. A Risk Management Plan should contain prioritized risks to CBK, options for mitigation of those risks, and a plan for implementation. The plan for implementation component of the Risk Management Plan should address: the risks (threat and vulnerability combinations) being addressed; security measures selected to reduce the risks; and implementation project priorities, such as required resources, assigned responsibilities, start and completion dates, and maintenance requirements.[1]

3) Ensure that in the event the affected patients or their personal representatives request an accounting of disclosures of PHI under 45 C.F.R. §164.528, CBK will include the impermissible disclosure of their PHI to Christopher Vickery.

4) Ensure that all information systems that create, maintain, receive, and transmit ePHI are patched up to date and supported by their respective developers.

5) Submit documentation to OCR within six (6) months of the date of this letter showing that the foregoing actions have been taken.

Based on the foregoing, OCR is closing this case without further action, effective the date of this letter. OCR's determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions regarding this matter, please contact Robert Chirila, Investigator, by email at robert.chirila@hhs.gov or by telephone at (212) 264-8900 (Voice), or (212) 264-2355 (TDD). Thank you for bringing this matter to our attention.

Sincerely,

Linda C. Colón
Regional Manager

[1] For additional guidance on the requirements of a Risk Analysis and Risk Management Plan, please refer to the following:
https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es;
https://www.healthit.gov/providers-professionals/security-risk-assessment