Witness Name: Dr Susan Elcock

WITN0356090

Statement No: 2

Dated: 13 May 2026

THE NOTTINGHAM INQUIRY

SECOND WITNESS STATEMENT OF DR SUSAN ELCOCK

I, Dr Susan Elcock, will say as follows:

Introduction

1. I have been Deputy Chief Executive Officer of Nottinghamshire Healthcare NHS Foundation Trust (the "**Trust**") since October 2023 and Executive Medical Director of the Trust since May 2021.

2. This witness statement is made to assist the Nottingham Inquiry (the "**Inquiry**") with the matters set out in the request made under Rule 9 of the Inquiry Rules 2006, dated 10 April 2026. This statement principally relates to my role as the Trust Caldicott Guardian from May 2021 – present day. I can speak to this period from my personal knowledge, and for the period from May 2020-May 2021, I have addressed these arrangements as far as I am able.

3. This witness statement was drafted on my behalf by the external solicitors acting for NHFT in respect of the Inquiry, with my oversight and input, following discussions in writing by email and by video conference. Where necessary, I have also consulted with subject matter experts within the Trust. However, I can confirm that all the facts set out in this statement are true to the best of my knowledge and belief.

4. The Rule 9 request received on 10 April 2026 has asked for a short summary of my career, including my role at the Trust. I have set out detail in regard to these matters in detail in paragraphs 8 to 33 of my First Witness Statement to the Inquiry [**WITN0356001**], and do not propose to repeat that here.

The role of the Caldicott Guardian

Data Protection and other key roles and responsibilities within the Trust

5. I have set out some detail about the role of the Caldicott Guardian in paragraphs 453-458 of my First Witness Statement [**WITN0356001**]. This included my understanding of the role, and the relevant principles. I do not propose to repeat that detail here, but I have reviewed my First Statement and confirm again that it is true and accurate. I would like to note further that all eight Caldicott Principles are relevant to the role, and the role itself serves as the 'conscience' of the organisation regarding the protection and confidentiality of patient information.

6. There are a range of roles and responsibilities regarding information sharing in addition to the Caldicott Guardian. The SIRO ("Senior Information Risk Owner")

is a role introduced as a requirement within the NHS in 2008. This role is held by the Executive Director of Partnerships and Strategy of this Trust and is responsible and accountable for information risk policy and strategy in the organisation. This means understanding how information risks can impact on services, owning information risk assessment processes, ensuring compliance with data protection legislation and ensuring the board is informed of information risk issues. They work alongside the Data Protection Officer ("Data Protection Officer") and Caldicott Guardian.

7. The DPO is a requirement of the GDPR Article 37 introduced in 2018 and a mandatory appointment for public authorities. The role is held by the Head of Data Security and Data Protection (formerly Information Governance) within this Trust. The role of the DPO is set out in the GDPR Article 39 and includes providing independent advice to staff and the Trust on their data protection obligations, monitoring internal compliance, providing advice regarding Data Protection Impact Assessments, maintain a register of data processing activities, and act as a point of contact for data subjects and the Information Commissioner's Office.

8. In regard to information sharing within the Trust, the three roles are key and there is an extent of overlap, especially with the Caldicott Guardian and DPO. Both the Caldicott Guardian and DPO will receive requests in relation to information sharing and will often discuss queries and issues raised, sharing their knowledge and expertise, resulting in an agreed outcome. The DPO is responsible for

maintaining the Trust Record of Processing of Activities (ROPA), this is in relation to data processing and within the ROPA the Caldicott Guardian Log is held.

9. The Trust produces an Annual SIRO Report which is received by the Audit and Risk Committee and is presented by the SIRO. The report informs the Audit and Risk Committee of the work being undertaken to recognise and manage risks regarding information processed by the Trust, satisfying legal and regulatory requirements and to uphold the data protection rights of patients and employees. The report includes information risk management, incident reporting, the DSPT annual submission, the DSPT annual audit and outcomes, cyber security. It is initially received by the Information Security Group before being presented to the Audit and Risk Committee. The Information Security Group membership includes the Caldicott Guardian, SIRO and DPO.

10. The Trust completes the annual NHS England Data Security and Protection Toolkit ("DSPT") which is an online self-assessment tool allowing organisations to measure performance against the National Data Guardian's 10 data security standards.

11. All organisations that have access to NHS patient data and systems must use the toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. There are 5 Objectives with multiple Contributing Outcomes where the Trust has to collate evidence to provide the necessary assurances to meet the Objectives. Objective E of the DSPT is "Using and sharing information appropriately". The organisation ensures

that information is used and shared lawfully and appropriately and must provide the appropriate evidence. Contributing Outcomes E3.a and E3.b are specifically related to information use and sharing:

a. E3.a Using and sharing information sharing for direct care - You lawfully and appropriately use and share information for direct care.

b. E3.b Using and sharing information for other purposes - You lawfully and appropriately use and share information for purposes outside of direct care.

12. The Caldicott Guardian Log is managed by the Data Protection Team. The Log captures events where Caldicott Guardian advice or decision making is sought, the dates and outcome. The log is held within the Trust's Records of Processing (ROPA) and is evidenced in the Trust's NHSE Data Security and Protection Toolkit annual assessment.

13. On 30 June 2025 the Trust submitted the NHS England Data Security and Protection Toolkit (DSPT) 2024/2025 (version 7) final assessment. [**NHFT0019596**] The submission was recorded with 'All Standards Met' and further assurance was provided by the independent annual audit. The scope for the annual audit is mandated by NHS England. The Trust is currently working towards completion of the DSPT 2025/2026 (version 8) final assessment. The

NHSE DSPT is an annual submission and the Trust has achieved 'All Standards Met' for each submission since the DSPT began in 2018.

14. Legislation is in place to ensure that information is shared lawfully, fairly and transparently. We must establish a lawful basis for sharing personal data which can include consent, legal obligation or public interest. Trust policies will refer to not only legislation, such as that listed below, but also guidance from various professional bodies. Procedures are developed from the overarching policies, and they are all available on our intranet for staff to access. Queries on information processing and sharing are regularly posed to the Data Protection Team, the DPO and Caldicott Guardian.

15. The key legislation/law is:

    a. Data Protection Act 2018
    b. The common law duty of confidentiality
    c. Human Rights Act 1998
    d. Freedom of Information Act 2000
    e. Caldicott Principles 2000
    f. The Health and Social Care (National Data Guardian) Act 2018
    g. UK General Data Protection Regulation
    h. Data (Use and Access) Act 2025

How does the Caldicott Guardian work with Trust staff?

16. In respect of care and treatment provided to mental health patients, the Caldicott Guardian can work with Responsible Clinicians (and indeed any other clinicians) in various ways to support the provision of mental health services. Specifically at the Trust, I am occasionally approached directly by clinicians rather than via the Data Protection Team regarding queries such as the proportionality of sharing information with third parties in a specific situation, or requests for guidance and/or discussions in respect of complex, case specific, decision making. These queries relate to information sharing and matters of confidentiality. The majority of approaches are through the Data Protection Team and I tend to be approached directly around 5-8 times a year.

17. Since April 2021, staff seeking advice from the Data Protection Team, the Data Protection Officer or the Caldicott Guardian have been able to use a generic email account (CaldicottGuardian@ **NHFT**

18. There is recognition that the Caldicott Guardian role is considered the 'conscience of the organisation' regarding patient information and confidentiality. However, it is important to note that the Caldicott Guardian is only for patient information, whereas the Data Protection Officer has specific responsibilities under the Data protection legislation in relation to personal data generally.

19. Staff within the Trust are able to approach the Caldicott Guardian, SIRO and DPO directly but more often will approach the Data Protection Team (formerly Information Governance) for advice, guidance and support on information

sharing, and matters related to confidentiality, data protection, records management, data subjects' rights, information risk management and Freedom of Information. Dependent on the query in hand, the team and/or the DPO may then seek advice and decision making from the Caldicott Guardian and/or SIRO.

Issues raised to the Caldicott Guardian

20. Queries made to the Trust Caldicott Guardian are recorded within the Caldicott Guardian Log, which is part of the Trust's Record of Processing (as a requirement of Article 30 of the UK GDPR). The Record of Processing captures the Trust's data processing activities and the legal basis and retention policies for these. The Caldicott Guardian Log has been in its current format since 2015 with records from then, to date, of queries and decisions raised with the Caldicott Guardian. I have exhibited an example of the log, which shows two cases taken from 2025 and 2026, to this statement **[WITN0356091]**. The two example cases described in this log are as follows:

    a. A clinician involved in the care of a patient who was also supported by a mental health advisor from an educational establishment, shared information with the clinician regarding historical and current incidents of acts of aggression. Due to risk concerns, the clinician sought confirmation of their belief that risk management information could be shared with the third party mental health advisor. Support and guidance were provided to the clinician.

b. A clinician requested advice regarding a request to share health information with third parties where safeguarding concerns had previously been noted. Capacity to consent and the legal framework regarding data processing were discussed and established.

Patient consent and sharing information

21. There will be occasions where a patient has withdrawn their consent for clinicians to share information about their treatment with their nearest relative, or other third party. The Inquiry has specifically asked me to address the circumstances in which it would be considered appropriate for a clinician to disclose information about a patient's treatment to their nearest relative or the police. My response on this point below should be read alongside paragraph 352 of my First Witness Statement, where I describe that the Trust has in place information sharing agreements with relevant partners and as Caldicott Guardian I sign these on behalf of the organisation.

Disclosure of information to a patient's Nearest Relative under the Mental Health Act

22. The Nearest Relative is a legal term that is recognised role under section 26 of the Mental Health Act and attracts statutory rights. It is not considered the same as 'next of kin'. The Nearest Relative and the patient's next of kin may be different people.

23. In relation to a patient who is detained under Part 2 of the Mental Health Act certain information about the patient may be shared with the Nearest Relative

without consent, but this is not an absolute right. Chapter 10 (specifically paragraphs 10.3, 10.12 and 10.13) of the Mental Health Act Code of Practice [**DHSC0000007**] provides guidance on this. Areas of information that can be shared with a Nearest Relative in the absence of consent include whether the patient is detained in hospital under Section, which Section, basic reasons for the detention, for the management of serious risk or serious harm, and details regarding their discharge from hospital. General information to assist with the Nearest Relative's understanding of a known diagnosis may be shared without the patient's consent. Any such disclosure will be documented within the patient record.

Disclosure of information without consent

24. There are circumstances where a patient does not provide, or has withdrawn, their consent for information to be shared by clinicians with a third party (such as the police, other public body or a relative other than those circumstances described in paragraph 24 above) and it is nonetheless appropriate for this information to shared. These circumstances include:

    a. Where there is a legal duty to disclose, such as under the Prevention of Terrorism Act, Terrorism Act, Road Traffic Act, Female Genital Mutilation Act, or a Court Order;

    b. Where the disclosure would need to be in the public interest, such as:

        - to protect individuals or society from risks of serious harm, or

- for the prevention, detection or prosecution of serious crime, especially crimes against the person

25. The GMC issues guidance in relation to the above **[NUHT0000044]** and has provided examples of when information may be shared when there is no consent. The Trust doctors would use this guidance to inform their decision making

26. Requests for information in these circumstances are considered on a case by case basis, and Trust staff will often first discuss the matter with the Trust's Data Protection Officer and that may be escalated to the Caldicott Guardian. As stated at paragraph 365 of my First Witness Statement **[WITN0356001]**, the Trust Caldicott Guardian does not have a formal role in liaising with the police, but I do give advice to colleagues about the proportionality of information that should be shared in some individual circumstances.

27. Information Sharing arrangements with the police are formalised with an Information Sharing Agreement (a previous draft version of this Agreement has been disclosed to the Inquiry as **[NHFT0009273]**, I exhibit the agreed version as **[NGPF0010738]**. The most recent review of this agreement was signed by Nottinghamshire Police in January 2026.

Professional guidance relied upon in the course of assessments

28. I would expect doctors to rely on professional guidance in the course of assessments, including the Mental Health Act Code of Practice, the GMC's

Practice Guidance – Confidentiality: good practice in handling patient information (2017) **[NUHT0000044]**, and guidance by the Royal College of Psychiatrists, 'Good Psychiatric Practice: Confidentiality and Information Sharing (3rd edition) (November 2017) **[WITN0320017]**.

29. The GMC guidance referenced in the above paragraph is the GMC core guidance, makes clear that patients have a right to expect that their personal information will be treated as confidential. This guidance, which forms part of the professional standards, sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow.

30. Page 4 of this guidance outlines the framework, "*for considering when to disclose patients' personal information and then applies that framework to:*

a. *disclosures to support the direct care of an individual patient*

b. *disclosures for the protection of patients and others*

c. *disclosures for all other purposes.*" **[NUHT0000044]**.

31. I refer the Inquiry to page 4-5 of this guidance which sets out the responsibilities of all doctors for managing and protecting patient information. In addition, the guidance sets out how it uses the terms "you must" and "you should" – and that "you must" refers to a legal or ethical duty, and you should is for duties and principles which may not apply to the situation the individual is in, or that might be impacted by other factors.

32. There is further guidance in this document on pages 7-8 that provides information on ethical and legal duties of confidentiality and acting within the law. I would expect all doctors at the Trust to understand this guidance, and the eight principles set out at page 8.

33. The guidance on pages 9-21 helpfully provides a framework on when patient information can be disclosed, and I would expect doctors at the Trust to be aware of this and use this guidance as a point of reference when making decisions on the disclosure of patient information.

34. In addition, the guidance from the Royal College of Psychiatrists, the Good Psychiatric Practice: Confidentiality and information sharing, notes that it is informed by the GMC guidance, and is complementary to that. I consider this is another useful tool for doctors to review during the course of assessing disclosure and I would expect them to refer to this guidance.

35. The NMC Code **[NUHT0000058]**, at section 5, also sets out the expectation for nurses to review confidentiality and the sharing of information.

Trust policies relied on in the context of assessments

36. Clinicians could also consult the following Trust policies (the relevant extracts have been set out below):

    a. Mental Health Legislation Policy and Procedure Manual 05 **[NHFT0019603, version 3, updated December 2025]**, which refers

to section 132 of the Mental Health Act 1983 (, and Chapter 4 of the Mental Health Act Code of Practice 2015.

4.3.2 Information to Detained Patients (Section 132, MHA Code of Practice 2015, Chapter 4):

*4.3.2.3 The managers must also take whatever steps are practicable to give or send a copy of the written information to the person they think is the patient's nearest relative unless the patient requests otherwise (or does not have a nearest relative). This must be done either at the same time [*as detention*] or within a reasonable time afterwards (Section 132(4)).*

4.3.3 Information to Community Patients (Patients Subject to a Community Treatment Order (CTO)) Section 132A, MHA Code 2015 Chapter 4:

4.3.3.1 Section 132A requires the managers of the responsible hospital to take whatever steps are practicable to ensure that community patients understand:

• The effect of the provisions of the MHA which apply to them as community patients and

• Their rights to apply to the Tribunal.

*4.3.3.2 This must be done as soon as practicable after the patient becomes a community patient [*when a patient is subject to a Community Treatment Order] *and must include providing*

the necessary information both orally and in writing. The managers must also take whatever steps are practicable to give or send a copy of the written information to the person they think is the patient's nearest relative unless the patient requests otherwise (or does not have a nearest relative). This must be done either at the same time, or within a reasonable time afterwards.

4.3.3.3 Information to Community Patients Subject to Recall (Mental Health Regulations 2008): As soon as practicable, the managers of the hospital to which a patient is recalled must take whatever steps are reasonably practicable to arrange for the patient to be informed, orally and in writing, of the provisions of the MHA under which they have been recalled and the effect of those provisions. The managers must also take whatever steps are reasonably practicable to ensure that the patient understands the consent to treatment provisions of Part 4 of the MHA (Regulation 6(7) (a) and (b)).

4.3.6.6 A record should be made on the form of any objections made by the patient to information about their detention being sent to their nearest relative.

4.3.10 <u>Information to the Nearest Relative</u>

Upon admission under the MHA, unless the patient objects, the nearest relative will be informed of the patient's detention and sent the relevant statutory leaflet by the MHA administrator. Under Section 133 of the MHA, unless the patient objects, the Trust has a duty to inform the nearest relative of a patient's discharge from Section, and this will normally be done by the MHA administrator. Unless the nearest relative requests not to be informed, they may also be given by the ward team, details of any care that will be provided once discharged from hospital. If the patient objects to information regarding their detention being sent to their nearest relative, this should be indicated on the Patient's Rights Notification Form

b. Information Sharing between Professionals, Patients and Carers 08.01 [**NHFT0012786**].

6.2.5 If an individual is unable to provide consent, the decision can be made on their behalf by taking into account their best interests and the views of their carers or others close to the individual. Advice should also be sought from the Information Governance team, the Divisional Mental Capacity Act Lead, the Trust's Caldicott Guardian or appropriate Senior/Service Manager.

6.2.6 The issue of consent to information sharing should be discussed and documented as part of the initial process when care is being

planned with the individual and reviewed and documented regularly thereafter.

6.3.1 Whilst everyone has a right to information that they don't want to be shared kept confidential (which applies to carers as well as patients), there are occasions when that right of confidentiality can be breached such as when there is a statutory duty to do so or where sharing information is in the public interest. Examples of when it is appropriate to breach confidentiality are:

- *When there is a requirement by statute (in law)*
- *When there is a requirement in the public interest*
- *When required in the private interest of a person lacking capacity to decide whether to consent to disclosure*

6.3.2 The decision to disclose information in any circumstance without consent should, wherever possible, only be made by a Senior Healthcare Professional involved in the individual's care. Advice from the Information Governance team, or Trust's Caldicott Guardian should also be sought, and it may also be necessary in certain circumstances to seek legal advice.

If information is disclosed without consent, then the reason why the decision was taken and the person who authorised the disclosure should be recorded in the individual's records in addition to details about to whom it was disclosed.

c. Access to Information 12.09 (Data Subject Access Requests) [**NHFT0015701**].

6.3 On Behalf of the Data Subject Anyone applying on behalf of the data subject must supply written authorisation/consent from the data subject, this authorisation/consent being signed by the data subject; if it is not possible to provide signed authorisation/consent from the data subject, another lawful basis for sharing (such as a court order) must be identified. The current Trust policy requirements stipulate that wherever possible, signed authorisation/consent should be dated within the last six months of the date on which the request is received.

d. Data Protection 12.09 [**NHFT0015701**].

1.2 Current data protection legislation (Data Protection Act 2018 and the UK General Data Protection Regulation) provides the legal framework by which we are able to process personal information. This applies to information that might identify any living person.

1.3 The Common Law Duty of Confidentiality general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

2.2 Guidance will be provided on keeping personal information secure and confidential, and the correct procedures for accessing and

disclosing information will be outlined within Standard Operating Procedures linked to this policy.

e. Police & Criminal Justice Liaison 13.04 **WITN0263069**

7.11 Requests for additional patient records will be made by the police to the Trust Information Governance department (as per the Information Sharing Agreement) who will ensure the timely sharing of information required for the police / CPS to make a charging decision.

7.12 Senior managers from the Trust involved in PIPOT investigations may need to liaise with the police and share appropriate information on both Trust and police investigations. All sharing of information is to be conducted with due regard to the Trust Information Sharing agreement with Notts police.

37. The Inquiry has asked whether the Trust use a form, similar to that used by the Leeds and York Partnership NHS Trust [**WITN0412015**] in order to obtain information from the police or any other organisation. I can confirm that the Trust does not use a specific organisation wide form when requesting information from the police. Current processes include exercising the information sharing arrangements as agreed in the Trust and Police Information Sharing Agreement, the Street Triage Policy and via key police contacts within the Trust. Non urgent requests for information from the police are directed to the generic email account

for the Data Protection Officer. Here they are reviewed to ensure the request is complete, proportionate and lawful prior to being processed by the Access to Information Team.

38. The Information Sharing Agreement with the police, and as authored by the Trust, covers when information can be shared by the police with the Trust. These points can be found in Appendix C of the Agreement. They include written requests, and verbal requests when information is required in an emergency.

39. For requests of police data relating to persons who are or who have been in custody (non urgent enquiry) the Appendix provides the following:

Such information may include but is not limited to –

- *Any relevant personal information, including any relevant Special Category Data*
- *Details of any relevant events leading to the individual being taken in to custody*
- *Where relevant, whether the individual is known to the police for similar or related activity for risk assessment/safeguarding purposes where there is a perceived risk to NHS staff or other patients*
- *Details of welfare, treatment and behaviour leading up to or during police custody*
- *Details of any medical treatment or assessment while in custody*
- *Details of any risk assessments or risks identified and any relevant history which may assist in assessing and/or treating the individual*

- *Any relevant, specific information regarding a violent or sexual criminal history for risk assessment/safeguarding purposes where there is a perceived risk to NHS staff or other patients*
- *Details of any relative, carer or other person who may have information relevant to the treatment or assessment of the person concerned*

40. The guidance within the Appendix goes on to include agreed information to be shared when there is a request for police data

- *Relating to a person or persons whom a police officer has reasonable grounds to believe may be in need of assessment, care or treatment for mental health difficulties*
- *Relating to patients reported as missing from an inpatient location (including patients who have absconded from escorted leave and/or escaped from a secure unit) and/or whose whereabouts are not known to their clinical team*
- *Relating to patients recalled from a Community Treatment Order (CTO)*
- *Relating to allegations of a crime committed on or by patients or visitors of the Trust and/or Trust property/assets*
- *Relating to allegation of a crime committed against an individual employed by or working on behalf of the Trust by a patient or visitor*
- *Relating to staff employed by or working on behalf of the Trust who are the subject of police enquiries without prejudice to the Notifiable Occupation Process*

41. In addition, the Trust participates in the Police Liaison Operational Group (PLOG) with colleagues from the police force in attendance. I have provided information about the Police Liaison Operational Group at paragraph 208 of my First Witness Statement [**WITN0356001**]. The requests the Trust makes to the police for information relating to patients or staff will be done via email or telephone.

42. In my role as Caldicott Guardian, I will continue to consider the evidence that the Inquiry hears on this topic and will reflect internally and with Police colleagues on whether any further measures, in addition to the recently updated Information Sharing Agreement, would be beneficial; such as the development of a form similar to that referred to by the Inquiry. Given that the Information Sharing Agreement was entered into in January of this year, the Trust is keen to monitor its effectiveness before implementing any further changes.

Caldicott Guardian involvement with VC's care between May 2020 – June 2023

43. I can confirm that no discussions between clinicians / any Trust staff and the Trust Caldicott Guardian took place regarding the care of VC between May 2020 and June 2023. The Trust has confirmed this by way of checking the relevant personal email accounts of the Caldicott Guardians in the time period, as well as the generic Caldicott Guardian inbox.

Potential unauthorised access to records at Nottingham University Hospitals NHS Trust

44. As the Inquiry is aware, Nottingham University Hospitals NHS Trust ("**NUH**") is undertaking investigatory work in respect of unauthorised access to patient records, including access to the patient records of two of the surviving victims of VC's attacks. This work identified two members of Nottinghamshire Healthcare NHS Foundation Trust staff as having accessed these records.

45. An internal investigation was undertaken in accordance with the Trust's Data Protection and Clinical Information Access and Audit policies. The two members of nursing staff work within the Emergency Department at NUH, as part of the Liaison Psychiatry team. This team is a clinical team who work collaboratively with the clinical staff within Emergency Department and is a branch of psychiatry which sits at the intersection of mental and physical healthcare. The team focus on assessing and treating psychiatric symptoms in patients being treated for medical conditions with the aim of improving health outcomes through holistic treatment.

46. At the time of the tragic events of 13 June 2023, the role of this team included proactively screening patients and the provision of a triage service to establish whether their support and a subsequent referral to Trust services was required. Information available to staff within NUH records was minimal, as I understand the electronic patient record used by NUH in the Emergency Department has limited information available to the user. The information available to the staff included demographics, and reason for admission to the Emergency Department.

47. The Trust investigations concluded that the access by the two staff on 13 June 2023 was legitimate in terms of the team's processes and procedures. The access was part of an agreed and recognised process that was in place at the time. The process enabled the team to take a pre-emptive approach for patients who had been exposed to traumatic events, who then may require support and potentially a referral to Trust services.

48. We have found no evidence that any information viewed on 13 June 2023 has been shared onwards by our Trust staff and can confirm no referral to our services was made.

49. We therefore concluded that no unauthorised access was made by the two members of Trust staff. I wrote to the Medical Director of NUH on 8 May 2026 to confirm that the Trust would be content for this information to be shared with the two patients on our behalf through their existing relationships.

Reflections and recommendations

50. At paragraphs 452-458 of my First Witness Statement, I set out my view on improvements that could be made locally and nationally to multi-agency working

and information sharing, including in relation to the Caldicott Guardian. I wish to endorse those again here, but do not reproduce them here. [1]

Statement of Truth

I believe the content of this statement to be true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed: GRO-B

Dated: 13 May 2026

[1] I would like to correct a small error at paragraph 456 of my First Witness Statement. I stated that a "*key relationship is with the Senior Information Risk **Officer** (SIRO)*". This should read "*Senior Information Risk **Owner***".

Index to Second Witness Statement of Susan Elcock

No.	URN	Document Description
1	WITN0356001	First Witness Statement of Dr Susan Elcock
2	NHFT0019596	NHS England Data Security and Protection Certificate, 2024/25
3	WITN0356091	Example of Caldicott Guardian Log
4	DHSC0000007	Mental Health Act Code of Practice
5	NHFT0009273	Information Sharing Agreement – NHFT and Nottinghamshire Police (unsigned 2025 draft)
6	NGPF0010738	Information Sharing Agreement – NHFT and Nottinghamshire Police – January 2026
7	NUHT0000044	GMC's Practice Guidance – Confidentiality: good practice in handling patient information (2017)
8	WITN0320017	Royal College of Psychiatrists, 'Good Psychiatric Practice: Confidentiality and Information Sharing (3rd edition) (November 2017)
9	NUHT0000058	The Code – Nursing and Midwifery Council
10	NHFT0019603	Mental Health Legislation Policy and Procedure Manual 05 – updated December 2025
11	NHFT0012786	Information Sharing between Professionals, Patients and Carers 08.01
12	NHFT0015701	Access to Information 12.09 (Data Subject Access Requests)
13	NHFT0015701	Data Protection 12.09

14	**WITN0263069**	Police & Criminal Justice Liaison 13.04
15	WITN0412015	Form used by Leeds and York Partnership NHS Trust