The Tavistock and Portman NHS
NHS Foundation Trust

Freedom of Information Act 2000 disclosure log entry

Reference

18-19314

Date sent

14/01/2019

Subject

IG Security and Training

Details of enquiry

1. Does the organisation have training that covers:
   a. Recognising and reporting Phishing emails
   b. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)
   c. Disposal of confidential information
   d. Dangers of using USB sticks being given away or finding one that looks like it has been dropped
2. Does the organisation allow the use of USB sticks?
3. Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, ie finance, execs etc)?
4. Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit?
   Can you also answer relating to the audits:
   a. Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc?
   b. Would an audit ever be carried out unannounced?
   c. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.
   d. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.
5. Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?
6. Does the organisations Exec board receive board level training relating to Cyber Awareness?
7. How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable):

a. Third party application package	☐
b. Third party Trainer / class room	☐
c. eLearning for Health Data Security Awareness	☐
d. In house developed package	☐
e. Combination of any of the above	☐

Response Sent

1. Does the organisation have training that covers:
   a. Recognising and reporting Phishing emails
      Yes
   b. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)
      Yes, We have guidance posters supporting this.

c. Disposal of confidential information
Yes

d. Dangers of using USB sticks being given away or finding one that looks like it has been dropped
Part of Trust Data Security Training. All USB are encrypted before use.

2. Does the organisation allow the use of USB sticks?
Yes, but must be encrypted

3. Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, ie finance, execs etc)?
Yes

4. Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit?
Yes

Can you also answer relating to the audits:

a. Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc?
Yes, Manager/Head or Director would be aware

b. Would an audit ever be carried out unannounced?
Yes, Spot Checks, occasionally

c. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.
We have an Information Management Audit which covers Records Management, Confidentiality and Data Quality which is completed every year by at least two area of the Trust's business. It is a internal document.

d. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.
Yes, results are recorded and returned to the Data Security and Protection Manager.

5. Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?
Yes

6. Does the organisations Exec board receive board level training relating to Cyber Awareness?
Yes, Every member of staff irrespective of their role is required to complete Data Security Awareness Training.

7. How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable):

a. Third party application package	☐
b. Third party Trainer / class room	☐
c. eLearning for Health Data Security Awareness	Yes ☐
d. In house developed package	Yes ☐
e. Combination of any of the above	Yes ☐