Reference: FOI.ICB-2526/070

Subject: HSCN Connectivity (Health and Social Care Network) and Connectivity (SD/WAN, LAN, WIFI)

I can confirm that the ICB does hold some of the information requested; please see responses below:

QUESTION	RESPONSE
1. HSCN connectivity (Health and Social Care Network) a. Please can advise who is the existing supplier b. Contract end dates c. Total contract value d. Which framework this was purchased under e. Name of the contact responsible for this	1a. and 1b. The ICB has applied Section 24 (Safeguarding National Security) to questions 1a and 1b. Disclosing the existing supplier and contract dates would make the local healthcare systems vulnerable to cyberattack. Section 24 is a qualified exemption and subject to a public interest test. This has been outlined below. 1c. £350,000 1d. Crown Commercial Solutions Dynamic Purchasing System 1e. This is completed by our ICB Digital Lead: bnssg.digital@nhs.net
	Public Interest test for Section 24 application The ICB believes that disclosure of the information would leave local health care IT services and particularly the HSCN vulnerable to cyberattack. The exemption has been considered in more detail below: Public interest arguments in favour of disclosing the information:

	The public interest arguments in favour of disclosing the information took into account the FOIA definition of where there is a public interest as well as the legal framework for public authority procurements as set out in the Public Contracts Regulations 2015. These Regulations require the ICB to conduct all procurement activity openly and in a manner which enables behaviour to be scrutinised. The ICB maintains a contract register which outlines supplier details and contract costs and this is available on the ICB website. The ICB understands that there will be a public interest in any supplier of public services, particularly in highly competitive areas, where value for money is paramount. The HSCN contains highly sensitive, personal special category data and therefore there is a local public interest for residents of BNSSG in knowing the supplier to understand which company is facilitating the storage and transfer of their personal data. In the wider context, as these services can be provided on a national footprint, other suppliers would have an interest in the information in readiness to bid for the contract during a procurement process. <u>Public interest arguments in favour of maintaining the exemption:</u> By disclosing the name and contract end date, the ICB believes that this would make these healthcare systems vulnerable to cyberattack as targeted attacks could take place. Cyberattacks cannot be predicted but particularly within the NHS should be expected. Health providers are a known target for cyberattacks due to the large

	amounts of confidential and personal data held and this data can be sold for significant amounts of money. Cyberattacks to these systems could result in data breaches, healthcare providers not having access to patient data or the systems required to provide care, and costs to the ICB related to emergency measures or equipment repairs. Patient health and care would be negatively affected if there was an attack on the HSCN. Fines may also be applied for any data breaches if the ICB was found not to have managed the risk appropriately. Data breaches would likely have a negative impact on the wellbeing of those affected particularly as health data is so sensitive for patients. These healthcare systems also play a vital role in the wider local socio-economic landscape and support organisations wider than health such as local authorities. These organisations and their staff would also be negatively affected by any cyberattacks to the HSCN. The GDPR requires organisations to process personal data securely and "…ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." As part of this, organisations are expected to have measures in place to protect against cyberattack. Training has been provided to ICB staff which has alerted staff to possible disclosures which may be detrimental to cyber security. Disclosure of the supplier of the HSCN has been identified as one of the areas of risk.

	The ICB has exempted the answers to question 1a and 1b but has answered the remaining questions, including the question regarding cost. This is an area of significant interest for the public as the NHS is publicly funded and therefore there is specific interest in the costs of contracts. <u>Public Interest Test</u> Under the Network and Information Systems (NIS) regulations, ICBs are considered “operators of essential services” in the health sector. This means ICBs are responsible for ensuring the security of the network and information systems which support essential healthcare systems such as infrastructure for healthcare providers. The ICBs must take appropriate action to manage risk, prevent incidents and ensure service continuity. The ICB believes that applying Section 24 to questions 1a and 1b manages this risk appropriately in line with ICB responsibilities. The ICB has considered the public interest in the information and weighed the risk of cyberattacks against this. The ICB has applied a risk based approach to the application of Section 24 and considered: • the general public interest in NHS contracting • the specific interest in the supplier and contract end date for local residents and businesses • that the exemption only applies to 2 questions

	• the significant threat of cyberattack to the NHS • the legal requirements of the NHS to protect personal data under the Data Protection regulations • the requirements under NIS regulations to protect cyber security • the impact of a cyberattack (significant financial impact, loss of trust in services, personal impact of patients both in terms of care and associated with data breaches, impact on health and social care staff) • the wider impact on the health and social care system of a cyberattack In its consideration of the above points, the ICB has applied Section 24 as the public interest in the information does not outweigh the risks should a cyberattack occur due to the disclosure of the information. The public interest lies in maintaining continuity of services and ensuring that data remains secure.
2. Software Defined WAN (SDWAN) a. Please can advise who is the existing supplier b. Contract end dates c. Total contract value d. Which framework this was purchased under e. Name of the contact responsible for this	IT infrastructure for BNSSG (Bristol, North Somerset and South Gloucestershire Integrated Care Board) ICB is provided by South Central and West Commissioning Support Unit (SCW CSU) as part of a wider contract for support services. SCW can be contacted at: england.contactus@nhs.net
3. Local Area Network (LAN) a. Please can advise who is the existing supplier b. Contract end dates	

c. Total contract value d. Which framework this was purchased under e. Name of the contact responsible for this	
4. Wireless Access (WIFI) a. Please can advise who is the existing supplier b. Contract end dates c. Total contract value d. Which framework this was purchased under e. Name of the contact responsible for this	

The information provided in this response is accurate as of 25 June 2025 and has been approved for release by Deborah El-Sayed, Chief Transformation and Digital Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.