East Sussex Healthcare
NHS Trust

FOI REF: 25/870

30th December 2025

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD

Tel: 0300 131 4500
Website: www.esht.nhs.uk

FREEDOM OF INFORMATION ACT

I am responding to your request for information under the Freedom of Information Act. The answers to your specific questions are as follows:

1. **A list of all external suppliers, contractors, or partner organisations who currently fall within the remit of the NHS Data Security & Protection Toolkit (DSPT) for your organisation.**

   This includes any supplier that handles patient data, accesses NHS systems, or provides digital, software, cloud, data-processing, or cyber-security services requiring DSPT compliance.

   Under Section 31(1)(a) of the Freedom of Information Act (FOIA), the Trust can confirm that it holds information relevant to your request, however, we are unable to disclose it for the reasons explained below.

   Historically, we would disclose information relevant to the Trust's IT systems, infrastructure and software as part of our transparency agenda under the terms of the Freedom of Information Act (FOIA). However, in light of the recent cyber-attacks on NHS hospitals and the serious impact these have had on patient services and the loss of patient data, we are having to reconsider this approach. Please see several links to news articles about these recent cyber incidents provided below for your information.

   - *NHS England — London » Synnovis Ransomware Cyber-Attack*
   - *NHS England confirm patient data stolen in cyber attack - BBC News*
   - *Merseyside: Three more hospitals hit by cyber attack - BBC News*

   As a result of these attacks, thousands of hospital and GP appointments were disrupted, operations were cancelled, and confidential patient data was stolen which included patient names, dates of birth, NHS numbers and descriptions of blood tests.

   When we respond to a Freedom of Information request, we are unable to establish the intent behind the request. Disclosure under the FOIA involves the release of information to the world at large, free from any duty of confidence. Providing

information about our systems or security measures to one person is the same as publishing it for everyone. While most people are honest and have no intention of misusing information to cause damage, there are criminals who look for opportunities to exploit system weaknesses for financial gain or to cause disruption.

In the context of the FOIA, the term ‘’public interest’’ does not refer to the private or commercial interests of a requestor; its meaning is for the “public good”. The Trust receives a significant number of requests each year regarding our IT systems, infrastructure and cyber security measures. Most of these requests are commercially driven and serve no direct public interest. Information relevant to our IT portfolio is often requested by consultancy companies who then pass on this information to their client base. Many of these requests are submitted through the FOI portal whatdotheyknow.com who publish our responses, making this information available to an even wider audience.

As a large NHS Trust we hold extensive personal data relevant to our patients and staff, much of which is considered very sensitive. A lot of this information is held electronically on various administration and clinical systems. We have a duty under the Data Protection Act 2018 and the UK GDPR to protect this personal information and take all necessary steps to ensure this data is kept safe. This means not disclosing information that could allow criminals to gain unlawful access to our systems and infrastructure. The Trust can be heavily fined should it be found to have acted in a negligent way which results in a personal data breach. We need to demonstrate that we comply with our legal obligations under data protection and freedom of information legislation, but we must be careful that too much transparency does not result in harm to our patients or staff, or cause disruption to our services.

Moreover, under the Network and Information Systems (NIS) Regulations Act 2018, operators of essential services such as NHS organisations like ours have a legal obligation to protect the security of our networks and information systems in order to safeguard our essential services. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in section 10 of the Network and Information Systems Regulations 2018. Should we not comply with these requirements regulatory action can be taken against the Trust. Further information about the Network and Information Systems (NIS) Regulations Act 2018 can be found here – The Network and Information Systems Regulations 2018: guide for the health sector in England - GOV.UK

Your request asks for specific details regarding our suppliers and contractors which, for the reasons explained above, would be inappropriate to release into the public domain. If disclosed, it is possible that patient data as well as other confidential information would be put at risk. Such disclosure could also impact on the security of our systems and result in serious disruption to the health services we deliver to the local community. Section 31(1)(a) of FOIA provides that information is exempt if its disclosure would, or would be likely to, prejudice (a) the prevention or detection of crime. In this case, disclosure would be likely to prejudice the prevention of crime by enabling or encouraging malicious acts which could compromise the Trust’s IT systems and infrastructure. The Trust’s capacity to defend itself from such acts relates to the purposes of crime prevention and therefore section 31(a) exemption is applicable in these circumstances. For these reasons, the Trust considers disclosure of the information you are seeking to be exempt under section 31(1)(a)

[*law enforcement*] of the FOIA and the information requested is being withheld for this part of your request. The full wording of section 31 can be found here: Freedom of Information Act 2000

Section 31 is a *qualified* exemption and therefore we must consider the prejudice or harm that may be caused by disclosure of the information you have requested, as well as apply a public interest test that weighs up the factors in maintaining the exemption against those in favour of disclosure.

In considering the prejudice or harm that disclosure may cause, as explained should the Trust release information into the public domain which draws attention to any weaknesses relevant to the security of our systems or those of a supplier, this information could be exploited by individuals with criminal intent. Increasing the likelihood of criminal activity in this way would be irresponsible and could encourage malicious acts which could compromise our IT systems or infrastructure, result in the loss of personal data and/or impact on the delivery of our patient services. We consider these concerns particularly relevant and valid considering the increasing number of cyber incidents affecting NHS systems in recent years and the view by government, the ICO and NHS leaders that the threat of cyber incidents to the public sector is real and increasing.

- Organisations must do more to combat the growing threat of cyber attacks | ICO

In the Government's Cyber Security Strategy 2022-2030, the Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office states on page 7:

"Government organisations - and the functions and services they deliver - are the cornerstone of our society. It is their significance, however, that makes them an attractive target for an ever-expanding army of adversaries, often with the kind of powerful cyber capabilities which, not so long ago, would have been the sole preserve of nation states. Whether in the pursuit of government data for strategic advantage or in seeking the disruption of public services for financial or political gain, the threat faced by government is very real and present.

Government organisations are routinely and relentlessly targeted: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating."

With this in mind, we then considered the public interest test for and against disclosure. It should be noted that the public interest in this context refers to the public good, not what is 'of interest' to the public or the private or commercial interests of the requester. In this case we consider the public interest factors in favour of disclosure are:

- Evidences the Trust's transparency and accountability
- Provides information relevant to the IT systems and applications the Trust uses

- Reassures the public and partners that the Trust procures these systems in line with Procurement legislation

- Reassures the public and partners that the Trust's IT infrastructure and systems are secure

Factors in favour of withholding this information are:

- Public interest in crime prevention

- Public interest in avoiding disruption to our health services

- Public interest in maintaining the integrity and security of the Trust's systems

- Public interest in the Trust avoiding the costs associated with any malicious acts (e.g. recovery, revenue, regulatory fines)

- Public interest in complying with our legal obligations to safeguard the sensitive confidential information we hold

In considering all of these factors, we have concluded that the balance of public interest lies in upholding the exemption and not releasing the information requested. Although disclosure would provide transparency about our software systems and IT infrastructure, this is outweighed by the harm that could be caused by people who wish to use this information to assess any vulnerabilities in our security measures and consequently use this information for unlawful purposes. Cybercrime can not only lead to major service disruption but can also result in significant financial losses. As a publicly funded organisation, we have a duty for ensuring our public funding is protected and spent responsibly. Moreover, as a public body the Trust must demonstrate that it keeps its confidential data and IT infrastructure safe and complies with relevant legislation, but at the same time we must be vigilant that transparency does not provide an opportunity for individuals to act against the Trust. In considering the impact that recent cyber-attacks have had on NHS services, including the cancellation of thousands of patient appointments and procedures as well as the loss of confidential patient data, we consider the overriding public interest lies in withholding this information. The private or commercial interests of a requester should not outweigh the public interest in protecting the integrity of our systems and continuity of our essential patient services. Although we appreciate there may be legitimate intentions behind requesting this information, we must take a cautious approach to requests of this nature and appreciate your understanding in this matter.

It is important to note that the Trust and its commissioning partners are required to follow very specific rules when procuring equipment or services. Information about procurement and tendering can be found on our website – Governing documents, incorporating: Standing Orders, Standing Financial Instructions, Scheme of Delegation.

To contact the Procurement Service, please email - esht.procurement@nhs.net.

Cont…/

2. **A list of any new, incoming, or planned suppliers (contracted or due to go live within the next 12 months) who will fall within the DSPT remit for the same reasons.**

Section 31 applied, please see Q1.

3. **For each supplier identified in Q1 or Q2, please confirm (if recorded):**

   a. **Whether they are required to maintain a "Standards Met" DSPT submission**

   As per the NHS guidance (Link: Data Security and Protection Toolkit) All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

   b. **The date you last checked or verified their DSPT status (or expected verification date for new suppliers)**

Section 31 applied, please see Q1.

4. **Does your organisation maintain an internal register or log of DSPT-relevant suppliers (including planned or onboarding suppliers)?**

   If yes, please provide the relevant extract.

   If no, please confirm that no such register exists.

Section 31 applied, please see Q1.

If I can be of any further assistance, please do not hesitate to contact me.

Should you be dissatisfied with the Trust's response to your request, you have the right to request an internal review. Please write to the Freedom of Information Department (esh-tr.foi@nhs.net), quoting the above reference, within 40 working days. The Trust is not obliged to accept an internal review after this date.

Should you still be dissatisfied with your FOI request, you have the right of complaint to the Information Commissioner at the following address:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Telephone: 0303 123 1113

Yours sincerely

Freedom of Information Department
esh-tr.foi@nhs.net