DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (415) 437-8310, (800) 368-1019
TDD - (415) 437-8311, (800) 537-7697
(FAX) - (415) 437-8329
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region IX
90 7th Street, Suite 4-100
San Francisco, California 94103

September 17, 2013

Ms. Siran Hagopian
Practice Specialist, Privacy and Security
Kaiser Foundation Health Plan, Inc.
Southern California Region
SCAL Regional Compliance and Privacy Office
393 E. Walnut St., 7nd Floor
Pasadena, CA 91188

Mr. Stephan Dean
44 700 Ronald St
Indio, CA 92201

Our Transaction Number: 12-141754

Dear Mr. Dean and Ms. Hagopian:

On April 5, 2012 the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a complaint filed by Mr. Stephan Dean (Complainant) alleging that Kaiser Permanente 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 Subpart D - Notification in Case of Breach of Unsecured Protected Health Information (45 C.F.R. §§ 164.400-164.414). The Complainant, a business associate of Kaiser Permanente, alleged that he was storing medical records for Kaiser Permanente from October 2008-August 2009, and that during this time Kaiser Permanente sent the Complainant several unencrypted e-mails containing patient protected health information, which included patient names, addresses, phone numbers, Social Security numbers, and diagnoses.

The Complainant stated that he has had several viruses on his computer that could have potentially exposed the information contained in the unencrypted e-mails to third parties. Complainant further alleged that the unencrypted e-mails have been stored on MSN servers for years. OCR investigated this complaint as a potential violation of 45 C.F.R. §§ 164.502, the use and disclosure standard of the Privacy Rule,164.530(c), the safeguards standard of the Privacy Rule, and 164.504(e), the business associate contracts standard of the Privacy Rule; 45 C.F.R. §§ 164.312(a)(2)(iv), the encryption and decryption standard of the Security Rule, 164.308(b)(1), the business associate contracts standard of the Security Rule, and 164.314(a), the business associate contracts standard of the Security Rule. OCR has concluded its investigation and has determined that all issues raised by the Complainant have been resolved through the voluntary compliance actions of Kaiser Permanente.

OCR enforces the Privacy and Security Rules, and also enforces Federal civil rights laws which prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and under certain circumstances, sex and religion.

The Privacy, Security, and Breach Notification Rules apply to covered entities, which include only: (a) a healthcare clearinghouse; (b) a health plan; or (c) a healthcare provider which transmits any health information in electronic form in connection with a transaction for which HHS has adopted standards.

In a letter dated April 17, 2013, OCR notified Kaiser Permanente about its investigation of this complaint. Ms. Siran Hagopian, Practice Specialist, Privacy and Security presented a response in a letter dated June 14, 2013. As part of its investigation of this complaint, OCR obtained and reviewed documentary evidence supplied by the Complainant and Kaiser Permanente.

Background

The Complainant stated that he was storing medical records for Kaiser Permanente from October 2008-August 2009, and that during this time Kaiser Permanente sent the Complainant several unencrypted e-mails containing patient protected health information, which included patient names, addresses, phone numbers, Social Security numbers, and diagnosis. The Complainant stated that he has had several viruses on his computer that could have potentially exposed the information contained in the unencrypted e-mails to third parties. The Complainant further alleged that the unencrypted e-mails have been stored on MSN servers for years.

In response to OCR's investigation, Kaiser Permanente reported that the Complainant's company began providing services to Kaiser Permanente in the fall of 2008. During this time Kaiser Permanente's medical records department sent some of the processing requests to the Complainant's company via unencrypted email. In June 2009, Kaiser Permanente and the Complainant's company entered into a business associate agreement (BAA). Pursuant to the terms of the BAA, the Complainant's company agreed to take appropriate steps to preserve all confidential information maintained in the records. Kaiser Permanente and the Complainant's company also signed a service agreement, in March 2010, in order to remove, prepare, deactivate, transport, store, and retrieve medical data for Kaiser Permanente and to comply with the existing BAA. Upon completion of the services, Kaiser Permanente sent a termination notice to the Complainant's company along with a request to return all of the medical records. The Complainant's company refused to allow Kaiser Permanente access to medical records, or return them. Kaiser Permanente and the Complainant's company later negotiated a transfer agreement in July 2010, in which the company agreed to take appropriate steps to preserve all confidential information including PHI. Kaiser Permanente also signed a settlement agreement with the Complainant's company, in July 2011, to resolve the outstanding disputes between the parties.

Pursuant to the agreements, the Complainant's company was required to maintain the confidentiality of Kaiser Permanente's PHI at all times. Kaiser Permanente was never informed of any data compromise or unauthorized release. However, after the settlement agreement had been executed, the Complainant informed Kaiser Permanente that his company was still in possession of emails containing PHI. Kaiser Permanente investigated and found that a former employee sent the emails to the Complainant's company with unencrypted electronic protected health information (EPHI). Kaiser Permanente stated that the employee's actions were in direct

violation of Kaiser Permanente's policies and procedures. Kaiser Permanente reported that the employee, who sent the unencrypted EPHI to the complainant, is no longer with the company. The employee violated Kaiser Permanente's's EPHI security and confidentiality policies and did not notify her managers about the incident.

Kaiser Permanente immediately demanded the return or destruction of EPHI that was in possession of the Complainant's company. Kaiser Permanente offered to engage a third party IT expert to assist in this endeavor. The Complainant's company refused any such offers unless Kaiser Permanente paid the Complainant's company. The Complainant's company also refused all Kaiser Permanente's request for return, disposal and access to EPHI. Because of its conduct and refusal to comply with Kaiser Permanente's demands for the return and destruction of the EPHI, Kaiser Permanente filed a civil lawsuit against the Complainant's company. During the course of litigation, the Complainant filed declarations and testified that they have deleted all PHI in their possession including any email. Kaiser Permanente has requested the right to inspect any device in the possession of the Complainant's company that stored any PHI. As of June 14, 2013, the issue is still pending with the court in the litigation.

Privacy Rule

Under the Privacy Rule, a covered entity, such as Kaiser Permanente, may not use or disclose protected health information except as permitted by the Rule.[1] In general, a covered entity must obtain a valid authorization from the individual to disclose protected health information for purposes other than treatment, payment, or healthcare operations.[2] A covered entity must also have in place appropriate procedural, administrative, and technical safeguards to protect the privacy of protected health information against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures.[3] Also, the Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate.[4]

In this case, OCR was unable to substantiate that any protected health information was impermissibly disclosed. Specifically, there was no evidence that the emails were disclosed to unauthorized third parties and Kaiser Permanente was never informed of any data compromise or unauthorized release. Also, Kaiser Permanente provided the signed BAA with the Complainant's company, which meets the requirements of the Privacy Rule. Lastly, Kaiser Permanente has the appropriate safeguards in its HIPAA policies to prevent the impermissible use or disclosure of protected health information to unauthorized third parties.

---

[1] 45 C.F.R. § 164.502(a).
[2] 45 C.F.R. § 164.502(a)(1)(ii).
[3] 45 C.F.R. § 164.530(c).
[4] 45 C.F.R. § 164.504(e)(1).

In an effort to voluntarily comply with the Privacy Rule, Kaiser Permanente reported the following corrective actions:

- Provided HIPAA compliance training to its workforce members and the training material covers topics related to EPHI security, encryption and stronger password controls.

Security Rule

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of EPHI.[5] According to the Security Rule, a covered entity is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.[6] Also, the Security Rule requires that a covered entity obtain satisfactory assurances from a business associate that creates, receives, maintains, or transmits EPHI on the covered entity's behalf that the business associate will appropriately safeguard the information.[7]

In this case, the signed BAA met the requirements of the Security Rule. Specifically, it contained the provisions for security safeguard implementation and requirements of return and disposal of PHI after the termination of the contract. Also, Kaiser Permanente provided its *Email and Secure Messaging* Policy which requires that all email containing EPHI must be encrypted. Lastly, Kaiser Permanente's HIPAA compliance training material covers the topic of email encryption.

Conclusion

All Issues raised by the subject complaint at the time it was filed have been resolved through Kaiser Permanente's voluntary compliance. OCR is, therefore, closing this complaint. OCR's determination as stated in this letter applies only to the allegations in this complaint that OCR reviewed.

Advisements

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 Megan Yelorda, OCR Investigator, at (213) 534-1436 (Voice) or by e-mail at Megan.Yelorda@hhs.gov. Please be advised that communication by unencrypted e-mail presents a risk of disclosure of the transmitted information to, or interception by, unintended third parties. Please keep this in mind

[5] 45 C.F.R. §§ 164.308-318.
[6] 45 C.F.R. § 164.308(a)(6)(ii).
[7] 45 C.F.R. § 164.308(b)(1).

when communicating with us by e-mail. When contacting this office, please remember to include the reference number that we have given your file. That number is located in the upper left-hand corner of this letter.

Sincerely,

Michael Leoz
Regional Manager