Chaplaincy
HEALTH CARE

HOSPICE CARE | PALLIATIVE CARE | GRIEF CARE | BEHAVIORAL HEALTH

Email Breach Incident Questions and Answers

Question: When did this occur and when was it resolved?

Answer: On November 20, 2018 an unknown individual gained access to one email account. The issue was quickly identified and resolved the same day. The password on the email account was quickly changed which limited the access to approximately four hours.

Question: What information was accessed?

Answer: The computer forensic firm we hired to investigate believes that the unknown individual was interested in gaining access to more email accounts to further their Phishing tactics to obtain bank and payment information. While it is not possible to identify which, if any, emails were seen, it was found that they could include the patients' name, date of birth, medical record number, masked social security numbers (xxx-xx-1234), prescriptions, dates of service and home address. Complete social security numbers, financial records, and credit card information were not included in the emails.

Question: Did the breach impact healthcare records?

Answer: No, the Electronic Health Records (EHR) system was not accessed. The breach only included one employees' email account.

Question: Who can I talk to about this?

Answer: You can call our Privacy Officer toll-free at (855) 659-8793 between the hours of 8 a.m. and 5 p.m., Monday to Friday Pacific Time; send an e-mail message to Privacy@chaplaincyhealthcare.org; visit our website ChaplaincyHealthCare.org/News; or by letter to Privacy Officer, Chaplaincy Health Care, 1480 Fowler St, Richland, WA 99352.

Question: Were birth dates and social security numbers viewed?

Answer: While it's not possible to know if a date of birth or social security number was actually viewed, the limited social security numbers included in the emails were all presented in a masked format (xxx-xx-1234).

Question: The patient has passed away, should anything be done?

Answer: The IRS recommends that you send copies of the death certificate to the IRS and to each of the credit reporting bureaus. Specific information about how to do this is available on the IRS.gov website, search for "Protecting the deceased's identity". If you are a surviving spouse, feel free to register with LifeLock.

Question: What has Chaplaincy Health Care done in response to this event?

Answer: We have undertaken several steps:

- We required a mandatory password reset on the day of the breach across the agency.
- We are upgrading our systems to include more security features and implementing two factor authentications.

- We have provided additional awareness training to all employees about authorized methods to send or receive Protected Health Information. We have provided educational information to staff about phishing emails and the staff has reaffirmed their awareness and understanding of password security, internet usage and related policies.
- We have added a banner to identify all emails that originate outside of the organization, to improve staff awareness.
- We have filed documents with the Office of Civil Rights and the Washington State Attorney General as required.
- We have sent letters to those individuals potentially impacted by this event and we are offering free identity and credit monitoring for one year.

We continue to use our mandatory complex password reset policy and will continue with mandatory training.

Question: How many people were impacted by this breach?

Answer: The investigation has revealed that approximately 1,086 individuals were potentially impacted by this event.

Question: I have donated to Chaplaincy Health Care, is my information included in the breach?

Answer: No. Donor related information was not included in any of the emails that were breached.