

22 February 2018

Freedom of Information Request – Ref: FOI 275-1718

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

1. Does your organisation adhere to the Network Security guidance outlined by the National Cyber Security Centre, within its '10 Steps to Cyber Security'?
 - Yes
2. Do you ensure that security patches for critical vulnerabilities are routinely patched within 14 days, as recommended by the National Cyber Security Centre?
 - No

The Trust aims to apply all critical patches as per NCSC guidelines, where the application of a critical patch to the operational environment can be tested and applied in such a manner as not to compromise the Confidentiality, Integrity or Availability of Trust information assets; however, with such a vast and disparate estate this is not always achievable within 14 days. Moreover, certain applications/business systems will function only with specific versions of browsers, plugins and supporting software, so updates are not possible (and indeed suppliers often only warrant specific configurations). It is for this reason we apply a 'defence-in-depth' approach, which is to say that we don't rely on any one toolset to provide protection. We also, as part of NCSC '10 steps to cyber security' apply the following controls:

- employ complex passwords;
- don't allow admin accounts to access the internet;
- don't allow users to install applications;
- scan for malicious content with Anti-Virus/Malware solutions;
- control web and email traffic;
- apply additional intrusion prevention measures;
- perform penetrations tests;
- carry out exercises to test cyber readiness;
- ensure that our users are properly trained and aware of cyber risks.

It's a balancing act – ultimately a risk assessment against the perceived threat and keeping business applications up & running. A good example would be the latest Intel Meltdown & Spectre vulnerabilities: the fix proved to be more of a threat to operations than the vulnerability itself, causing many organisations to deal with a loss of information asset availability and roll back the patch and await version 2.

3. Have you suffered from any service outages on your network in the last two years, however small?
 - Yes
4. Did any of these outages cause a loss, reduction or impairment to your organisation's delivery of essential services?
 - Yes

5. Was the root cause of the service outage identified and confirmed – at the time or afterwards?
 - o Yes

6. Is it possible that any service outages you have suffered in the last two years was caused by a cyber attack – such as ransomware, DDoS attack, or malware?
 - o Yes

7. Are you aware that Distributed Denial of Service (DDoS) attacks are a significant contribution to service interruptions, outages and downtime?
 - o Yes

Should you have any queries in relation to our response in this letter, please do not hesitate to contact me. If you are unhappy with the response you have received in relation to your request and wish to ask us to review our response, you should write to:-

Anna Hilditch
Assistant Trust Secretary,
2gether NHS Foundation Trust
Rikenel
Montpellier
GLOUCESTER GL1 1LY
Tel: 01452 894165
E-mail: anna.hilditch@nhs.net

If you are not content with the outcome of any review, you may apply directly to the Information Commissioner's Office (ICO) for further advice/guidance. Generally, the ICO will not consider your case unless you have exhausted your enquiries with the Trust which should include considering the use of the Trust's formal complaints procedure. The ICO can be contacted at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

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.