DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (800) 368-1019
TDD - (214) 767-8940, FAX - (214) 767-0432
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Southwest Region
1301 Young Street, Suite 1169
Dallas, TX 75202

SEP 28 2018

Patients Choice
Attn: Ara Dayian, MD, CEO
4801 South Buckner Blvd, Suite 200
Dallas, TX 75227

Re: OCR Transaction Number: 17-283246

Dear Dr. Dayian:

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), Southwest Region has completed its investigation pertaining to the breach notification report (the report) submitted by Patients Choice (Covered Entity), pursuant to the HITECH Breach Notification Rule, 45 C.F.R. § 164.408 and § 164.414. The report indicated possible noncompliance with certain aspects of 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, D, and E, the Privacy, Security, and Breach Notification Rules). Specifically, the report informed OCR that on November 19, 2016, an individual hacked into an FTP server, stole documents, and subsequently reported the incident to OCR himself.[1] The documents contained names, social security numbers, clinical, demographic, and financial information of patients at various Covered Entity locations. Approximately 3,547 individuals were affected by the breach.

The report indicated potential violations of 45 C.F.R. §§ 164.502(a) (Uses and Disclosures of PHI), 164.308(a)(l)(ii)(A) (Risk Analysis), 164.308(a)(l)(ii)(B) (Risk Management Plan), 164.308(a)(7)(ii)(A) (Data Backup Plan), 164.312(a)(2)(iv) (Encryption and Decryption), 164.312(d) (Person or Entity Authentication), 164.312(e)(1) (Transmission Security), 164.404 (Notification to Individuals), 164.406 (Notification to Media), and 164.408 (Notification to Secretary)

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.

Under the Privacy Rule, a covered entity may not use or disclose PHI, except as permitted or required by the Privacy Rule. *See* 45 C.F.R. § 164.502(a). The Security Rule requires that a covered entity conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it maintains and implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. *See* 45 C.F.R. §§ 164.308(a)(1)(ii)(A)-(B). A covered entity must also

[1] OCR opened an investigation into this complaint under Transaction Number 17-257655. In the complaint, the complainant alleged he discovered 1,069 scanned pdf files on a public FTP server belonging to Covered Entity. After receipt of the report, OCR closed Transaction Number 17-257655 and consolidated it with Transaction Number 17-283246.

implement procedures for creating and maintaining retrievable exact copies of electronic protected health information (ePHI). *See* 45 C.F.R. § 164.308(a)(7)(ii)(A).

Additionally, a covered entity must implement a mechanism to encrypt and decrypt ePHI. *See* 45 C.F.R. § 164.312(a)(2)(iv). Further, a covered entity must implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. *See* 45 C.F.R. § 164.312(d). A covered entity must also implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. *See* 45 C.F.R. § 164.312(e)(1).

By letters dated March 2, 2017, and January 26, 2018, OCR notified Covered Entity of its investigation into this matter.[2] In its responses to OCR from March 31, 2017 to September 21, 2018, and during a site visit by OCR, Covered Entity provided evidence of its internal investigation concerning the breach incident as well as extensive corrective action it has taken in response to the incident. The evidence revealed that at the time of the breach incident, Covered Entity's satellite offices utilized the involved FTP server to send billing documents to Covered Entity's Billing Department.[3] Covered Entity discovered that a contractor handling multiple hardware issues allowed the FTP server to accept anonymous logins while trouble shooting network errors. The contractor inadvertently failed to disable the anonymous login on the FTP server. Covered Entity ceased using the IT vendor that employed the involved contractor and hired a new IT vendor.

In response to this matter, Covered Entity took corrective actions, including, but not limited to, implementing additional technical safeguards to prevent similar breach incidents. For example, Covered Entity implemented encryption and firewall protection to ensure the security of its servers. Covered Entity no longer utilizes any FTP servers and billing documents are now accessed from a secure file server. Covered Entity also implemented intrusion detection and prevention software, which detects suspicious login activity. Additionally, Covered Entity updated its Privacy and Security policies and procedures to ensure full compliance with the Privacy and Security Rules. Further, with technical assistance from OCR, Covered Entity conducted an updated risk analysis and implemented a corresponding risk management plan. OCR recommends that Covered Entity update its risk analysis and risk management plan on an annual basis. See OCR's website for information regarding risk analysis: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

Covered Entity provided OCR sufficient documentation demonstrating that updated policies and procedures that it adopted during the course of the investigation comply with the applicable provisions of the Privacy and Security Rules as cited above. Moreover, Covered Entity provided OCR sufficient documentation showing that it trained workforce members accordingly on the updated policies and procedures.

Further, covered entities must have policies and procedures in place to comply with the Breach Notification Rule and must notify individuals, the Secretary and in some cases the media, about a breach of PHI. *See* 45 C.F.R. §§ 164.404-164.408. OCR verified that Covered Entity has adopted Breach Notification policies and procedures that comply with the requirements of the Breach Notification Rule specified at 45 C.F.R. §§ 164.404-164.408. OCR also verified that individual notification to affected individuals, notification to the Secretary, and notification to the media

---

[2] The March 2, 2017 notification was for OCR Transaction Number 17-257655, which, as previously noted, OCR closed and consolidated with OCR Transaction Number 17-283246.

[3] Workforce members scanned and faxed, via a pre-programed fax number on their computers, billing documents directly to the FTP server.

issued by Covered Entity included the requirements specified at 45 C.F.R. §§ 164.404 - 164.406; however, the notifications were untimely. Upon review, OCR also noted that Covered Entity's substitute notice did not include a brief description of the breach, the types of PHI involved in the breach, steps affected individuals should take to protect themselves from potential harm, and a brief description of what Covered Entity is doing to investigate the breach, mitigate the harm, and prevent further breaches. Further, the substitute notice did not include a toll-free number for individuals to contact Covered Entity regarding the breach. OCR, therefore, provided technical assistance to Covered Entity regarding Breach Notification requirements, including timeliness of notifications and requirements for substitute notice. Covered Entity re-educated appropriate workforce members on Breach Notification requirements specified at 45 C.F.R. §§ 164.404-164.408. Covered Entity provided OCR sufficient documentation of the aforementioned re-education.

Based on Covered Entity's responses, we have determined that no further OCR action is required at this time. Therefore, OCR is closing this case. OCR's determination as stated in this letter applies only to the issues in the aforementioned breach notification report that were reviewed by OCR. In addition, please note that, after a period of six months has passed, OCR may initiate and conduct a compliance review related to Covered Entity's compliance with the Privacy, Security, and Breach Notification matters raised in the breach notification report.

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.

[Contact information redacted by DataBreaches.net]