FOI 35956 Disclosure Log

The Trust has considered each line item. While certain items may appear low-risk in isolation, the request seeks multiple categories of information across several core digital services. Disclosure of this combined dataset would increase aggregated cyber risk.

Stakeholder title, generic procurement assurance and publicly available programme information has been disclosed/signposted, with the remaining information withheld under sections 31(1)(a) and 38 as detailed in the key below and in the result of the Public Interest Test.

Decision

Disclosure:

Withhold most of the requested contract-specific, technical and operational detail due to aggregated risk; provide title of senior internal stakeholder, generic procurement assurance and signposting to already published information where appropriate.

Withheld:

For the reasons above, the Trust will withhold (where held) the cross-service dataset items requested such as supplier/product, licence numbers, contract values/dates, operational volumes, and integration descriptions, because of the aggregated cyber risk.

Exemption(s):

Apply Section 31(1)(a) and Section 38 for withheld information.

Section 31 – Law Enforcement

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

 To protect the work of one that does

 To withhold information that would make anyone, including the public authority itself, more vulnerable to crime

Section 38 – Health & Safety

Section 38 states that information is exempt if its disclosure could lead to the physical or mental harm of, or endanger the safety of, individuals.

Disclosure of the requested information would leave the Belfast Trusts digital infrastructure at significant risk of cyber security attack. A cyber-security attack may lead to the placing of sensitive health & social care information into the public domain and, as such, the Trust believes there is a link between the risk of endangerment for data subjects and the disclosure of the requested information. There would likely be a substantial detrimental effect on the physical or mental health of patients, clients, staff or their families should the requested information be released.

Key:

Outcome:	Disclose / Withhold / Part disclose (signpost)
Exemptions:	**s31(1)(a)** = Prevention/detection of crime (cyber-enabled crime) **s38** = Health & safety (risk to individuals arising from cyber incident impacts)
Summary rationale:	Summary rationale for exemption which intentionally withholds information about security, setup, or suppliers.

1) Digital Dictation

Information requested	Outcome	Exemption(s)	Summary rationale for exemption
Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Disclosure would contribute to an aggregated profile of core systems/suppliers, increasing cyber-attack risk to services and data.

Number of user licences	**Withhold**	**s31(1)(a), s38**	Licence/scale data supports footprint estimation and can assist targeted attack planning when aggregated.
Procurement method (e.g., framework)	**Disclose (generic statement)**	N/A	Belfast Trust complies with procurement legislation/policy; procurements undertaken in conjunction with Business Services Organisation (BSO) Procurement and Logistics Services (PaLS) as CoPE
Contract start date	**Withhold**	**s31(1)(a)**	Contract timelines across multiple systems can reveal operational pressure points useful to attackers.
Contract expiry date / extension/rolling	**Withhold**	**s31(1)(a)**	As above—contract lifecycle information contributes to aggregated intelligence about dependencies and timing.
Total contract value (if available)	**Withhold**	**s31(1)(a)**	Financial/value indicators across multiple suppliers can increase targeting incentives and prioritisation.
Integration with PAS/EPR (inbound/outbound)	**Withhold**	**s31(1)(a), s38**	Integration/interconnectivity data can inform attack pathways and increase risk to healthcare operations.
Key internal stakeholder role/title	**Disclose**	N/A	Co-Director of Digital Services.
Desired features not currently delivered (optional)	**Withhold**	**s31(1)(a)**	Capability gaps across systems could be exploited as part of an aggregated risk picture.

2) Outsourced Transcription

Information requested	Outcome	Exemption(s)	Summary rationale for exemption
Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Contributes to aggregated supplier/technology map for core services, increasing cyber risk.

Procurement method (e.g., framework)	**Disclose (generic statement)**	N/A	Procurement conducted in line with legislation/policy via BSO PaLS.
Contract start date	**Withhold**	**s31(1)(a)**	Contract lifecycle data across systems can reveal dependency timing/transition windows.
Average monthly volume of letters	**Withhold**	**s31(1)(a), s38**	Operational volumes indicate scale/criticality; when combined can aid targeting and impact planning.
Average monthly volume of lines	**Withhold**	**s31(1)(a), s38**	As above—quantitative usage indicators contribute to an aggregated system footprint profile.
Total contract value (if available)	**Withhold**	**s31(1)(a)**	Financial/value indicators across multiple suppliers can increase targeting incentives and prioritisation.
Key internal stakeholder role/title	**Disclose**	N/A	Co-Director of Digital Services.
Desired features not currently delivered (optional)	**Withhold**	**s31(1)(a)**	Capability gaps across systems could be exploited as part of an aggregated risk picture.

3) Speech Recognition

Information requested	Outcome	Exemption(s)	Summary rationale for exemption
Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Supplier/product identifiers across core services contribute to aggregated targeting intelligence.
Number of user licences	**Withhold**	**s31(1)(a)**	Licence/scale data supports footprint estimation and can assist targeted attack planning when aggregated.
Procurement method (e.g., framework)	**Disclose (generic statement)**	N/A	Procurement conducted in line with legislation/policy via BSO PaLS.

Contract start date	**Withhold**	**s31(1)(a)**	Contract lifecycle data across systems can reveal dependency timing/transition windows.
Contract expiry date / extension/rolling	**Withhold**	**s31(1)(a)**	As above—timing information contributes to aggregated risk and targeting opportunity.
Total contract value (if available)	**Withhold**	**s31(1)(a)**	Financial/value indicators across multiple suppliers can increase targeting incentives and prioritisation.
Integration with PAS/EPR (inbound/outbound)	**Withhold**	**s31(1)(a), s38**	Interconnectivity information can reveal potential routes of compromise, inform target profiling and increase risk to healthcare operations.
Key internal stakeholder role/title	**Disclose**	N/A	Co-Director of Digital Services.
Desired features not currently delivered (optional)	**Withhold**	**s31(1)(a)**	Capability gaps across systems could be exploited as part of an aggregated risk picture.

4) Ambient AI Scribe

Information requested	**Outcome**	**Exemption(s)**	**Summary rationale for exemption**
Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Contributes to aggregated supplier/technology profile of core services, increasing cyber risk.
Number of user licences	**Withhold**	**s31(1)(a)**	Licence/scale data supports footprint estimation and can assist targeted attack planning when aggregated.
Procurement method (e.g., framework)	**Disclose (generic statement)**	N/A	Procurement conducted in line with legislation/policy via BSO PaLS.
Contract start date	**Withhold**	**s31(1)(a)**	Contract lifecycle data across systems can reveal dependency timing/transition windows.

Contract expiry date / extension/rolling	**Withhold**	**s31(1)(a)**	As above—timing information contributes to aggregated risk and targeting opportunity.
Total contract value (if available)	**Withhold**	**s31(1)(a)**	Financial/value indicators across multiple suppliers can increase targeting incentives and prioritisation.
Integration with PAS/EPR (inbound/outbound)	**Withhold**	**s31(1)(a), s38**	Interconnectivity information can reveal potential routes of compromise, inform target profiling and increase risk to healthcare operations.
Pilot stage (supplier/duration/scope)	**Withhold**	**s31(1)(a)**	Implementation scope/timing can add to aggregated intelligence about system deployment and exposure.
Key internal stakeholder role/title	**Disclose**	N/A	Co-Director of Digital Services.
Desired features not currently delivered (optional)	**Withhold**	**s31(1)(a)**	Capability gaps across systems could be exploited as part of an aggregated risk picture.

5) Video Consultation

Information requested	**Outcome**	**Exemption(s)**	**Summary rationale for exemption**
Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Supplier/product identifiers across core services contribute to aggregated targeting intelligence.
Number of user licences	**Withhold**	**s31(1)(a)**	Licence/scale data supports footprint estimation and can assist targeted attack planning when aggregated.
Procurement method (e.g., framework)	**Disclose (generic statement)**	N/A	Procurement conducted in line with legislation/policy via BSO PaLS.
Contract start date	**Withhold**	**s31(1)(a)**	Contract lifecycle data across systems can reveal dependency timing/transition windows

Contract expiry date / extension/rolling	**Withhold**	**s31(1)(a)**	As above—timing information contributes to aggregated risk and targeting opportunity.
Total contract value (if available)	**Withhold**	**s31(1)(a)**	Financial/value indicators across multiple suppliers can increase targeting incentives and prioritisation.
Integration with PAS/EPR (inbound/outbound)	**Withhold**	**s31(1)(a), s38**	Interconnectivity information can reveal potential routes of compromise, inform target profiling and increase risk to healthcare operations.
Key internal stakeholder role/title	**Disclose**	N/A	Co-Director of Digital Services.
Desired features not currently delivered (optional)	**Withhold**	**s31(1)(a)**	Capability gaps across systems could be exploited as part of an aggregated risk picture.
Average number of video appointments per month/year	**Withhold**	**s31(1)(a), s38**	Operational volumes indicate criticality/scale and can assist targeting and impact planning.
% video vs telephone consultations	**Withhold**	**s31(1)(a)**	Usage pattern indicators contribute to aggregated understanding of service reliance.

6) Health Information Systems

System	Information requested	Outcome	Exemption(s)	Summary rationale for exemption
PAS / EPR	Name of supplier & product	**Part disclose (signpost) + withhold remainder**	**s31(1)(a), s38** (for withheld remainder)	Public programme information is signposted online at: https://belfasttrust.hscni.net/about/encompass/ ; additional product detail would add to aggregated profiling of core systems.

eDMS	Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Supplier/product identification contributes to aggregated system mapping and increases cyber risk to healthcare operations/data.
RIS / LIMS	Name of supplier & product	**Part disclose (signpost) + withhold remainder**	**s31(1)(a), s38** (for withheld remainder)	Regional programme information is signposted online at: https://bso.hscni.net/directorates/digital/ ; additional product detail would add to aggregated profiling of core systems.
e-Correspondence	Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Supplier/product identifiers contribute to aggregated profiling and targeting risk.
Hybrid Mail	Name of supplier & product	**Withhold**	**s31(1)(a), s38**	Identifies dependencies within communications workflows; adds to aggregated threat intelligence.
Patient Portal	Name of supplier & product	**Part disclose (signpost) + withhold remainder**	**s31(1)(a), s38** (for withheld remainder)	Public portal programme info is signposted online at: https://belfasttrust.hscni.net/about/encompass/my-care-your-patient-portal/ ; additional product detail would add to aggregated profiling of core systems.