The Clatterbridge Cancer Centre
NHS Foundation Trust

Clatterbridge Road
Bebington
Wirral
CH63 4JY

Tel: 0151 556 5000
Web: www.clatterbridgecc.nhs.uk

Date: 16 February 2022

Re: Freedom of Information Request
Ref: 18-2022

Thank you for your email dated the 21/1/22, requesting information in relation to various topics.

The information that you require is as follows:

How many staff do you employ?
As of 31st December, 1632 staff

Do you have a critical care function? **The Clatterbridge Cancer Centre (CCC) NHS Foundation Trust has a Service Level Agreement (SLA) with Liverpool University Hospitals Foundation Trust (LUHFT) for critical care. The LUHFT team attend handover in a morning and are available at handover in an afternoon. They provide review to CCC patients within the same timeframe as for LUHFT patients. They will review patients and, if deemed appropriate, patients will be moved to HDU or ITU care.**

Are you actively involved in/contributing to ICS level initiatives?
The Clatterbridge Cancer Centre (CCC) NHS Foundation Trust plays an active role in the Cheshire and Merseyside Health and Care Partnership. We host the Cheshire and Merseyside Cancer Alliance and our Chief Executive Officer is the alliance's Senior Responsible Officer.

Members of the CCC team represent the trust at a wide range of Cheshire and Merseyside forums, most notably the Cheshire and Merseyside Acute and Specialist Trust Provider Collaborative.

This active engagement has also led to CCC's further involvement in the work of the Health and Care Partnership, including for example leading the ICS's programme for the development of Community Diagnostic Centres in line with national diagnostic policy.

How many desktop devices do you have in the Trust? **VDI – 407, Desktop PC – 517, Laptop – 799 & 282**

What makes & models are most used? **VDI – iGel, Desktop PC – Fujitsu Esprimo – multiple models, Laptop – Dell, Toshiba**

What is your main web browser? **IE11**

How many trust mobile devices do you have? (phones/tablets) **1272 = 867 phones and 405 tablets**

What are the main makes and models? **Samsung, various A series**

As a whole, does the Trust favour Apple or Android devices? **Android mobile devices**

Are employees encouraged to use their personal devices for work? **No**

Do you use an MDM solution to manage devices? **Yes, Vodafone VDSM**

Who is your Internet provider? **Virgin Media**

Do you have any known Wifi dead zones? **Yes**

Who is your cellular provider? **Yes**

Do you have known cellular coverage dead zones? **Yes**

Do you use pagers/bleeps? **Yes**

Who is your current pager/bleep service provider? **Stanley currently supply the pager/critical bleep solution in the Trust**

Do you rely on commercial apps such as whatsapp to communicate internally? **No**

Which commercial/external apps do you use? **Microsoft Teams**

Do you use any of the following supplier's services: Careflow Connect, Hospify, Vocera, Ascom, Multitone, Netcall? **No**

Do you use any software to manage tasks at night? If yes, what software do you use?
There is an electronic handover system embedded into MediTech, which is used throughout the evenings, nights, and weekends. Throughout the week, jobs are handed over to teams at 9am, 4pm and 9pm. E-handover is setup for all days and once rolled out to nursing staff is anticipated to be used daily.

If not, how do you manage your tasks at night (word of mouth, whiteboard etc)?

Which roles are responsible for managing the workload at night?
There are deputy ward managers on each night shift on each ward, two advanced nurse practitioners (ANPs), a resident junior doctor, a resident solid tumour registrar, a non-resident haemato-oncology speciality registrar, and non-resident oncology and haemato-oncology consultants on call for advice who are able to attend if needed. All ANPs and doctors are trained in Advanced Life Support.

Which authentication protocol(s) do you use (ie. SAML, O Auth 2, OIDC)?

Section 31(1a): The prevention or detection of crime of the Freedom of Information Act 2000

We have carefully considered your request and although we hold the information within the Data Protection Impact Assessment, we have concluded that we will not be able to provide you with this information and we will rely on the exemption under Section 31(1a) - The prevention or detection of crime of the Freedom of Information Act 2000 ("the Act").

Section 31(1a) the Act provides that information is exempt from disclosure if the information would or would be likely to prejudice law enforcement and the prevention or detection of crime by making the Trust vulnerable to criminal activity through cyber security attacks.

The Trust, as a public body is mindful that in order to engage this exemption, we must demonstrate that disclosure of the information would, or would be likely to, prejudice the prevention of crime.

The term "would …prejudice" has been defined as it is more likely than not to occur whereas "would likely…. prejudice" is a lower threshold. The Trust has applied the prejudice test under Section 31, and we are content that the requirements of the test have been met.

Having reached the conclusion that the prejudice test has been met, we have also considered whether the public interest in maintaining the exemption outweighs the public interest in disclosure.

Public Interest Test

Factors favouring disclosure

- **The Trust recognises that providing the information would promote openness and transparency with regards to the Trust's IT security**

Factors in favour of non-disclosure

- **Increased risk of Cyber-attacks, which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018. Cyber-attacks are rated as a Tier 1 threat by the UK Government. Cyber-attacks could result in:**
  - **Breaches in Trust security and is therefore a reasonable threat to the confidential patient/staff/public data held on our systems**
  - **Temporary or long-term lack of availability of IT systems**
  - **Corruption/loss of patient data which would prevent or interrupt provision of patient care**

Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities

Having carefully considered the public interest test we have concluded that there is a strong public interest in protecting the confidentiality of patient/staff/public data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access.

Taking the above into consideration, having applied the necessary, relevant tests and taking all the current circumstances into consideration we are content that the requirements of all necessary and relevant tests have been met and the application of the exemption under Section 31(1a) is appropriate on this occasion.

What PAS/EPR system do you use?
The current supplier of our Electronic Patient Record (EPR) is Meditech 6.08.42.

Do you have APIs to integrate with the PAS/EPR? **Yes**

Do you use Business Intelligence software? If so, what?
Microsoft Power BI

Do you raise alerts/send emails triggered by data? If yes, please provide any examples you can.
Yes, environmental alerts, air conditioning, uninterrupted power supplies

Do you have other mechanisms to raise an alert/alarm other than a bleep? If yes, please specify examples **Yes, PRTG for network and server monitoring**

Should you require any further information please do not hesitate to contact me on the email address provided below.

Please remember to quote the reference number above in any future communications.

If you are dissatisfied with the handling of your request, you have the right to ask for this to be investigated internally.

If you are dissatisfied with the information you have received, you have the right to ask for an internal review.

Both processes will be handled in accordance with our Trust's Freedom of Information Policy and the Freedom of Information Act 2000.

Internal investigation and internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Freedom of Information Review, The Clatterbridge Cancer Centre NHS Foundation Trust, Clatterbridge Road, Bebington, Wirral, CH63 4JY

If you are not satisfied with the outcome of the internal investigation/review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

In order for us to ensure customer satisfaction and to monitor compliance with the Freedom of Information Act 2000, we would be grateful if you could take a couple of minutes to complete a short feedback form via the link below:

https://www.surveymonkey.co.uk/r/H39RFMM

Kind Regards,

Margaret Moore

Information Governance Administrator
Contact Email: ccf-tr.foi@nhs.net