Lancashire & South Cumbria NHS Foundation Trust

FOI Request Response information

FOI request reference:	2019/007
Date request received:	06/01/2019
Date request responded to:	14/01/2019
Category:	IM&T
Tags:	Training, phishing, confidential, USB, data, security, protection, toolkit, audit, policy, procedure, cyber, awareness, board, waste,

Request Detail:

1. Does the organisation have training that covers:
    1. Recognising and reporting Phishing emails
    2. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)
    3. Disposal of confidential information
    4. 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:
    1. Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc?
    2. Would an audit ever be carried out unannounced?
    3. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.
    4. 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?

NHS
Lancashire & South Cumbria
NHS Foundation Trust

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 Detail:

1. Does the organisation have training that covers: Yes to all 4
    1. Recognising and reporting Phishing emails
    2. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)
    3. Disposal of confidential information
    4. 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? Yes, encrypted managed devices only

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:

    1. Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc? With all appropriate managers and directors.
    2. Would an audit ever be carried out unannounced? Yes it is possible
    3. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy. Yes, this forms part of our ISMS and we will therefore not supply as it may compromise our security.

4. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy. Yes, this forms part of our ISMS and we will therefore not supply as it may compromise our security.

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

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