

14 January 2019

Freedom of Information Request – Ref: FOI 285-1819

Thank you for your recent Freedom of Information request. Please find the Trust's response below.

1. Does the organisation have training that covers:
 1. Recognising and reporting Phishing emails **Yes, within the annual IG refresher training - Data Security Awareness level 1**
 2. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc) **As above**
 3. Disposal of confidential information **As above**
 4. Dangers of using USB sticks being given away or finding one that looks like it has been dropped **As above**
2. Does the organisation allow the use of USB sticks? **Only approved encrypted 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)? **No. All staff receive training as described above**
4. Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit? **Audits are undertaken where there is a concern that unauthorised access to a clinical record has taken place. Periodic audits of confidential waste disposal processes also take place. Policies are subject to review at least every three years**

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? **Clinical records audits are undertaken centrally by the IG Officer. Confidential waste audits are undertaken by senior managers in the Estates Department.**
2. Would an audit ever be carried out unannounced? **No**
3. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy. **There is no documented procedure**
4. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy. **Results are not documented, but a confirmation is provided to the relevant team manager as to whether unauthorised access has taken place or not.**
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, Board members complete the IG refresher training as described above**

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. <i>Third party application package</i>	<input type="checkbox"/>
b. <i>Third party Trainer / class room</i>	<input type="checkbox"/>
c. <i>eLearning for Health Data Security Awareness</i>	<input checked="" type="checkbox"/>
d. <i>In house developed package</i>	<input type="checkbox"/>
e. <i>Combination of any of the above</i>	<input type="checkbox"/>

Yours sincerely,

Lisa Evans

LISA EVANS
Information Governance Officer
2gether NHS Foundation Trust

Copyright & Reuse of Public Sector Information

The information and material that is routinely published is subject to 2gether NHS Foundation Trust's copyright unless otherwise indicated. Unless expressly indicated on the material to the contrary, it may be reproduced free of charge in any format or medium, provided it is reproduced accurately and not used in a misleading manner. Where any of the copyright items are being re-published or copied to others, you must identify the source of the material and acknowledge the copyright status. Permission to reproduce material does not extend to any material accessed through the Trust website that is the copyright of third parties. You must obtain authorisation to reproduce such material from the copyright holders concerned. For further guidance on a range of copyright issues, see the Office of Public Sector Information (OPSI) web site: www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/index.htm

or write to: OPSI, 102 Petty France, London SW1H 9AJ.