



**North West London  
Acute Provider Collaborative**

29 APRIL 2025 - NWL APC BOARD IN  
COMMON - PUBLIC MEETING -  
READING ROOM



## 29 APRIL 2025 - NWL APC BOARD IN COMMON - PUBLIC MEETING - READING ROOM

 29 April 2025

 10:00 GMT+1 Europe/London

 The Oak Suite, W12 Conference Centre, Hammersmith Hospital



## AGENDA

• 4.1.3. Learning from deaths quarter 3 report - individual Trust reports.....	1
4.1.3a. CWFT Learning from deaths Q3 2024_25 Final V2.pdf .....	2
4.1.3b. ICHT Learning from Deaths Q3 2024-25 v2.pdf .....	20
4.1.3c. LNWH Learning from Deatgs Q3 2024-25 - FINAL.pdf .....	29
4.1.3d. THH Learning from Deaths Report Q3 2024_25.pdf .....	54
• 5.1. Collaborative Data and Digital Committee Report - NWL ICB Cyber Security Strategy.....	71
5.1b. Cyber security strategy - NWL ICB Cyber Security Strategy - v4.5 final draft.....	72

## 4.1.3. LEARNING FROM DEATHS QUARTER 3 REPORT - INDIVIDUAL TRUST REPORTS

### REFERENCES

Only PDFs are attached

-  4.1.3a. CWFT Learning from deaths Q3 2024\_25 Final V2.pdf
-  4.1.3b. ICHT Learning from Deaths Q3 2024-25 v2.pdf
-  4.1.3c. LNWH Learning from Deatgs Q3 2024-25 - FINAL.pdf
-  4.1.3d. THH Learning from Deaths Report Q3 2024\_25.pdf

NWL Acute Provider Collaborative Board in Common (Public)

29/04/2025

Item number: 4.1.3a

This report is: Public

# Chelsea and Westminster Hospital NHS Foundation Trust Learning from Deaths report Quarter 3 2024/25

Author: Stacey Humphries  
Job title: Head of Clinical Governance

Accountable director: Sanjay Krishnamoorthy  
Job title: Site Medical Director, WM

## Purpose of report (for decision, discussion or noting)

Purpose: Assurance

The board is asked to note this paper.

## Report history

Outline committees or meetings where this item has been considered before being presented to this meeting.

CWNHST Trust Mortality  
Surveillance Group  
07/03/2025  
Approved

CWNHSFT Executive  
Management 26/02/2025  
Approved

CWNHSFT Trust Quality  
Committee  
04/03/2025  
Approved

## Executive summary and key messages – linked to the section above, please update this to include key discussion points and actions agreed at previous meetings

The Trust is one of the best performing acute (non-specialist) providers in England in terms of relative risk of mortality with a Trust wide SHMI of 0.70 (where a number below 1 is better than expected mortality) for period September 2023 and August 2024 (Source HES). This positive assurance is reflected across the Trust as both sites continue to operate significantly below the expected relative risk of mortality.

During the 12-month period to the end of December 2024; 1,292 in-hospital adult or child deaths were recorded on the Trust mortality review system (Datix), of these 93% were screened and 43% had a full mortality case review closed following speciality discussion.

During Q3 24/25; There were no cases of sub-optimal care that might have or would reasonably be expected to have made a difference to the patient's outcome. For the 12 month period ending December 2024, 5 cases of sub-optimal care (grade CESDI 2) were identified and escalated for a decision on appropriate learning response.

Where the potential for improvement is identified learning is shared at Divisional review groups and presented to the Trust-wide Mortality Surveillance Group; this ensures outcomes are shared and learning is cascaded.

## Impact assessment

Tick all that apply

- Equity
- Quality
- People (workforce, patients, families or careers)
- Operational performance
- Finance
- Communications and engagement
- Council of governors

Mortality case review following in-hospital death provides clinical teams with the opportunity to review expectations, outcomes and learning in an open manner. Effective use of mortality learning from internal and external sources provides enhanced opportunities to reduce in-hospital mortality and improve clinical outcomes and experience for patients and their families.

## Strategic priorities

Tick all that apply

- Achieve recovery of our elective care, emergency care, and diagnostic capacity (APC)
- Support the ICS's mission to address health inequalities (APC)

- Attract, retain, develop the best staff in the NHS (APC)
- Continuous improvement in quality, efficiency and outcomes including proactively addressing unwarranted variation (APC)
- Achieve a more rapid spread of innovation, research, and transformation (APC)
- Help create a high quality integrated care system with the population of north west London (ICHT)
- Develop a sustainable portfolio of outstanding services (ICHT)
- Build learning, improvement and innovation into everything we do (ICHT)

## Main report

### 1. Learning and Improvements

The Trust's Mortality Surveillance programme offers assurance to our patients, stakeholders, and the Board that high standards of care are being provided and that any gaps in service delivery are being effectively identified, escalated, and addressed. This report provides a Trust-level quarterly review of mortality learning for Q3 2024/25 with performance scorecard (see Appendix 1 and 2) reflecting all quarters of the financial year.

#### 1.1. Relative Risk of mortality

The Trust uses the Summary Hospital-level Mortality Indicator (SHMI) and Hospital Standardised Mortality Ratio (HSMR) to monitor the relative risk of mortality. Both tools are used to determine the relative risk of mortality for each patient and then compare the number of observed deaths to the number of expected deaths; this provides a relative risk of mortality ratio (where a number below 100 represents a lower than expected risk of mortality).

Population demographics, hospital service provision, intermediate / community service provision has a significant effect on the numbers of deaths that individual hospital sites should expect; the SHMI and HSMR are designed to reduce this impact and enable a comparison of mortality risk across the acute hospital sector. By monitoring relative risk of mortality the Trust is able to make comparisons between peer organisations and seek to identify improvement areas where there is variance.

#### 1.2. Summary Hospital-level Mortality (SHMI) Indicator: Trust wide

The SHMI is the ratio between the actual number of patients who die following hospitalisation and the number that would be expected to die based on the England average, given the characteristics of the patients treated. It includes deaths which occurred in hospital and deaths which occurred outside of hospital within 30 days (inclusive) of discharge. Deaths related to COVID-19 are excluded from the SHMI.

The SHMI gives an indication of whether the observed number of deaths on our Trust sites within 30 days of discharge from hospital is 'higher than expected', 'as expected' or 'lower than expected' when compared to the national baseline. This report is largely using the latest release of Hospital Episode Statistics (HES) dataset to the period ending August 2024.

There were significant changes made to the SHMI methodology in May 2024. Figures published after this date cannot be precisely compared with previous publications.

## Site Level position

Figure one shows that both of the Chelsea and Westminster Hospital NHS Foundation Trust (CWHFT) sites have overall outcomes that are significantly below the national expected rate.

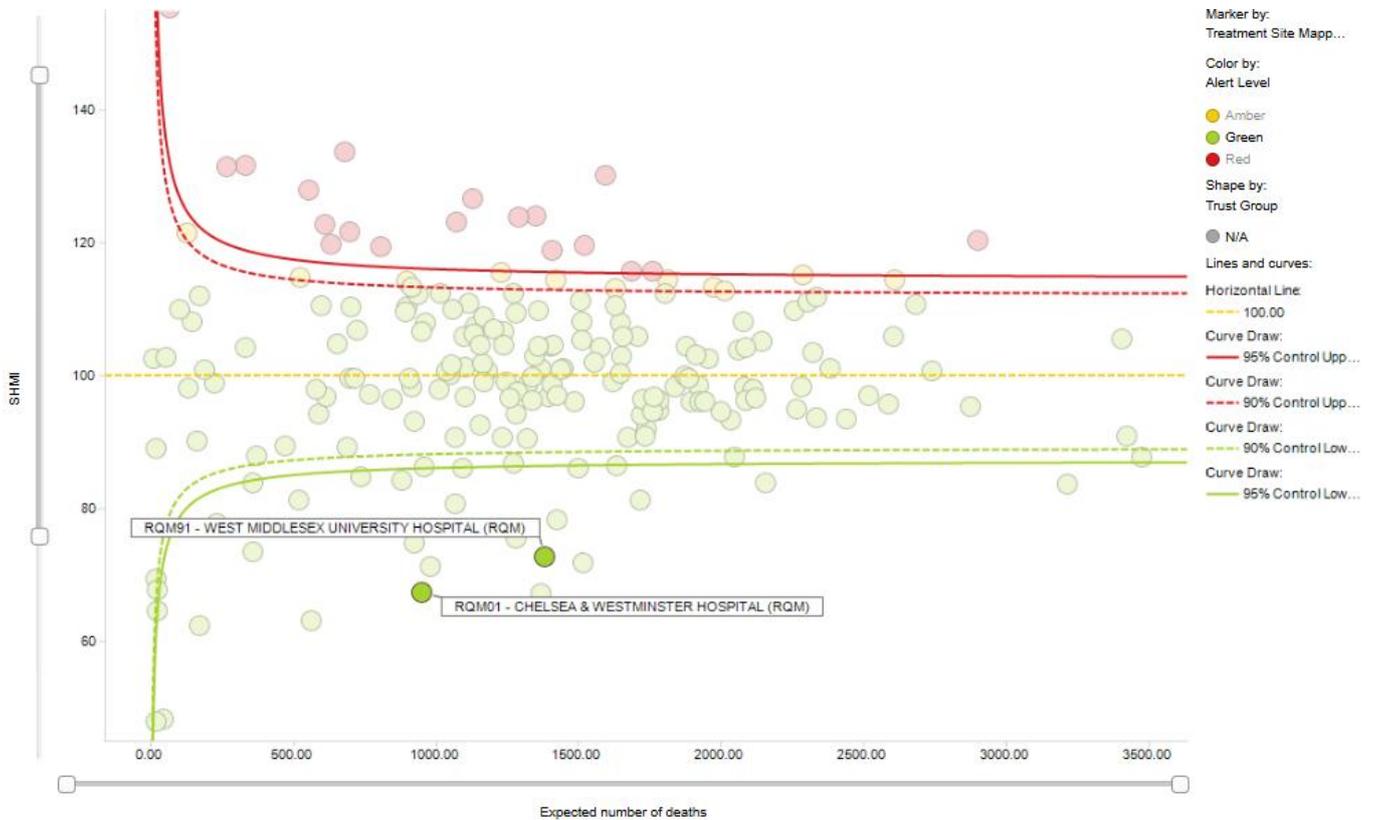


Figure 1: Funnel Plot (Rebasing period up to July 2024). SHMI comparison of England acute hospital sites based on outcomes between September 2023 and August 2024 - Updated 30/01/2025.

Using the SHMI dataset, within the period between September 2023 and August 2024, there have been 96332 discharges, of which 1628 patients died either in hospital or within 30 days of discharge. The number of expected deaths was 2305.

The ‘in hospital’ and ‘out of hospital’ SHMI values are also below the expected range. Overall 75% of patients died in hospital (n=1218). Table 1 below shows that both Trust sites have similar SHMI outcomes.

Site	SHMI	LCL 95%CI	UCL 95%CI	Expected number of deaths	Observed number of deaths	Total discharges	% adms. with palliative care coding	Mean comorbidity score per spell
CWH	69.45	64.2	75.02	931.56	647	44369	1.26%	2.86
WMUH	71.39	66.99	76	1374.17	981	51963	1.09%	3.78
CWHFT	70.61	67.22	74.12	2305.74	1628	96332	1.17%	3.36

Table 1. SHMI breakdown by site – Updated 30/01/2025

The positive assurance provided by the SHMI is reflected across the Trust as both sites continue to operate significantly below the expected relative risk of mortality.

**Diagnostic Groups:** The SHMI is made up of 142 different diagnostic groups which are then aggregated to calculate the Trust’s overall relative risk of mortality. The Mortality Surveillance

Group monitors expected and observed deaths across diagnostic groups; where statistically significant variation is identified the group undertakes coding and care review to identify any themes or potential improvement areas.

**Data Quality:** The Trust identified an issue with its HES submissions where some spells were appearing incomplete and as a result were moved by NHS Digital into the diagnostic group 'residual codes unclassified'. The problem has been fixed and since May 23, the number of records appearing in this group have subsequently been reduced.

### 1.3. Hospital Standardised Mortality Ratio (HSMR)

The HSMR is a ratio of the observed number of in-hospital deaths at the end of a continuous inpatient spell to the expected number of in-hospital deaths (multiplied by 100) for all diagnostic (CCS) groups in a specified patient group. The expected deaths are calculated from logistic regression models with a case-mix of: age band, sex, deprivation, interaction between age band and co-morbidities, month of admission, admission method, source of admission, the presence of palliative care, number of previous emergency admissions and financial year of discharge.

The traditional HSMR is based on the 56 diagnostic groups which contribute to 80% of in-hospital deaths in England. We can access outcomes against the above or all diagnosis group. HSMR (56 diagnosis groups) outcomes during the period September 2023 to August 2024 were below the expected range. The Trusts HSMR is 85 (upper CI 90: lower CI 80), with 1036 observed deaths over the period with 1222 expected.

Provider	HSMR	HSMR 95% Upper CI	HSMR 95% Lower CI	Number of super-spells	Expected number of deaths	Number of observed deaths
R1K - LONDON NORTH WEST UNIVERSITY HEALTHCARE NHS TRUST	95.39	100.2	90.76	57237	1665.77	1589
RAS - THE HILLINGDON HOSPITALS NHS FOUNDATION TRUST	94.09	102.24	86.43	21684	592.01	557
RQM - CHELSEA AND WESTMINSTER HOSPITAL NHS FOUNDATION TRUST	84.73	90.05	79.65	45489	1222.73	1036
RYJ - IMPERIAL COLLEGE HEALTHCARE NHS TRUST	72.74	76.8	68.85	69546	1794.02	1305

Table 2 – HSMR Top 56 diagnosis groups outcomes over period September 2023 to August 2024 – updated 31/01/2025

### 1.4. Crude mortality

Emergency spells (activity) and the deaths associated with those spells (crude number) can be used to calculate the rate of in-hospital deaths per 1000 patient spells (this calculation excludes elective and obstetric activity).

Crude mortality rates must not be used to make comparisons between sites due to the effect that population demographics, services offered by different hospitals, and services offered by intermediate / community care has on health outcomes (e.g. crude mortality does not take into account the external factors that significantly influence the relative risk of mortality at each site). Crude mortality is useful to inform resource allocation and strategic planning.

The following crude rates only include adult emergency admitted spells by age band. This approach is used as it reduces some of the variation when comparing the two sites and support understanding and trend recognition undertaken by the Mortality Surveillance Group.

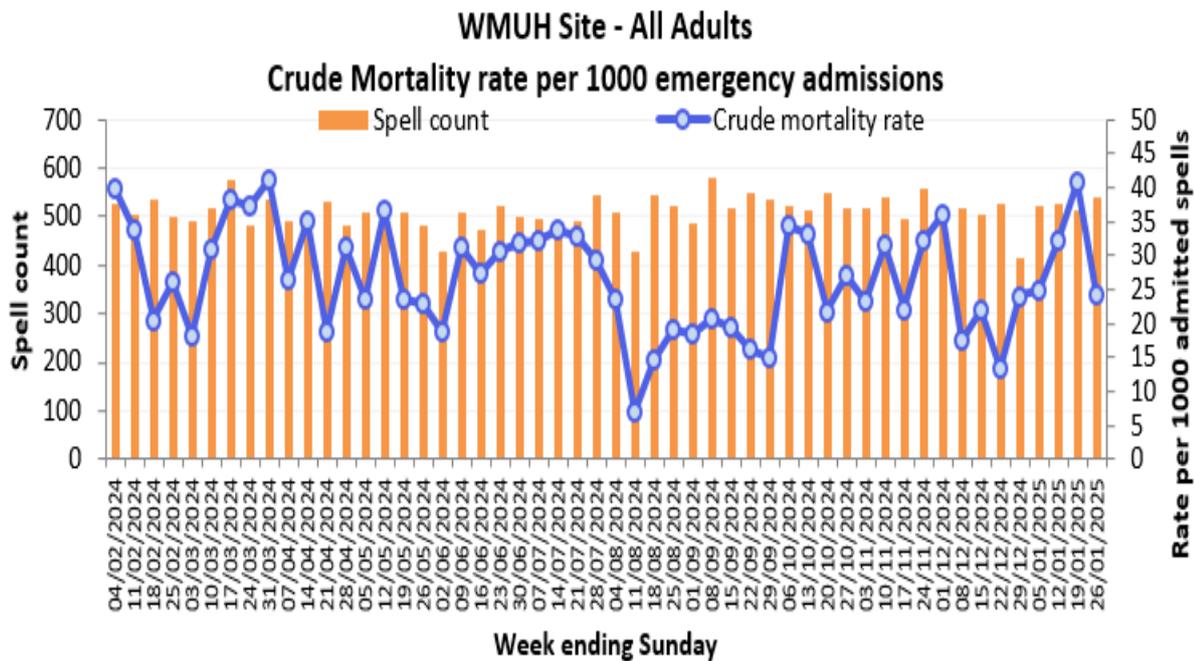


Figure 2 – Weekly adult emergency spell counts and crude mortality rate per 1000 patients, West Middlesex University Hospital

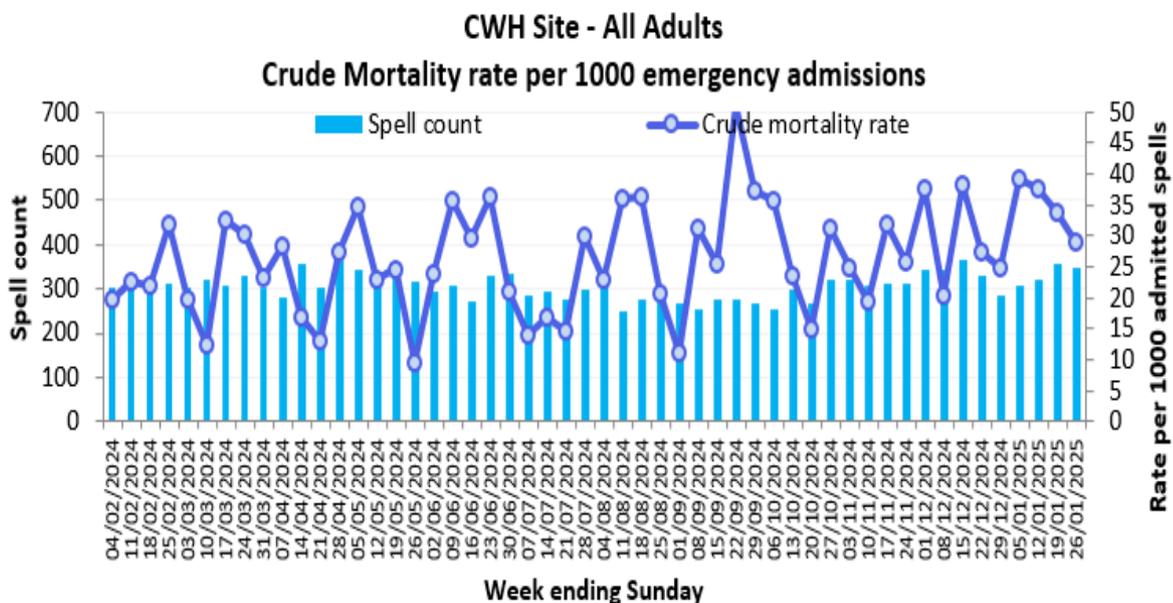


Figure 3 – Weekly adult emergency spell counts and crude mortality rate per 1000 patients, Chelsea and Westminster Hospital

**WMUH site - comparison of number of deaths over previous 52 weeks  
with 5 year mean (2015-2019)**

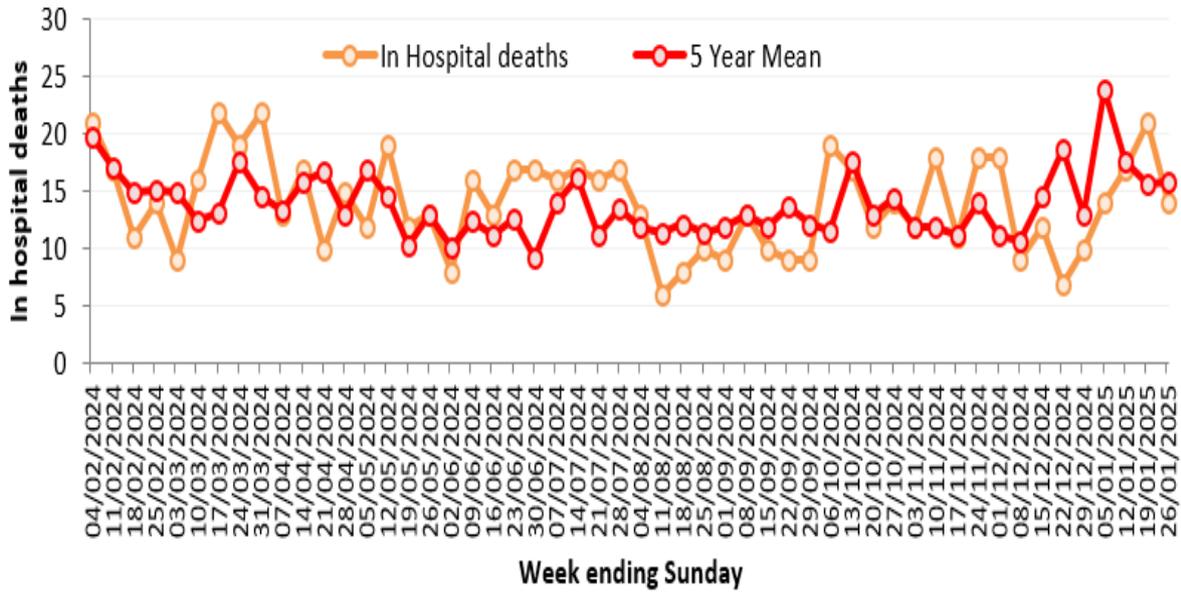


Figure 4 – Crude mortality in last 52 weeks compared with 5 year mean, West Middlesex University Hospital

**CWH site - comparison of number of deaths over previous 52 weeks  
with 5 year mean (2015-2019)**

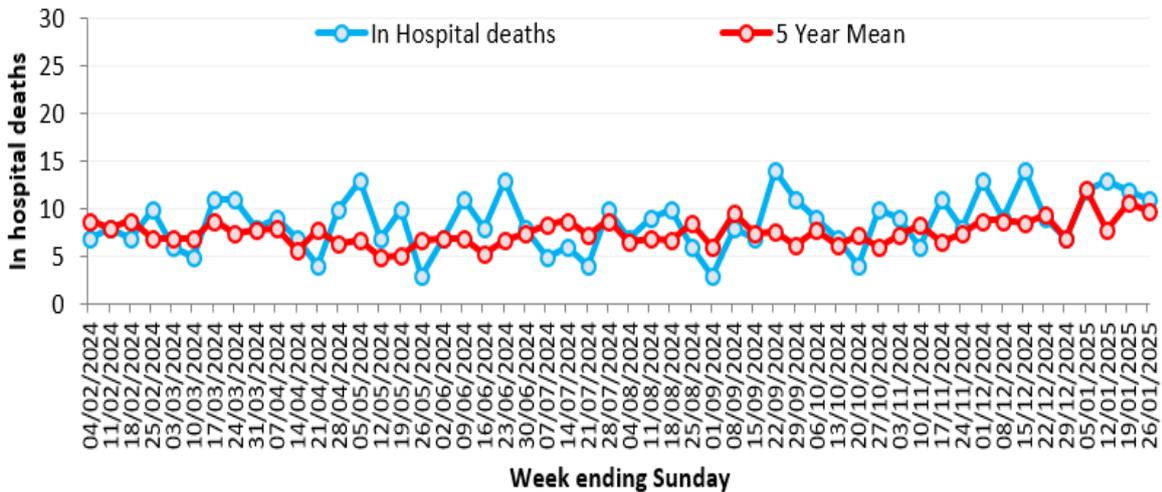
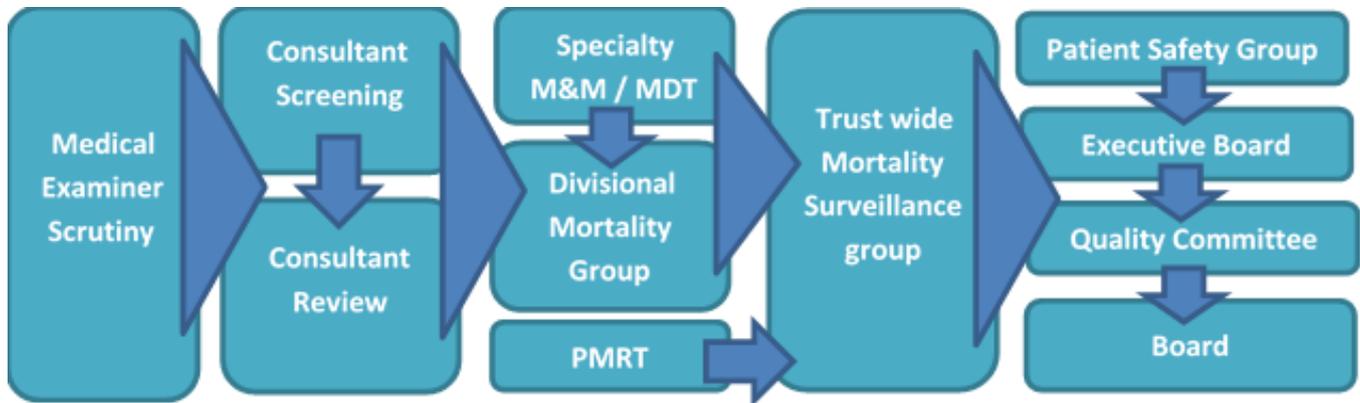


Figure 5 – Crude mortality in last 52 weeks compared with 5 year mean, Chelsea and Westminster Hospital

Crude mortality is monitored by the Mortality Surveillance Group on a monthly basis; no further review has been triggered as a result of this monitoring during this reporting period.

## 1. Thematic Review

The Mortality Surveillance Group (MSG) challenges assurance regarding the opportunity and outcomes from the Trust's learning from deaths approach.



MSG provides leadership to this programme of work; it is supported by monthly updates on relative risk of mortality, potential learning from medical examiners, learning from inquests, and divisional learning from mortality screening / review. MSG is a sub-group of the Patient Safety Group and is aligned to the remit of the Quality Committee.

### 1.1. Medical Examiner's office

An independent Medical Examiner's service was introduced to the Trust in April 2020 to provide enhanced scrutiny to deaths and to offer a point of contact for bereaved families wishing to raise concerns.

The purpose of this service is to:

- Provide greater safeguards for the public by ensuring proper scrutiny of all non-coronial deaths
- Ensure the appropriate direction of deaths to the coroner
- Provide a better service for the bereaved and an opportunity for them to raise any concerns to a doctor not involved in the care of the deceased
- Improve the quality of death certification
- Improve the quality of mortality data

During Q3 2024/25 the medical examiners service scrutinised 99% of in-hospital adult and child deaths and identified 78 cases of potential learning for the Trust and 15 cases of potential learning for other organisations. Potential learning identified during medical examiner scrutiny is shared with the patient's named consultant, divisional mortality review group and the Trust-wide Mortality Surveillance Group. Full consultant led mortality review is required whenever the MEs identify the potential for learning.

Thematic learning from medical examiner scrutiny is reported to the Mortality Surveillance Group, Executive Management Board, and Quality Committee (via annual ME report).

## 1.2. Adult and child mortality review

Mortality case review provides clinical teams with the opportunity to review expectations, outcomes and potential improvements with the aim of:

- Identifying sub-optimal or excellent care
- Identifying service delivery problems
- Developing approaches to improve safety and quality
- Sharing concerns and learning with colleagues

In-hospital adult and child deaths are screened by consultant teams using the screening tool within Datix, this supports the identification of cases that would benefit from full mortality review.

Learning from review is shared at specialty mortality review groups (M&Ms / MDTs); where issues in care, trends or notable learning is identified action is steered through Divisional Mortality Review Groups and the trust-wide Mortality Surveillance Group (MSG).

Trust mortality review targets:

- 100% of in-hospital adult and child deaths to be screened
- At least 30% of all adult and child death aligned to the Emergency and Integrated Care (EIC) Division to undergo full mortality review
- At least 80% of all adult and child deaths aligned to Planned Care Division (PCD), Women's Neonates, HIV/GUM, Dermatology (WCHGD), and West London Children's Health (WLCH) to undergo mortality review
- 100% of cases aligned to a Coroner inquest to undergo full mortality review
- 100% of cases where potential learning identified by Medical Examiner to undergo full mortality review

During January 2024 to December 2024; 1292 in-hospital adult or child deaths were recorded within the Trust's mortality review system (Datix), of these 93% have been screened and 43% have had full mortality case review.

	No. of deaths	No. of cases screened only and closed	No. of cases with full mortality review	No. of cases pending screening	% Screened	%	%
						with Full Review	Pending
Q4 23/24	363	196	155	12	96.7%	42.7%	3.3%
Q1 24/25	317	153	145	19	94.0%	45.7%	6.0%
Q2 24/25	272	127	123	22	91.9%	45.2%	8.1%
Q3 24/25	340	168	128	44	87.1%	37.6%	12.9%
<b>Totals</b>	<b>1292</b>	<b>644</b>	<b>551</b>	<b>97</b>	<b>92.5%</b>	<b>42.6%</b>	<b>7.5%</b>

Table 3: Adult and child mortality review status by financial quarter, Jan 2024 – Dec 2024

Process compliance is monitored by the Divisional Mortality Review Groups, Mortality Surveillance Group, and overseen by the Patient Safety Group, Executive Management Board, and Quality Committee.

	No. of deaths	No. of cases screened and closed	No. of cases with full mortality review	No. of cases pending screening	% Screened	% with Full Review	% Pending
EIC	1051	633	358	60	94.3%	34.1%	5.7%
PCD	225	1	187	37	83.6%	83.1%	16.4%
SCD	9	9	0	0	100.0%	0.0%	0.0%
WLCH	7	1	6	0	100.0%	85.7%	0.0%
<b>Totals</b>	<b>1292</b>	<b>644</b>	<b>551</b>	<b>97</b>	<b>92.5%</b>	<b>42.6%</b>	<b>7.5%</b>

Table 4: Adult and child mortality review status by Division, Jan 2024 – Dec 2024

Gaps in process compliance at Specialty and Divisional level are monitored by the Mortality Surveillance Group. Divisional plans to achieve the required compliance are reported to the Mortality Surveillance Group and Executive Management Board.

	No. of deaths	No. of cases screened and closed	No. of cases with full mortality review	No. of cases pending screening	% Screened	% with full review	% Pending
Acute Medicine	363	259	102	2	99.4%	28.1%	0.6%
Burns	5		3	2	60.0%	60.0%	40.0%
Cardiology	43	18	25		100.0%	58.1%	0.0%
Care Of Elderly	268	194	66	8	97.0%	24.6%	3.0%
Colorectal	9		6	3	66.7%	66.7%	33.3%
Diabetes/Endocrine	77	55	22		100.0%	28.6%	0.0%
Emergency Department	91		86	5	94.5%	94.5%	5.5%
Gastroenterology	52	20	27	5	90.4%	51.9%	9.6%
General Surgery	28		11	17	39.3%	39.3%	60.7%
Gynaecology	1	1			100.0%	0.0%	0.0%
Haematology	5	1	1	3	40.0%	20.0%	60.0%
HDU	1		1		100.0%	100.0%	0.0%
Hepatology	9	1		8	11.1%	0.0%	88.9%
HIV	8	8			100.0%	0.0%	0.0%
ICU	140		136	4	97.1%	97.1%	2.9%
Medical Oncology	20	7		13	35.0%	0.0%	65.0%
Paediatric Medical	7	1	6		100.0%	85.7%	0.0%
Palliative Care	3	3			100.0%	0.0%	0.0%
Respiratory	83	50	20	13	84.3%	24.1%	15.7%
Rheumatology	1			1	0.0%	0.0%	100.0%
Stroke	36	25	9	2	94.4%	25.0%	5.6%
Trauma / Orthopaedics	28	1	25	2	92.9%	89.3%	7.1%
Urology	14		5	9	35.7%	35.7%	64.3%
<b>Total</b>	<b>1292</b>	<b>644</b>	<b>551</b>	<b>97</b>	<b>92.5%</b>	<b>42.6%</b>	<b>7.5%</b>

Table 5: Adult and child mortality review status by Specialty, Jan 2024 – Dec 2024

The Trust operates a learning from deaths process that places significant value on case discussion and learning undertaken within specialty and divisional multi-disciplinary teams. These meetings are scheduled throughout the year (monthly) and supported by a wide range of clinical staff and the clinical governance department. This approach to quality ensures learning is agreed and widely cascaded.

Process compliance metrics should be reported to the Quality Committee and Board in arrears as some cases are still progressing and should therefore not be used to draw conclusions regarding process compliance.

### 1.3. Perinatal mortality review

The Perinatal Mortality Review Tool (PMRT) is a national mandatory monitoring and assurance dataset developed by MBRRACE-UK. It is used to collect very detailed information about the care mothers and babies have received throughout pregnancy, birth and afterwards. The purpose of the PMRT is to support hospital learn from deaths by providing a standardised and structured review process.

The PMRT is designed to support review of:

- All late fetal losses (22 weeks + 0 days to 23 weeks + 6 days);
- All antepartum and intrapartum stillbirths;
- All neonatal deaths from birth at 22 weeks + 0 days to 28 days after birth;

Learning from these cases is captured only within the PMRT and not duplicated within the Trust's mortality review system (Datix). The national target is to complete PMRT review within 6 months. The reporting time scales for PMRT do not align within the timescales of this report therefore the below data is 2 quarters behind. During the 3 month period ending June 2024; 9 perinatal deaths were reported to the MBRRACE-UK and a total of 11 cases were identified as requiring PMRT review (including post-neonatal deaths not reported via MBRRACE-UK).

	No. reported	Not supported for review	Review in progress	Review completed	Grading of care: no. with issues in care likely to have made a difference to outcome
Stillbirths and late fetal losses	10	5	0	5	0
Neonatal and post-natal deaths	7	1	0	6	1

Table 6: PMRT review status by case category, 1 April 24 – 30 June 24

Learning from PMRT review is reported to the Mortality Surveillance Group; where sub-optimal care that could have impacted outcome is identified cases are escalated as potential serious incidents. The organisation publishes a Learning from Serious Incidents report on a quarterly basis and outcomes / learning is received by the Patient Safety Group and Executive Management Board on a monthly basis.

## 1.4. Learning Disabilities Mortality Review (LeDeR)

The national Learning Disabilities Mortality Review (LeDeR) programme was established in May 2015 in response to the recommendations from the Confidential Inquiry into premature deaths of people with learning disabilities. From January 2022, LeDeR reports have included deaths of autistic people without a learning disability. In response to this change and following stakeholder engagement, the new name for the LeDeR programme is 'Learning from Life and Death Reviews – people with a learning disability and autistic people'.

The Trust reported 4 deaths to LeDeR in Q3.

Ref	Month of Death	Approval status	Specialty	CESDI grade
MM13900	Dec	Closed	Cardiology	CESDI 1
MM13954	Dec	Closed	Acute Medicine	CESDI 1
MM13559	Oct	Closed	Acute Medicine	CESDI 1
INC148753	Nov	Closed	TransPlus Service	N/A

Table 7: LeDer cases during October – December 2024

The LeDeR programme seeks to coordinate, collate and share information about the deaths of people with learning disabilities and autistic people so that common themes, learning points and recommendations can be identified and taken forward at both local and national levels. The Trust is committed to ensuring deaths of patients with known / pre-diagnosed learning disabilities and /or autism are reported to the LeDeR programme and reviewed accordingly.

Since July 2023 LeDeR notifications are only for those aged 18 years and over. The NWL ICB have LeDeR representatives attend Child Death Review Meetings. This ensures that the death is looked at from a health inequalities/LeDeR perspective. The Child Death Review Team monitor the themes from reviews and continue to share them with the NWL ICB LeDeR team.

## 2. Areas of focus

The Trust's mortality review programme provides a standardised approach to case review designed to improve understanding and learning about problems and processes in healthcare associated with mortality, and also to share best practice.

Where problems in care are identified these are graded using the Confidential Enquiry into Stillbirths and Deaths in Infancy (CESDI) categories:

- Grade 0: No suboptimal care or failings identified and the death was unavoidable
- Grade 1: A level of suboptimal care identified during hospital admission, but different care would NOT have made a difference to the outcome and the death was unavoidable
- Grade 2: Suboptimal care identified and different care MIGHT have made a difference to the outcome, i.e. the death was possibly avoidable
- Grade 3: Suboptimal care identified and different care WOULD REASONABLY BE EXPECTED to have made a difference to the outcome i.e. the death was probably avoidable

During the past 12 months, 497 full mortality reviews have been closed following discussion at specialty, divisional or Trust wide mortality review groups.

Period	CESDI 0	CESDI 1	CESDI 2	CESDI 3
Q4 23/24	125	21	2	0
Q1 24/25	122	12	1	0
Q2 24/25	93	18	2	0
Q3 24/25	92	9		0
Total	432	60	5	0

Table 8: Closed mortality cases by CESDI grade Jan 2024 – Dec 2024

Five cases were identified via the mortality review process as a CESDI 2 (different care MIGHT have made a difference to the outcome, i.e. the death was possibly avoidable). Each of these cases were escalated to the executive for a decision on appropriate learning response.

All cases of suboptimal care are presented to the Mortality Surveillance Group to ensure shared learning across the Trust. There were four cases identified at West Middlesex hospital and one case identified at Chelsea and Westminster hospital. This is within expectations in a patient cohort with increased frailty and comorbidities.

Mortality Ref	CESDI grade	Incident Ref	Site	Area	Category	Incident investigation status
MM11675	CESDI 2	INC124217	WMH	Care Of Elderly	Imaging/Radiation	Finally approved
MM11408	CESDI 2	INC122160	WMH	Paediatric Accident and Emergency	Death: Unexpected / unexplained	Finally approved
MM12159	CESDI 2	INC128857	CWH	Acute Medicine	Patient falls	Finally approved
MM12031	CESDI 2	INC129576	WMH	Gastroenterology	Provision of care / treatment	Finally approved
MM12743	CESDI 2	INC141129	WMH	Acute Medicine	Transfusion, Blood/Blood Products	Finally approved

Table 9: CESDI grade 2 cases linked to incident investigations, Jan 2024 – Dec 2024

Population demographics, hospital service provision, intermediate/community service provision all have an effect on the numbers of incidents occurring on each site. Mortality reviews graded CESDI 2 and 3 will have an associated patient safety incident reported.

The Trust is committed to delivering a just, open and transparent approach to investigations that reduces the risk and consequence of recurrence. Key themes from incident investigations linked to mortality review are submitted to the Patient Safety Group and the Executive Management Group for shared learning and consideration of whether further Quality Improvement Projects, deep-dives, or targeted action is required.

The organisation publishes a learning from Safety learning responses on a monthly basis and outcomes/learning is received by the Patient Safety Group, local Quality Committee and Executive Management Board on a monthly basis (with case outlines and associated actions).

There were 60 cases graded as a CESDI 1 (e.g. level of suboptimal care identified during hospital admission, but different care or management would NOT have made a difference to the outcome and the death was unavoidable). Learning from CESDI 1 cases provides the Trust and our teams with excellent learning from which to develop our improvement approaches.

The following specialist teams have successfully identified CESDI 1 learning opportunities from across the patient journey (not necessary occurring whilst the patient was under the care of that speciality). The identification of CESDI grade 1 cases should not be used to draw conclusions regarding quality and safety within the identifying speciality.

Specialty	CW	WM	Total
Acute Medicine	8	11	19
Care Of Elderly	7	4	11
ICU	6	4	10
Gastroenterology		6	6
Cardiology		5	5
Trauma / Orthopaedics	2	2	4
Urology		2	2
General Surgery		1	1
Colorectal		1	1
Diabetes/Endocrine	1		1
<b>Total</b>	<b>24</b>	<b>36</b>	<b>60</b>

Table 10: CESDI grade 1 cases by Specialty, Jan 2024 – Dec 2024

The Divisional Mortality Review Groups provide scrutiny to mortality cases so as to identify themes and escalate any issues of concerns.

Following the review of cases graded CESDI 1-2, several key themes and issues were identified through mortality reviews and flagged by the Mortality Surveillance Group between January and December 2024, including:

- Timely and accurate completion of Treatment Escalation Plans (TEP) and Do Not Attempt Resuscitation (DNAR) discussions. Consultant-level discussions should be clearly documented in Cerner.
- Inaccurate copying and pasting in Cerner has been a recurring issue lately, and staff are reminded to thoroughly review what they've copied to ensure the information accurately reflects the current situation.
- Communication with families to ensure their understanding of the care plan and manage expectations effectively.
- Gaps in end-of-life care:
  - Recognition and escalation of the actively dying patient, with early involvement of palliative care.
  - The importance of good communication with the families of palliative patients, ensuring that the risks and benefits of the care approach are clearly explained.

### 3. Conclusion

The outcome of the Trust's mortality surveillance programme continues to provide a rich source of learning that is supporting the organisation's safety improvement objectives.

The Trust continues to be recognised as having one of the lowest relative risk of mortality (SHMI) across the NHS in England. The Trust is committed to better understanding the

distribution of mortality according to the breakdown of our patient demographics (Appendix 2) and ensure we tackle any health inequalities that we identify in doing so.

As part of the rollout of the Patient Safety Incident Response Framework (PSIRF) the mortality review template is being used as a learning response tool and the follow-up of safety action plans will be done via the Divisional Mortality Review Groups as well as the Mortality Surveillance Group going forward. Any cases that are escalated as CESDI 2 and 3 are also brought to the weekly Initial Incident Review Group for a proportionate decision on learning response and approval by the executive team.

## 4. Glossary

- 4.1. **Medical Examiners** are responsible for reviewing every inpatient death before the medical certificate cause of death (MCCD) is issued, or before referral to the coroner in the event that the cause of death is not known or the criteria for referral has been met.. The ME will also discuss the proposed cause of death including any concerns about the care delivered with bereaved relatives.
- 4.2. **Specialty M&M** reviews are objective and multidisciplinary reviews conducted by specialties for cases where there is an opportunity for reflection and learning. All cases where ME review has identified issues of concern must be reviewed at specialty based multi-disciplinary Mortality & Morbidity (M&M) reviews.
- 4.3. **Child Death Overview Panel (CDOP)** is an independent review aimed at preventing further child deaths. All child deaths are reported to and reviewed through Child Death Overview Panel (CDOP) process.
- 4.4. **Perinatal Mortality Review Tool (PMRT)** is a review of all stillbirths and neonatal deaths. Neonatal deaths are also reviewed through the Child Death Overview Panel (CDOP) process. Maternal deaths (during pregnancy and up to 12 month post-delivery unless suicide) are reviewed by Healthcare Safety Investigation Branch and action plans to address issues identified are developed and implemented through the maternity governance processes.
- 4.5. **Learning Disabilities Mortality Review (LeDeR)** is a review of all deaths of patients with a learning disability. The Trust reports these deaths to the Local integrated care boards (ICBs) who are responsible for carrying out LeDeR reviews. SJRs for patients with learning disabilities are undertaken within the Trust and will be reported through the Trust governance processes.

## Appendix 1 - Performance Scorecard

	Q4 23/24	Q1 24/25	Q2 24/25	Q3 24/25	Comments	National LfD min. requirement?
<b>Summary data</b>						
Total no. deaths (adult and children)	363	317	272	340	Inpatients deaths only	
Total no. adult deaths	359	316	272	338	Inpatients over 18 years age	Y
Total no. child deaths	4	1	0	2	Inpatients over 28 days and less than 18 year only	
Total no. neonatal deaths	11	7	10	15	Inpatients livebirths under 28 days of age	
Total no. stillbirths	13	7	10	15	Inpatient not live births	
<b>Deaths reviewed by Medical Examiner</b>						
Deaths reviewed by Medical Examiner	100%	100%	100.0%	99%	% of total deaths (row 3)	
Deaths referred for Level 2 review	47%	51%	49%	44%	% of total deaths (row 3)	
Level 2 reviews completed	91%	86%	84%	67%	% of total referrals this quarter	Y
<b>Requests made by a Medical Examiner (Potential learning identified)</b>						
Requests made by a Medical Examiner (Potential learning identified)	40%	47%	46%	53%	% of total referrals	
Potential learning identified (Screening)	29%	37%	43%	37%	% of total referrals	
Concerns raised by family / carers (Screening)	8%	14%	13%	13%	% of total referrals	
Patients with learning disabilities (Screening)	3%	2%	3%	3%	% of total referrals	
Patients with severe mental health issues (Screening)	1%	0%	0%	0%	% of total referrals	
Unexpected deaths (Screening)	9%	11%	9%	11%	% of total referrals	
Requests made by speciality mortality leads through local Mortality and Morbidity review processes	34%	27%	23%	34%	% of total referrals	
Other reason (Linked SI, Inquest, Nosocomial Covid, DMRG request)	17%	8%	1%	3%	% of total referrals	
<b>CESDI 0 - No suboptimal care</b>						
CESDI 0 - No suboptimal care	80%	88%	82%	91%	% of cases reviewed (&closed)	
<b>CESDI 1 - Some sub optimal care which did not affect the outcome</b>						
CESDI 1 - Some sub optimal care which did not affect the outcome	13%	9%	16%	9%	% of cases reviewed (&closed)	
<b>CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death)</b>						
CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death)	1%	1%	2%	0%	% of cases reviewed (&closed)	
<b>CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death)</b>						
CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death)	0%	0%	0%	0%	% of cases reviewed (&closed)	Y

Table 11. Trust mortality review data as at 31/01/2025

**Appendix 2 – Ethnicity breakdown (for Total no. deaths adult and children)**

	Q4 23/24	Q1 24/25	Q2 24/25	Q3 24/25	Total
Data import pending	346				346
White - British	8	143	135	156	442
Other - Not Stated	2	48	43	56	149
White - Any Other White Background		35	16	28	79
Asian or Asian British - Indian	1	25	19	30	75
Other - Any Other Ethnic Group	1	22	11	20	54
Asian - Any Other Asian Background	4	17	15	14	50
Asian or Asian British - Pakistani		5	14	10	29
Black or Black British - African		4	5	5	14
White - Irish	1	5	3	5	14
Black or Black British - Caribbean		6	2	5	13
Black - Any Other Black Background		1	4	3	8
Mixed - Any Other Mixed Background		2	3	2	7
Other - Chinese		1	1	3	5
Asian or Asian British - Bangladeshi		2		1	3
Mixed - White and Black African		1	1	1	3
Mixed - White and Asian				1	1
<b>Total</b>	<b>363</b>	<b>317</b>	<b>272</b>	<b>340</b>	<b>1292</b>

NWL Acute Provider Collaborative Board in Common (Public)

29/04/2025

Item number: 4.1.3b

This report is: Public

# Imperial College Healthcare NHS Trust Learning from Deaths quarterly report – Quarter Three 2024/25

Author: Heena Asher & Shona Maxwell  
Job title: General Manager & Chief of Staff

Accountable director: Professors Julian Redhead & Raymond Anakwe  
Job title: Medical directors

## Purpose of report

Purpose: Assurance

This report presents the data from the Learning from Deaths programme for Quarter Three (Q3) of 2024/25 for information. It is a statutory requirement to present this information to the Trust public board. This is being achieved through presentation to the Trust Standing Committee, with an overarching summary paper drawing out key themes and learning from the individual reports from the four NWL acute provider collaborative (APC) trusts presented to the APC quality committee and then Board in common.

## Report history

### Learning from deaths forum

Various

The group discussed and agreed the content of this report, including themes for learning and improvement.

### Executive Management Board – Quality and Executive Management Board

01/02/2025

The committees noted the findings from our learning from deaths programme and approved the report for onward submission to Quality Committee.

### Quality committee and Standing Committee

06/03/25 and 08/04/25

The report was noted and approved for onward submission.

## Executive summary and key messages

- 1.1. Mortality rates remain statistically significantly low when compared nationally. The HSMR methodology has recently changed, despite this our rate remains amongst the lowest nationally.
- 1.2. All deaths in the quarter have been reviewed by the Medical Examiner, with cases where there are concerns about the quality of care referred for structured judgment review (SJR). Completed SJRs have identified examples of excellent team working and good communication with families. No new themes for improvement were identified with ongoing work to improve treatment for patients with signs of deterioration as part of our safety improvement programme.
- 1.3. There were five SJRs which identified some sub-optimal care which might or would reasonably have been expected to have made a difference to the patient's outcome. These are all investigated through the patient safety incident investigation framework (PSIRF) to confirm the learning response.
- 1.4. This level of scrutiny is important to ensure all issues are considered and questions from the bereaved are highlighted and answered. The low number of issues found that affected the outcome and our low mortality rates are positive reflections of the care delivered.
- 1.5. New statutory requirements relating to death certification came into effect in September 2024 with a marked increase in referrals to the Medical Examiner service this quarter from community providers. We continue to improve our internal processes to make the service more effective for bereaved families and engage with community partners to ensure we can effectively embed the new ways of working required across the system.

## Impact assessment

Quality

Quality impact: Improving how we learn from deaths which occur in our care will support identification of improvements to quality and patient outcomes.

## Strategic priorities

- Continuous improvement in quality, efficiency and outcomes including proactively addressing unwarranted variation (APC)
- Develop a sustainable portfolio of outstanding services (ICHT)
- Build learning, improvement and innovation into everything we do (ICHT)

## Key risks arising from report

The Committee is asked to note the findings from our mortality surveillance programme in Q3 2024/25 with no new issues to escalate. There is an ongoing risk around delays with issuing MCCDs which impact our bereaved families. We have increased medical examiner resource and an improvement plan is in place.

## Main Report

### 2. Learning and Improvements

- 2.1. Learning from Deaths (LFD) is a standard monthly agenda item on all Divisional Quality and Safety meetings where investigations and learning are shared which is then disseminated to all the directorates and throughout the division.
- 2.2. 50 structured judgment reviews (SJRs) were completed in this quarter (45 for deaths which occurred in Q3, and 5 for deaths which occurred in Q2) of which 31 cases (62%) identified patients received good or excellent care. 23 cases (46%) identified good communications with the next of kin, which has seen improvements across previous quarters.
- 2.3. Two cases (4%) showed issues around the importance of effectively responding to patient deterioration. This is a recurring area for improvement identified through SJRs. Improving treatment of patients with signs of deterioration remains a safety priority.
- 2.4. Five SJRs identified that sub-optimal care might have or would reasonably be expected to have made a difference to the patient's outcome (CESDI 2 and 3). Four of these occurred within intensive care and one in the Emergency department. No common themes have been identified but patient safety investigations are underway.

### 3. Key themes

#### 3.1. Mortality rates

- 3.1.1 Our mortality rates remain statistically significantly low. The rolling 12-month HSMR has increased slightly to 76.1 (compared to 73.7 in the previous quarterly report) and is 5th lowest when compared nationally. Our SHMI remains the second lowest at 73.32.
- 3.1.2 The small increase in HSMR can be attributed to the changes in methodology introduced in December 2024. This included removal of the adjustment for palliative care coding, implementation of a new comorbidity framework, use of a new devaluation scoring system and changes in the diagnostic groupings which make up the ratio.
- 3.1.3 Some directorates, such as Renal, Trauma, and Specialist Surgery, have seen increases of over 10 in their rates which Telstra Health have confirmed is likely linked in most cases to the methodology changes.
- 3.1.4 Maternity's rate has significantly reduced from over 100 to 0, which is likely due to the removal of 'other perinatal conditions' as a diagnosis group, but WLCH has seen an increase which is thought to be linked to the changes in maternity. Both are under review. Crude deaths during this period remained stable.
- 3.1.5 At Site level, CXH and SMH's HSMR is consistently low, with HH varying more but always within or below expected range, and never over 100.
- 3.1.6 There has been a period of recent increase at HH, likely linked to the rising HSMR in Cardiology and recent alerts for the acute myocardial infarction (AMI) diagnostic group due to the services operating on that site. This is being reviewed by the Hospital Medical Director for Hammersmith Hospital. Findings will be included in the Q4 report.

#### 3.2. Diagnostic group reviews

- 3.2.1 Reviews into the AMI and Asthma diagnostic groups have begun following alerts in Q3. A review of non-AMI deaths in Cardiology is also underway following an increase in HSMR above the national benchmark of 100 in August 2024, although this score is still within the expected range. These reviews are progressing and will be completed in Q4 and included in the next Learning from Deaths report. The reviews are complex meaning they are taking longer than we would have liked. No additional safety concerns have been noted in these areas during this period.

### 3.3. **Directorate reviews**

3.2.2 December saw an increase in crude death numbers (n=204), the highest since January 2023, which is likely to be due to seasonal variation. Directorates with increases will be reviewed via the LFD forum, with outputs reported in the next quarterly report.

### 3.4. **Medical Examiner reviews**

3.4.1. The Medical Examiner (ME) service continues to provide independent scrutiny of 100% of inpatient deaths. The service made 138 referrals to the Coroner in this quarter, which is an increase from 107 cases in the previous quarter. 46 will be taken to an inquest.

3.4.2. The largest percentage of coronial referrals were death resulting from violence, trauma, or injury (38%), reflecting the major trauma centre at SMH. The most common reason in the previous quarter was death associated with medical procedures or treatments (34%). Several of these cases involved patients who had undergone procedures or treatments at other hospitals prior to transfer to ICHT. All such cases are reviewed to determine whether incidents requiring further investigation have occurred. While no issues currently require escalation, this continues to be monitored.

3.4.3. Weekly review continues of all new cases to ensure investigations and file preparation can begin as early as possible where required. The increase in referrals and inquest listing over the last 3 years continues to cause resource implications, delays in response submission and adjournment requests. A restructure of the team in the MDO has completed with additional support and resource provided.

3.4.4. All non-coronial deaths within London boroughs of Hammersmith & Fulham and Westminster are now scrutinised by the Medical Examiner service following implementation of the death certification reforms on 9 September. Our service scrutinised 233 non-acute deaths in this quarter, an increase as more primary care and independent providers came on board with the process.

3.4.5. During this quarter, the service issued 60% of urgent MCCDs within 24 hours of death and 40% of non-urgent MCCDs within three calendar days. Whilst efforts have been made to improve the timeliness, this is being impacted by the increase in community referrals. Additionally, the increase in reported deaths during December, combined with the impact of additional bank holidays, has contributed to a reduction when compared to the previous quarter. Additional resource has been recruited and now commenced, a new rota implemented and data is being monitored and escalated in an increasingly timely way to directorates where required.

3.4.6. The service has embedded monthly governance processes to monitor KPIs and investigate cases that do not meet the expected turnaround time to identify potential improvements. Further work to reduce delays is underway, including more focussed support and engagement with clinical directors and heads of specialties when expected timelines are not met. This is reviewed monthly with divisions at the LFD forum.

### 3.5. **Structured Judgement reviews (SJR)**

3.5.1. The percentage of inpatient deaths referred for a SJR is slightly reduced (9% compared to 13% in Q2) with 'unexpected death' the most common reason (32%).

3.5.2. 82% of SJRs (n=37) found no suboptimal care (CESDI 0) compared to 77% in Q2 and 84% in Q1. Reviews have identified evidence of excellent care in many cases.

3.5.3. A further 7% of reviews (n=3) found some suboptimal care but this did not affect the patient outcome (CESDI 1) compared to 12% in Q1 and 16% in Q2. All CESDI 1 cases are reviewed to decide whether a further incident investigation is required and the harm levels. One case has been confirmed as no harm and one as low harm following review.

- 3.5.4. This quarter, 7% (n=3) found that suboptimal care may have made a difference to the patient outcome (CESDI 2). Two cases occurred in critical care and one in ED. No common themes were identified.
- 3.5.5. 4% of reviews (n=2) identified sub-optimal care which would reasonably be expected to have made a difference to the outcome (CESDI 3). Both cases occurred in critical care.
- 3.5.6. A directorate breakdown of SJR outcomes from this quarter is in the table below.
- 3.5.7. 4% of reviews (n=2) identified sub-optimal care where it would reasonably be expected to have made a difference to the outcome (CESDI 3). Both cases occurred in critical care.
- 3.5.8. All cases with a CESDI 2 or 3 outcome automatically trigger an immediate incident review (IIR). Once all investigations have been completed, the case is discussed at the Death Review Panel (DRP), which triangulates and agrees a final outcome, learning and improvements that need to be implemented.

#### **4. Other mortality review processes**

##### **4.1. PMRT**

- 4.1.1. The maternity and neonatal services have reported 23 perinatal deaths to MBRRACE-UK in Q3, of which 16 (10 stillbirths and 6 neonatal deaths) were eligible for full review under the PMRT framework.
- 4.1.2. Of the 16 cases eligible, 10 have been discussed at multidisciplinary panel review meetings, 6 are scheduled in Q4. There are no cases with a grading C/D in Q3. However, following an initial review (not yet formally discussed at PMRT panel) one case was highlighted as having potential significant care issues. A PSII has been declared.
- 4.1.3. Of the 10 stillbirths, one case (antenatal stillbirth at 38+4) showed missed opportunities related to the use of an interpreter throughout the woman's care. Learning and actions from this have fed into the wider Interpretation improvement work. Improving access to interpreting services has been identified as a key priority for Maternity in 2025/26.

##### **4.2. LeDeR**

- 4.2.1. Six SJRs have been completed in this quarter for patients with a learning disability, five of which found no sub-optimal care. There were common themes identified around excellent communication with families and support offered from the safeguarding team.
- 4.2.2. One review found some sub-optimal care where different care might have made a difference to the patient's outcome (CESDI 2). This was for a patient with Downs syndrome, very unwell with existing comorbidities who had been an inpatient for two months prior to death. There were challenges with sedation and clinical monitoring and responding in line with best practice. An After Action Review (AAR) is underway.
- 4.2.3. The Safeguarding team have completed LeDeR referrals for all cases that occurred.

##### **4.3. CDOP**

- 4.3.1. There were 5 deaths reported during this quarter for WLCH.
- 4.3.2. CDOP referrals have been made for all deaths and detailed investigations will now take place. These reviews can take several months.
- 4.3.3. A case reviewed in December by the North West London Overview panel involved a mother who had not been assessed for aspirin suitability. Although PMRT determined this did not impact the outcome, it highlighted the importance of thorough risk assessments, consistent documentation, and effective communication between trusts to ensure appropriate care and patient safety.

#### **5. Areas of focus**

##### **5.1. Ethnicity**

- 5.1.1. Analysis conducted in quarter one of ethnicity data of patients who died in the Trust from 2017 to 2023 identified lower than expected mortality rates for all ethnic groups but that we had a slightly higher than average number of patients where ethnicity was unknown.

- 5.1.2. Last quarter work was completed to include ethnicity data from NWL Whole System Integrated Care (WSIC) platform into our data set with the aim of improving data quality and reducing unknown numbers and the percentage of deaths in 2024/25 where ethnicity is unknown reduced from 17% when only using data from Cerner to 9% for the combined data set. This has further improved to 6% for Q3 (Appendix B).
  - 5.1.3. Work continues with the support of the Health Inequalities programme team to analyse this data from a population health perspective and to understand inequalities in services. The next steps will be to include data relating to hospital services used by deceased patients to reveal any differences in healthcare access or use of services. We will also bring in additional demographic details, including age, gender, deprivation and primary language to expand the data set used and widen this analysis work. Further areas of focus are under discussion.
- 5.2. Specialty Mortality and Morbidity meetings**
- 5.2.1. The LFD forum continues to monitor compliance with the Trust Specialty M&M guidance that was agreed and implemented in January 2024.
  - 5.2.2. There is evidence in Datix that Specialty M&M meetings are being held regularly in a number of specialties, including Cardiology and Renal. The Stroke and Neurosciences directorate has established new processes from Q2. Work continues to ensure outcomes are transferred and captured on Datix to accurately reflect the improvements.
  - 5.2.3. Compliance across the Trust remains low. Divisional action plans are being monitored through the divisional performance and accountability review meetings.

## **6. Conclusion**

- 6.1 Mortality rates across the Trust remain statistically significantly low. When considered with our harm profile and the outcomes of our SJRs we can provide assurance to the committee that we are providing safe care for the majority of our patients. Where care issues are found we have a robust process for referral for more in-depth review, the outcome of which is reported through the incident report and the quality function report to EMB and Quality Committee.

## Appendix A – Acute Provider Collaborative performance scorecard

Financial Year	2023-2024			2024-2025		
Financial Quarter	Q2	Q3	Q4	Q1	Q2	Q3
No. Deaths	414	445	459	432	379	512
No. Adult Deaths	392	419	437	412	358	484
Adult Deaths per 1000 Elective Bed Days	0.04	0.04	0.04	0.03	0.03	0.04
No. Child Deaths	5	9	10	7	8	9
No. Neonatal Deaths	7	9	5	5	8	7
No. Stillbirths	10	8	7	8	5	12
ME Reviewed Deaths in Qtr	404	437	449	422	372	497
% ME Reviewed Deaths - Deaths (excl Stillbirths) in Qtr	100%	100%	100%	100%	100%	100%
SJRs Requested for Deaths in Qtr	67	76	75	51	46	45
% SJRs Requested for Deaths in Qtr of total adult deaths in Qtr	17%	18%	17%	12%	13%	9%
No. SJRs Completed in period	65	63	84	54	46	47
SJRs Completed for Deaths in Qtr	67	76	75	51	46	45
% SJRs Completed for Deaths in Qtr	100%	100%	100%	100%	100%	100%
No. LeDeR Completed	6	4	5	0	1	0
Requests made by a Medical Examiner - SJRs Requested for Deaths in Qtr	14	7	22	11	8	8
% Requests made by a Medical Examiner - SJRs Requested for Deaths in Qtr	21%	9%	29%	22%	17%	18%
Concerns raised by family / carers - SJRs Requested for Deaths in Qtr	8	12	6	13	8	12
% Concerns raised by family / carers - SJRs Requested for Deaths in Qtr	12%	16%	8%	25%	17%	27%
Patients with learning disabilities - SJRs Requested for Deaths in Qtr	6	4	6	5	2	6
% Patients with learning disabilities - SJRs Requested for Deaths in Qtr	9%	5%	8%	10%	4%	13%
Patients with severe mental health issues - SJRs Requested for Deaths in Qtr	2	1	2	1	2	2
% Patients with severe mental health issues - SJRs Requested for Deaths in Qtr	3%	1%	3%	2%	4%	4%
Unexpected deaths - SJRs Requested for Deaths in Qtr	37	48	39	17	25	17
% Unexpected deaths - SJRs Requested for Deaths in Qtr	55%	63%	52%	33%	54%	38%
Elective admission deaths - SJRs Requested for Deaths in Qtr	5	6	6	5	2	3
% Elective admission deaths - SJRs Requested for Deaths in Qtr	7%	8%	8%	10%	4%	7%
Requests made by speciality mortality leads / through local Mortality and Morbidity review processes - SJRs Requested for Deaths in Qtr	1	1	1	0	1	1
% Requests made by speciality mortality leads / through local Mortality and Morbidity review processes - SJRs Requested for Deaths in Qtr	1%	1%	1%	0%	2%	2%
CESDI 0 - No suboptimal care - Completed SJRs for Deaths in Qtr	55	69	62	44	36	37
% CESDI 0 - No suboptimal care - Completed SJRs for Deaths in Qtr	82%	91%	83%	86%	78%	82%
CESDI 1 - Some sub optimal care which did not affect the outcome - Completed SJRs for Deaths in Qtr	8	6	7	6	7	3
% CESDI 1 - Some sub optimal care which did not affect the outcome - Completed SJRs for Deaths in Qtr	12%	8%	9%	12%	15%	7%
CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death) - Completed SJRs for Deaths in Qtr	3	1	6	1	3	3
% CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death) - Completed SJRs for Deaths in Qtr	4%	1%	8%	2%	7%	7%
CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death) - Completed SJRs for Deaths in Qtr	1	0	0	0	0	2
% CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death) - Completed SJRs for Deaths in Qtr	1%	0%	0%	0%	0%	4%

## Appendix B – Ethnicity data

	North West London		Ethnicity breakdown of all inpatient encounters in the Trust	Cerner data		Combined data set (WSIC and Cerner)		Difference (Combined-Cerner)	
	2021 Census data			2023/2024	2024/2025		2024/2025		
Ethnicity	Population	% population		No. Deaths	% Deaths	No. Deaths	% Deaths	No. Deaths	% Deaths
<b>Totals</b>	<b>2,092,995</b>	<b>100.00%</b>	<b>100%</b>	<b>1322</b>	<b>100.00%</b>	<b>1322</b>	<b>100.00%</b>	<b>0</b>	<b>0.00%</b>
Asian - Any Other Asian Background	154,465	7.38%	6.30%	57	4.31%	61	4.61%	4	0.30%
Asian or Asian British - Bangladeshi	24,738	1.18%	0.86%	8	0.61%	7	0.53%	-1	-0.08%
Asian or Asian British - Indian	329,149	15.73%	6.98%	84	6.35%	101	7.64%	17	1.29%
Asian or Asian British - Pakistani	79,645	3.81%	2.44%	19	1.44%	35	2.65%	16	1.21%
Black - Any Other Black Background	23,316	1.11%	2.85%	33	2.50%	20	1.51%	-13	-0.98%
Black or Black British - African	125,609	6.00%	6.05%	38	2.87%	55	4.16%	17	1.29%
Black or Black British - Caribbean	64,165	3.07%	4.29%	77	5.82%	98	7.41%	21	1.59%
Mixed - Any Other Mixed Background	38,560	1.84%	1.94%	8	0.61%	14	1.06%	6	0.45%
Mixed - White and Asian	30,428	1.45%	0.70%	4	0.30%	8	0.61%	4	0.30%
Mixed - White and Black African	15,927	0.76%	0.69%	3	0.23%	5	0.38%	2	0.15%
Mixed - White and Black Caribbean	23,379	1.12%	0.84%	6	0.45%	11	0.83%	5	0.38%
Other - Any Other Ethnic Group	109,126	5.21%	10.74%	199	15.05%	152	11.50%	-47	-3.56%
Other - Chinese	31,268	1.49%	1.06%	4	0.30%	3	0.23%	-1	-0.08%
Other - Not Known	n/a	n/a	0.46%	20	1.51%	14	1.06%	-6	-0.45%
Other - Not Stated	n/a	n/a	7.62%	151	11.42%	69	5.22%	-82	-6.20%

White - Any Other White Background	344,734	16.47%	18.07%	139	10.51%	192	14.52%	53	4.01%
White - British	563,903	26.94%	25.48%	400	30.26%	395	29.88%	-5	-0.38%
White - Irish	44,291	2.12%	2.63%	49	3.71%	69	5.22%	20	1.51%
Arab	77,548	3.71%	These ethnic groups are not recorded within the NHS as they are not part of the organisational data set						
Gypsy Or Irish Traveller	1,665	0.08%							
Roma	11,079	0.53%							

NWL Acute Provider Collaborative Quality Committee

29/04/2025

Item number: 4.1.3c

This report is: Public

# London North West University Healthcare NHS Trust Learning from Deaths Report Quarter 3 2024/25

Author: Laila Gregory  
 Job title: Head of Clinical Effectiveness

Accountable director: Jon Baker  
 Job title: Chief Medical Officer

## Purpose of report (for decision, discussion or noting)

Purpose: Assurance

This report presents the data from the Learning from Deaths programme for 2024/25 quarter 3 (Q3). It is a statutory requirement for Trusts to present this information to their boards; this is achieved through the presentation of this report to the LNWH Quality & Safety Committee and the submission of overarching learning drawn from across the acute provider collaborative (APC) to the APC Quality Committee and Board in common.

## Report history

Outline committees or meetings where this item has been considered before being presented to this meeting.

**Trust Executive Group**  
 19/02/2025  
 What was the outcome?

**Trust Quality & Safety Committee**  
 27/02/2025  
 What was the outcome?

**APC Mortality Surveillance Group**  
 26/02/2025  
 What was the outcome?

## Executive summary and key messages

The new model for HSMR (HSMR+) has had a small negative impact for Trust. Under the old model the rate was 93.1, which was a statistically significantly low mortality risk (and well below the NHS benchmark of 100). The new HSMR+ year to August 2024 is 95.0, which is statistically low but places the trust in the 'expected range' for mortality. While the trust is not in line with other London peers (non-specialist), it continues to outperform the NHS at regional level.

During the 12-month period to end of December 2024; 100% in-hospital adult and child deaths were recorded within the Trust's mortality review system (Datix), of these 100% have been screened and 359 have undergone level 2 in-depth review.

During Q3 2024/25; 19 cases with areas of sub-optimal care, treatment or service delivery have been identified at time of reporting. The Trust places significant value on case discussion and learning undertaken within specialty and divisional multi-disciplinary teams; for this reason teams are given 4 months to complete level 2 mortality review, therefore 7% of cases occurring in Q3 remain open and within review timeframe.

Where potential for improvement is identified learning is shared at Divisional Boards / groups and presented to the Trust-wide Learning from Patient Deaths Group; this ensures outcomes are shared and learning is cascaded.

## Impact assessment

Tick all that apply

- Equity
- Quality
- People (workforce, patients, families or carers)
- Operational performance
- Finance
- Communications and engagement
- Council of governors

Click to describe impact

## Reason for private submission (For Board in Common papers only)

Tick all that apply [*delete section if not applicable*]

- Commercial confidence
- Patient confidentiality
- Staff confidentiality
- Other exceptional circumstances

If other, explain why

## Strategic priorities

Tick all that apply

- Achieve recovery of our elective care, emergency care, and diagnostic capacity (APC)
- Support the ICS's mission to address health inequalities (APC)
- Attract, retain, develop the best staff in the NHS (APC)

- Continuous improvement in quality, efficiency and outcomes including proactively addressing unwarranted variation (APC)
- Achieve a more rapid spread of innovation, research, and transformation (APC)
- Help create a high quality integrated care system with the population of north west London (ICHT)
- Develop a sustainable portfolio of outstanding services (ICHT)
- Build learning, improvement and innovation into everything we do (ICHT)

## Key risks arising from report

### Main Report

#### 1. Learning and Improvements

The Trust's Mortality Surveillance programme offers assurance to our patients, stakeholders, and the Board that high standards of care are being provided and that any gaps in service delivery are being effectively identified, escalated, and addressed. This report provides a Trust-level quarterly review of mortality learning for Q3 2024/25.

All in-hospital deaths are scrutinised by the Trust's Medical Examiner Service; this initial screening provides an independent review of care and is the basis for triggering cases for enhanced (level 2) review by the Consultant Mortality Validators and the specialities involved.

The Trust undertakes in-depth (level 2) mortality review for cases meeting the following criteria:

National triggers:

- Potential learning identified at Medical Examiner scrutiny.
- Significant concerns raised by the bereaved.
- Deaths of patients with learning disability
- Deaths of patients under a mental health section
- Unexpected deaths
- Maternal deaths
- Deaths of infants, children, young people, and still births
- Deaths within a specialty or diagnosis / treatment group where an 'alarm' has been raised (e.g. via the Summary Hospital-level Mortality Indicator or other elevated mortality alert, the CQC or another regulator)

Local triggers:

- Deaths post elective surgery (at most recent admission)
- Deaths accepted by the Coroner for inquest / investigation.

During Q3 2024/25 deaths accepted by the coroner for inquest or investigation were added to the Trust's local trigger list for in-depth (level 2) review by the Trust's Consultant Mortality Validators

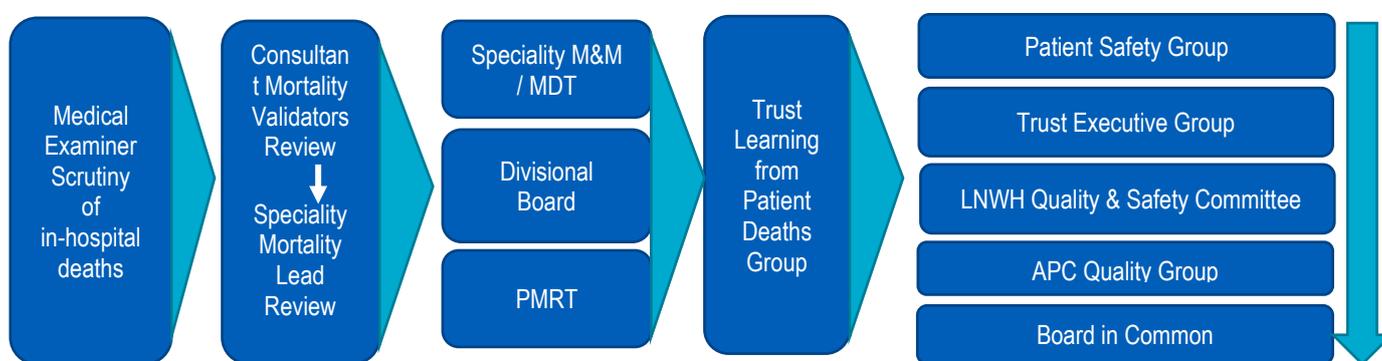
and the specialities providing care to the patient (as required). This addition has supported the identification of learning opportunities, providing enhanced assurance to the Trust and the bereaved, and support the Coroner’s inquest processes.

The addition of this local trigger has resulted in an upward trend of cases requiring in-depth review as at end of December, however, review completion performance remains strong.

2023-24	2024-25		
Q4	Q1	Q2	Q3
98%	94%	94%	93%

Tab 1: Percentage of completed level 2 reviews by quarter

The Learning from Patient Deaths Group (LfPDG) challenges assurance regarding performance and outcomes from the Trust’s learning from deaths approach as outlined below:



The Learning from Patient Deaths Group (LfPDG) provides leadership to this programme of work and is supported by standing items on relative risk of mortality, potential learning from medical examiners, learning from inquests, and divisional learning from mortality review. The LfPDG is a sub-group of the Patient Safety Group and is aligned to the remit of the Quality and Safety Committee.

## 2. Relative Risk

The Trust uses the Summary Hospital-level Mortality Indicator (SHMI) and Hospital Standardised Mortality Ratio (HSMR) to monitor the relative risk of mortality. Both tools are used to determine the relative risk of mortality for each patient and then compare the number of observed deaths to the number of expected deaths; this provides a relative risk of mortality ratio.

Population demographics, hospital service provision, intermediate / community service provision has a significant effect on the numbers of deaths that individual hospital sites should expect; the SHMI and HSMR are designed to reduce this impact and enable a comparison of mortality risk across the acute hospital sector. By monitoring relative risk of mortality, the Trust is able to make comparisons between peer organisations and seek to identify improvement areas where there is variance.

## 2.1. Summary Hospital-level Mortality Indicator (SHMI)

The SHMI is the ratio between the actual number of patients who die following hospitalisation at the Trust and the number that would be expected to die on the basis of average England figures, given the characteristics of the patients treated there. The SHMI calculation includes 100% of in-hospital deaths (excluding still-births) and those deaths that occur within 30 days of discharge. The SHMI is composed of 144 different diagnosis groups, and these are aggregated to calculate the overall SHMI value for each organisation.

The Trust is the 10th best performing acute provider in England in relation to the SHMI relative risk of mortality indicator. The Trust-wide SHMI for the period September 2023 – August 2024 is 0.8649 (where a number below 1 represents lower than expected risk of mortality).

### North West London Acute Collaborative SHMI indicators

Trust	SHMI	Observed Deaths	Expected Deaths	Provider Spells	% mortality: elective admission	% mortality: Palliative care coding	% mortality: 30 days post discharge
LNWH	0.86	2,755	3,190	106,505	0.0%	42%	26%
CWH	0.70	1,700	2,440	102,805	0.0%	45%	25%
ICH	0.71	2,080	2,930	115,340	0.0%	65%	25%
THH	0.98	945	965	49,685	0.0%	54%	29%

Tab 2, Data Source: NHS England, SHMI, September 2023 – August 2024, published 09/01/2025.

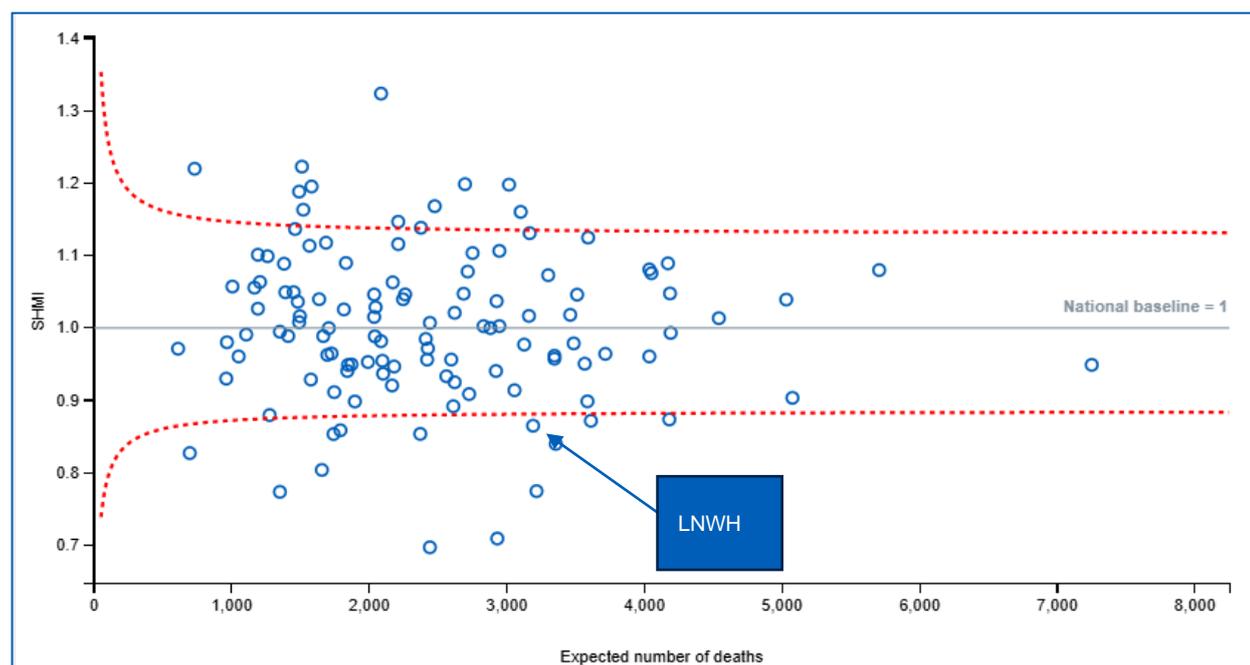


Fig 1 – SHMI, NHS England acute hospitals September 2023 – August 2024, published 09/01/2025.

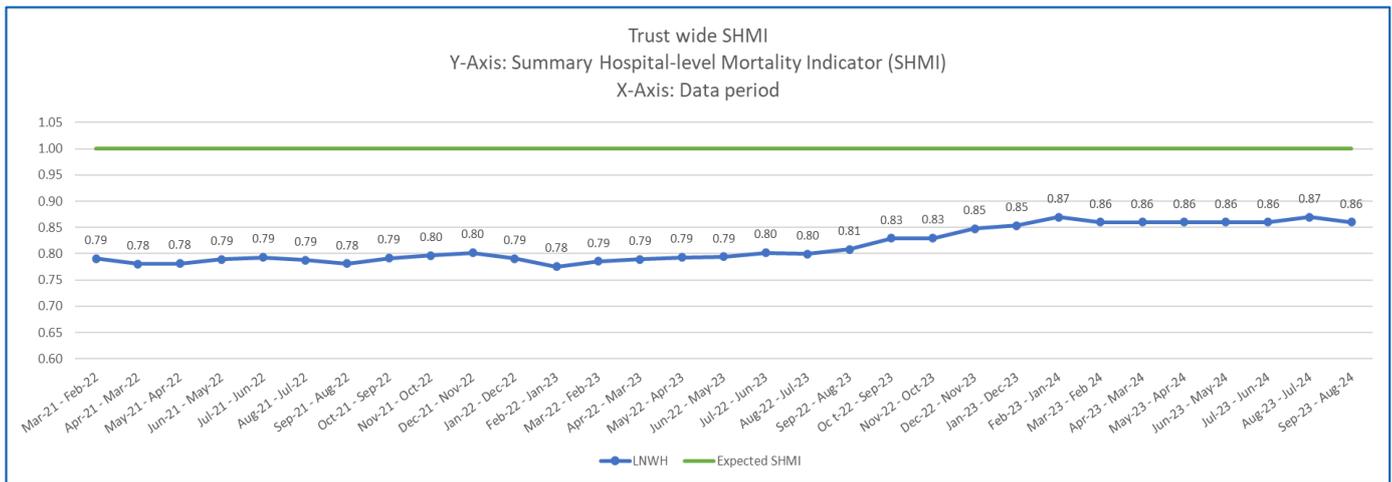


Fig 2 – Trust wide SHMI by reporting period, March 2021 to Aug 2024.

This positive assurance is reflected across the Trust as the organisation’s principal sites continue to operate below the nationally expected relative risk of mortality:

- Northwick Park Hospital: 0.88 (2,130 expected, 1,875 observed, 77,115 provider spells)
- Ealing Hospital: 0.74 (985 expected, 730 observed, 24,900 provider spells)
- St. Marks Hospital: SHMI value ‘not calculated’ (25 expected, 20 observed, 500 provider spells)
- Central Middlesex Hospital: 0.46 (20 expected, 10 observed, 2,700 provider spells).

Whilst the Trust continues to operate significantly below the national relative risk of mortality a small increase in the SHMI metric has been observed since September 2023.

### 2.1.1. SHMI Diagnostic groups

The SHMI is made up of 142 different diagnostic groups which are then aggregated to calculate the Trust’s overall relative risk of mortality. The Learning from Patient Deaths Group monitors expected and observed deaths across diagnostic groups; where statistically significant variation is identified the group undertakes coding and care review to identify any themes or potential improvement areas.

The trust is currently participating in the Same Day Emergency Care (SDEC) pilot under the aegis of NHSE which by the latter’s own acknowledgement may result in detrimental effects on SHMI performance. This is because it removes a high volume of low-risk spells from the Admitted Patient Care dataset from which the SHMI was derived. Even with this occurrence, and with all trusts not due to adopt this protocol until July 2025, LNWH is still a significantly low risk SHMI provider, one of only twelve in the NHS. The SHMI for Year to July 2024 is 86.77, with 2750 deaths observed against an expected 3170 given case mix.

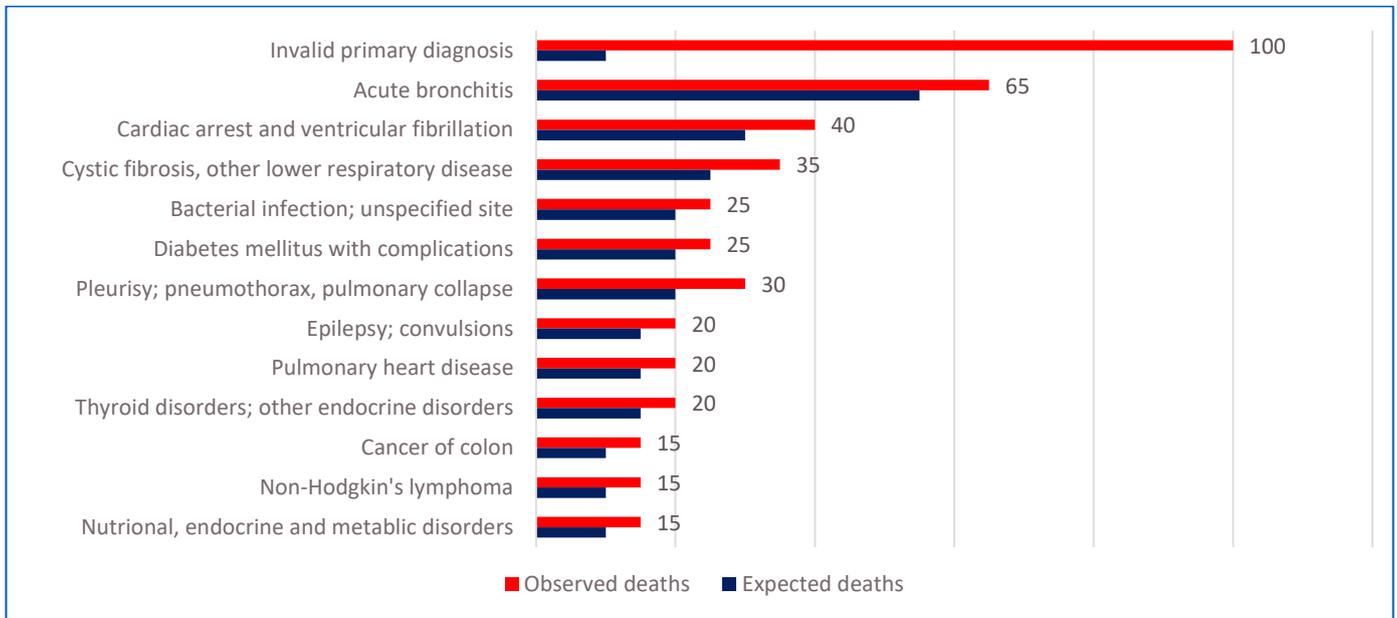


Fig 3: Expected deaths greater than observed deaths by diagnostic group, SHMI comparison of England acute hospital Trusts September 2023 – August 2024, published 09/01/2025.

## 2.2. Hospital Standardised Mortality Ratio (HSMR)

The HSMR compares the number of patients who die following hospitalisation at the Trust and the number that would be expected to die based on the type of cases treated. The HSMR calculation includes 80% of in-hospital deaths (including still-births); it excludes deaths post discharge and cases with palliative care coding.

The new model for HSMR (HSMR+) has had a small negative impact for Trust. Under the old model the rate was 93.1, which was a statistically significantly low mortality risk (and well below the NHS benchmark of 100, the 'average' NHS performance). The new HSMR+ for the year to the August 2024 is 95.0, which is also statistically low risk but very narrowly, so once the higher confidence interval breaks the figure of 100, the trust's status goes into the 'expected range' for mortality.

Based on the 41 top diagnostic groups the Trust's HSMR for period November 2023 to October 2024 is 95.0 (where a number below 100 represents lower than expected risk of mortality).

North West London Acute Collaborative HSMR based on top 56 diagnostic groups:

Trust	HSMR	Observed Deaths	Expected Deaths	Volume
LNWH	95.0	1,536	1,616	48,295
CWH	87.5	1,015	1,162	43,995
ICH	75.0	1,290	1,719	50,025
THH	102.9	565	549	20,345

Tab 3: Data Source: Telstra, HSMR (41 diagnostic groups) by APC provider, November 2023 – October 2024

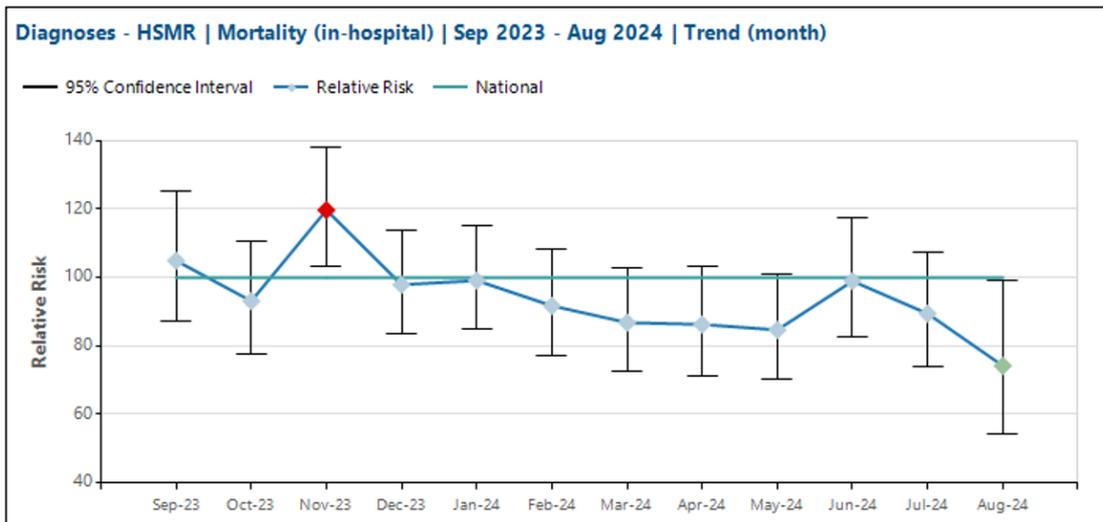


Fig 4: Data Source: Telstra, HSMR trend (56 diagnostic groups), September 2023 – August 2024

The most recent data available shows that the Trust continues to operate below the expected relative risk of mortality based on HSMR trend for the top 41 diagnostic groups.

### 2.2.1. HSMR Diagnostic groups

During Q3 2024/25, the Learning from Patient Deaths Group had its first access to HSMR diagnostic categories with higher-than-expected mortality rates, due to the trusts renewal of the Telstra Health UK contract (formerly known as Dr Foster).

The following diagnostic groups indicate higher than expected relative risk of mortality:

Diagnostic group alerts	Volume	Observed	Expected	Relative risk
Residual codes, unclassified	8,696	294	139	210.4
Bacterial infection, unspecified site	367	16	9	177.1
Cardiac arrest and ventricular fibrillation	51	31	25.9	119.7
Haemorrhoids	1,544	2	0.2	1070.6
Immunity disorders	40	1	0	9747.6
Other nutritional, endocrine, and metabolic disorders	1,326	8	5	210.4

Tab 4: Data Source: Telstra, Diagnostic groups with CUMSUM alerts, November 2023 – October 2024

The appropriate response to these diagnostic group alerts will be determined by the Learning from Patient Deaths Group; learning / outcomes will be described within the Trust's Q4 update.

### 2.2.2. Trust response to HSMR and SHMI alerts

During Q3 24/25 the Learning from Patient Deaths Group (LfPDG) considered diagnostic groups with higher observed deaths than expected and reviewed the Cardiac arrest and ventricular fibrillation patients.

A review of this diagnostic group found 39 cases outlying alerted with significantly higher mortality risk during Q3 2024/25, of the 38 cases one could not be traced (as Telstra does not hold patient identifiable data). Of the remaining 37 cases 82% (n=31) were confirmed as out of

hospital cardiac arrests, that received appropriate treatment and escalation to ITU as required. Each of these cases were graded as CESDI Grade 0, with no sub-optimal care identified.

The LfPD Group took assurance from this review, as the findings were concurrent with the review undertaken during Q4 2023/24.

### 3.0 Crude Mortality

Acute activity and the crude number of deaths occurring during that reporting activity can be used to calculate the rate of in-hospital deaths per 1,000 patient spells (this calculation excludes elective and obstetric activity).

Crude mortality rates must not be used to make comparisons between sites due to the effect that population demographics, services offered by different hospitals, and services offered by intermediate / community care has on health outcomes (e.g. crude mortality does not consider the external factors that significantly influence the relative risk of mortality at each site). Crude mortality is useful to inform resource allocation and strategic planning.

The following crude rates include only adult acute admitted spells by age band (>17). This approach is used as it reduces some of the variation when comparing sites and supports understanding and trend recognition undertaken by the Learning from Patient Deaths Group.

#### Trust wide – Adults, crude mortality rate per 1000 acute admissions (adults)

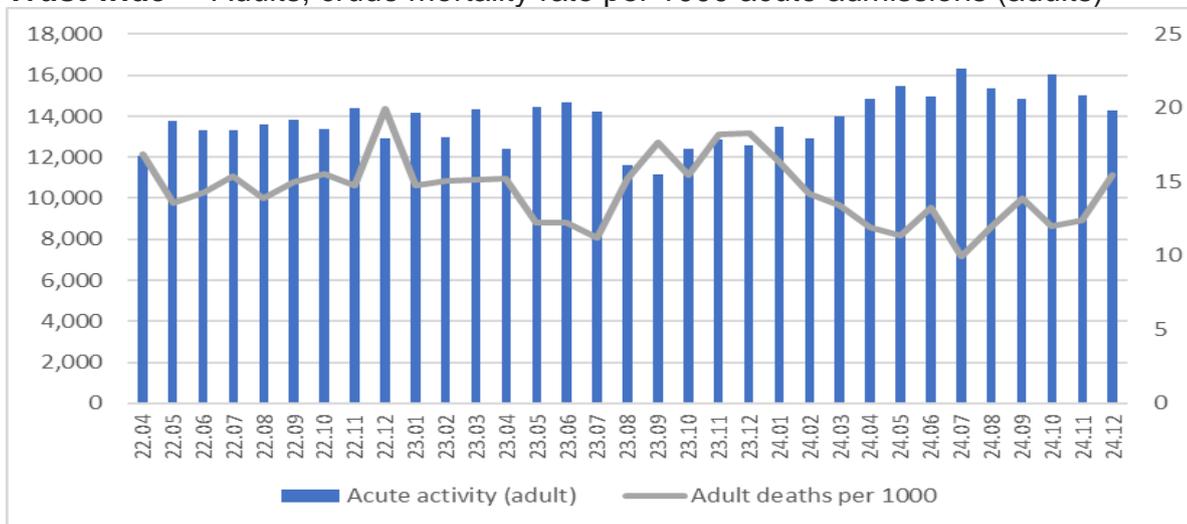


Fig 5 – Crude mortality rate per 1000 acute admissions, Trust wide

### Northwick Park Hospital – Adults, crude mortality rate per 1000 acute admissions (adults)

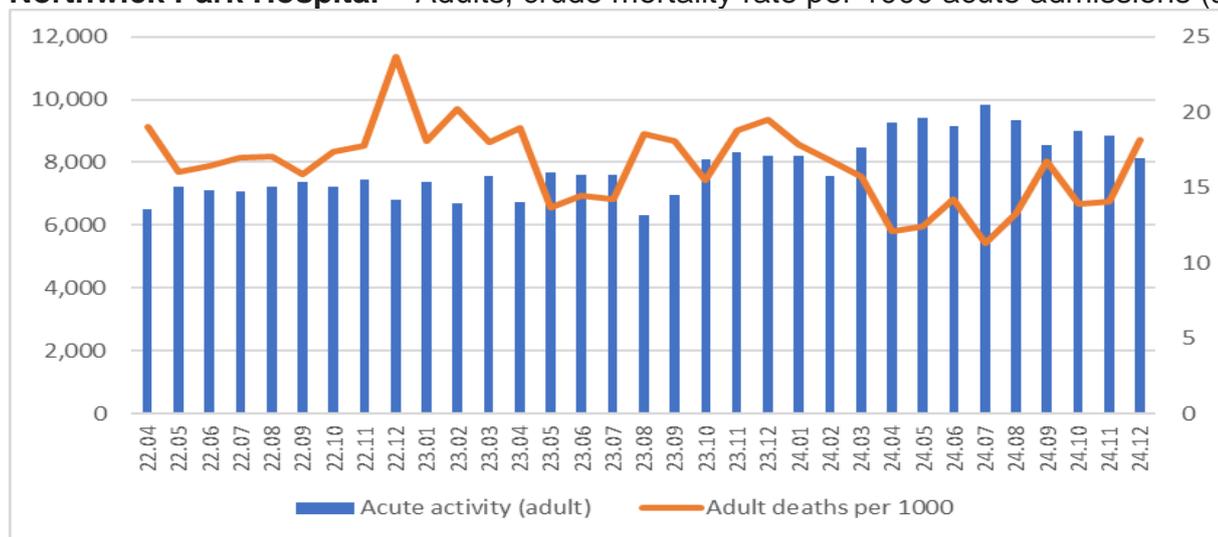


Fig 6 – Crude mortality rate per 1000 acute admissions, NPH

### Ealing Hospital – Adults, crude mortality rate per 1000 acute admissions (adults)

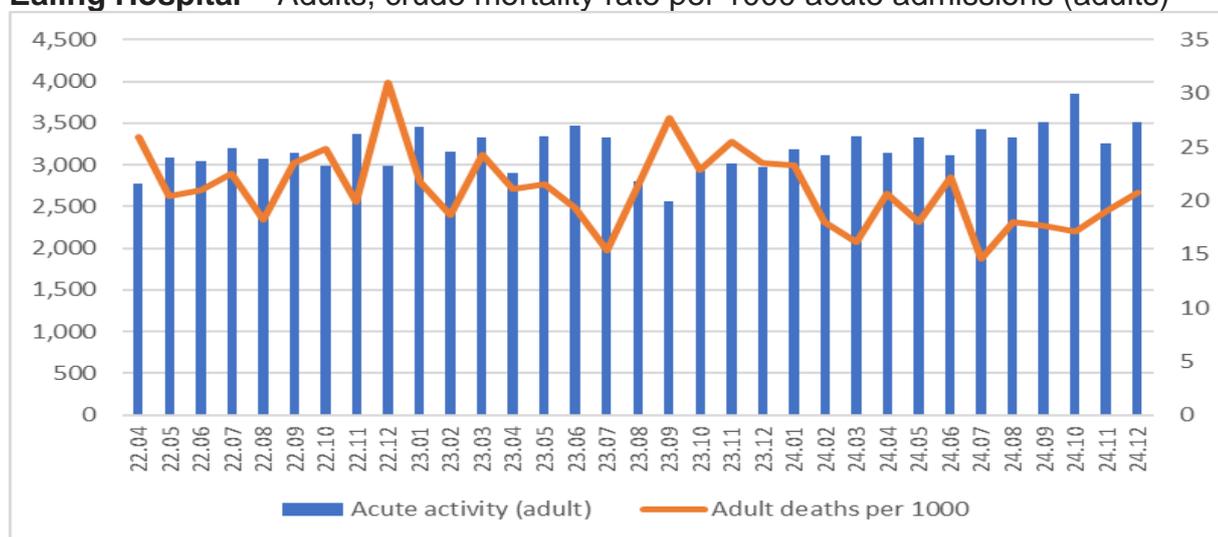


Fig 7 – Crude mortality rate per 1000 acute admissions, EH

## 4.0 Mortality Review

### 4.1 Medical Examiner’s Service

The Medical Examiner’s Service provides enhanced scrutiny to all in-hospital deaths, supports the identification of potential learning, and offers a point of contact for bereaved families wishing to raise concerns. The functions of this service are to:

- Provide greater safeguards to the public by ensuring scrutiny of all non-coronial deaths.
- Ensure the appropriate direction of deaths to the coroner.
- Provide a better service for the bereaved and an opportunity for them to raise any concerns to a doctor not involved in the care of the deceased.

- Improve the quality of death certification.
- Improve the quality of mortality data.

During Q3 2024/25 the service scrutinised 598 (100%) in-hospital deaths, this resulted:

- 41 cases referred to the coroner of which; 13 were retained for investigation, 28 were returned for certification with no requirement for further coroner investigation
- 10 cases with potential learning for the Trust, triggering in-depth (level 2) mortality reviews.

**Achievements:** The service continues to have the highest percentage of urgent 24-hour releases across the sector, when requested for reasons of religious observance. The service also has the highest percentage of out of hospital cases dealt with within 2 days (not working days).

**Challenges:** Budgetary challenges have delayed the service moving to weekend shift working, which should be resolved within Q4. Long-term sickness within the service has led to the redistribution of non-clinical tasks, placing a higher burden on some key staff.

There remain some GPs who do not fully engage with the service, and education is being offered to address this. Coroners are making greater use of the CN1A form, leading to the service being directed to undertake some initial Coronial enquiries.

**Improvements:** No further changes this quarter, focus has been on the ongoing improvement of staff capabilities and knowledge, that comes with the experience of working in a high-end service.

#### 4.2 In-depth (level 2) mortality review

Mortality case review provides clinical teams with the opportunity to review expectations, outcomes and potential improvements with the aim of:

- Identifying sub-optimal or excellent care
- Identifying service delivery problems
- Developing approaches to improve safety and quality
- Sharing concerns and learning with colleagues

Learning from review is shared at specialty mortality review groups (M&Ms / MDTs); where issues in care, trends or notable learning is identified action is steered through the Divisional Quality Boards / Governance Groups and the Trust-wide Learning from Patient Deaths Group (LfPDG).

During the 12-month period January to December 2024, 2,309 in-hospital adult or child deaths were recorded within the Trust's mortality review system (Datix), of these 100% have been screened. Screening identified 381 (17%) cases that would benefit from in-depth (level 2) review. Of these 94% have completed this in-depth review process, which represents a 4% increase since the last quarterly report.

	No. of deaths	No. of cases screened	No. of cases flagged for level 2 review	No. case with completed level 2 review	% cases Screened	% of level 2 reviews completed
Q4 23/24	595	595	64	63	100%	98%
Q1 24/25	560	560	83	78	100%	94%
Q2 24/25	556	556	139	130	100%	94%
Q3 24/25	598	598	95	88	100%	93%
<b>Totals</b>	<b>2,309</b>	<b>2,309</b>	<b>381</b>	<b>359</b>	<b>100%</b>	<b>94%</b>

Tab 5: Adult & child mortality review status by financial quarter, January to December 2024

The Consultant Mortality Validators undertake level 2 in-depth mortality reviews and identify cases that need Speciality Mortality Leads to conduct a further in-depth review. Speciality Mortality Leads have 4 months from the date of death to complete these reviews. Compliance is monitored by the Divisional Boards / Governance meeting, Learning from Patient Deaths Group, and overseen by the Trust Executive Group and Quality & Safety Committee.

Hospitals	No. of deaths	No. of cases screened	No. flagged for level 2 review	No. of completed level 2 reviews	% cases Screened	% of level 2 reviews completed
Northwick Park & St Marks	1,553	1,553	266	247	100%	93%
Ealing	752	752	114	112	100%	98%
Central Middlesex	4	4	1	0	100%	0%
<b>Totals</b>	<b>2,309</b>	<b>2,309</b>	<b>381</b>	<b>359</b>	<b>100%</b>	<b>94%</b>

Tab 6: Adult & child mortality review status by site, January to December 2024

The following key trends arising from process compliance monitoring have been noted:

- The percentage of in-patient deaths identified for in-depth review (level 2) reduced in Q3 to 16% (was 25% in Q2 2024/25). This reduction has been attributed to a review undertaken during Q3 looking at the triggers being used by the service. Now ME's focus just the cases they would like investigated, rather than adding national triggers to the system.
- 'Unexpected death' remains the most frequent trigger for in-depth mortality review at 38% (36 cases), there has been a reduction in the number of 'medical examiner concerns' from 35% in Q2 to 11% (10 cases), as explained above.
- 88 in-depth mortality reviews relating to deaths occurring during Q3 2024/25 have been undertaken at time of reporting; 78% of which identified no sub-optimal care (CESDI Grade 0), which is similar to the previous quarter (72%).

The Divisional Mortality Leads provide scrutiny to mortality cases so as to; identify themes and escalate any issues of concerns. Key themes / issues identified via mortality review this quarter:

- **Standardized care and communication:** development of supportive care guidelines for haematological malignancies receiving SACT, shared with new doctors. Clear relay of

complex haematology diagnostics (not always visible on CERNER) and MDT findings to all relevant teams.

- **Proactive Clinical Decision-Making:** Regular assessment of Treatment Escalation Plans during daily ward rounds. Low threshold for CTPA and PE investigations. Case by Case approach to feeding in frail and palliative patients.
- **Collaborative and Patient centred Care:** Strong multi-specialty decision-making (Surgery, Cardiology, ITU and Anaesthetics). Effective documentation of family and patient discussions, ensuring shared decision making. Early SPCT involvement in non-malignant conditions, reducing number of decompensated patients dying in hospital.

### 6.3 CESDI Grading of Care

Outcome, avoid ability and / or suboptimal care provision is defined using the Confidential Enquiry into Stillbirths and Deaths in Infancy (CESDI) categories that have been adopted by the Trust for use when assessing deaths:

- Grade 0: No suboptimal care or failings identified, and the death was unavoidable.
- Grade 1: A level of suboptimal care identified during hospital admission, but different care or management would NOT have made a difference to the outcome and the death was unavoidable.
- Grade 2: Suboptimal care identified, and different care MIGHT have made a difference to the outcome, i.e. the death was possibly avoidable.
- Grade 3: Suboptimal care identified, and different care WOULD REASONABLY BE EXPECTED to have made a difference to the outcome, i.e. the death was probably avoidable.

#### CESDI grades January to December 2024

Period	CESDI 0	CESDI 1	CESDI 2	CESDI 3
Q4 23/24	41	17	5	0
Q1 24/25	57	14	7	0
Q2 24/25	94	32	3	1
Q3 24/25	69	18	1	0
<b>Total</b>	261	81	16	1

Tab 7: Closed mortality cases by CESDI grade, January to December 2024

During this 12-month period 16 cases of sub-optimal care that might have made a difference to the patient's outcome (CESDI 2) and 1 cases where sub-optimal care would reasonably be expected to have made a difference to outcome were identified. All cases graded as CESDI 2 or 3 are presented to the Trust's Emerging Incident Review Group for confirmation of learning response (e.g. SI / PSII).

The graph below illustrates the distribution of CESDI grades across the three sites, reflecting the nature of events being reviewed by Mortality Leads. Northwick Park has the highest

number of sub-optimal care with 64 cases, followed by Ealing with 34 cases. This suggests that the majority of cases where different care might have made a difference to outcome were equally distributed.

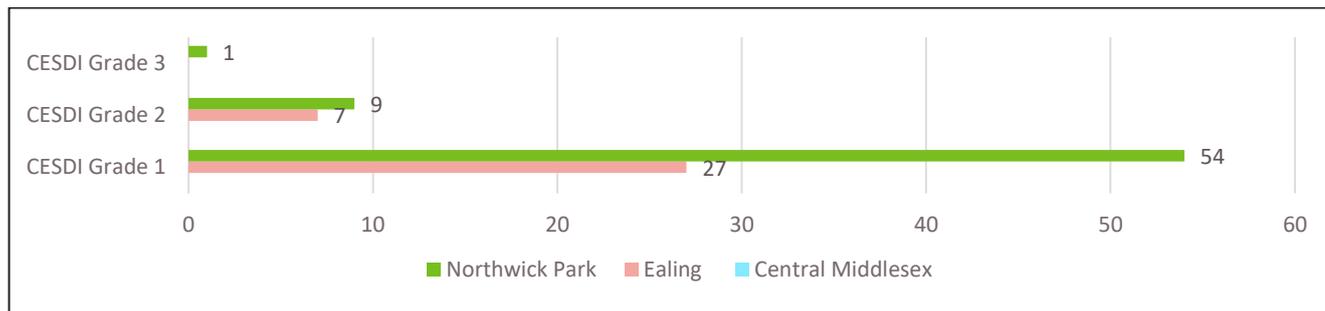


Fig 8 – CESDI Grade by Site, January to December 2024

## 5.0 Ethnicity & Gender

The ethnicity data shows a consistent picture in terms of the proportion of deaths by ethnicity during Q3 2024/25 as in previous quarters. Further analysis is provided in appendix B.

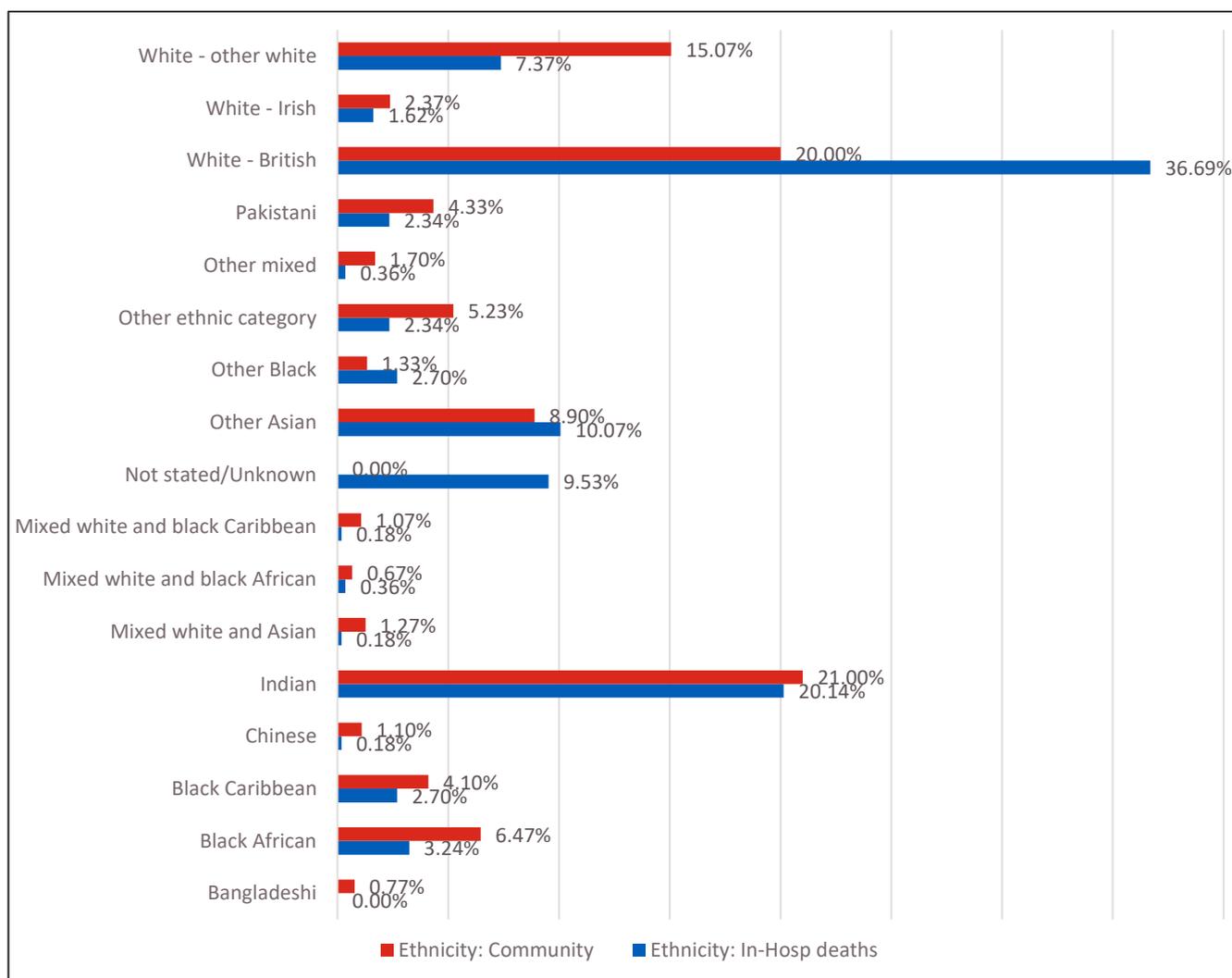


Fig 9 – Ethnicity breakdown, Q3 2024/25

In proportion to the community population for Brent, Ealing and Harrow, there is more in-hospital mortality in the Other Asian and White British demographic groups. While there is a high rate of in-hospital deaths for the Indian group, this is in keeping with the populations served.

This quarter White British remains is the most frequently identified ethnicity associated with in-hospital mortality, account for 36.69% of deaths occurring during Q3 2020/25. It is noted that the local populations of Brent, Ealing, Harrow recognises 20% of the population as this ethnicity. This suggests a higher rate of in-hospital deaths compared to community deaths for this group. Other Asian is the second most frequent ethnicity associated within in-hospital death at 10.07%.

In this 12-month period, the CESDI Grade 1 cases predominantly involve individuals of White British ethnicity followed by Indian. CESDI Grade 2 cases are currently evenly divided between Indian, White British and not known. These findings align with the demographic composition of the population in Brent, Ealing, and Harrow, where Indian and White British groups are the largest resident populations.

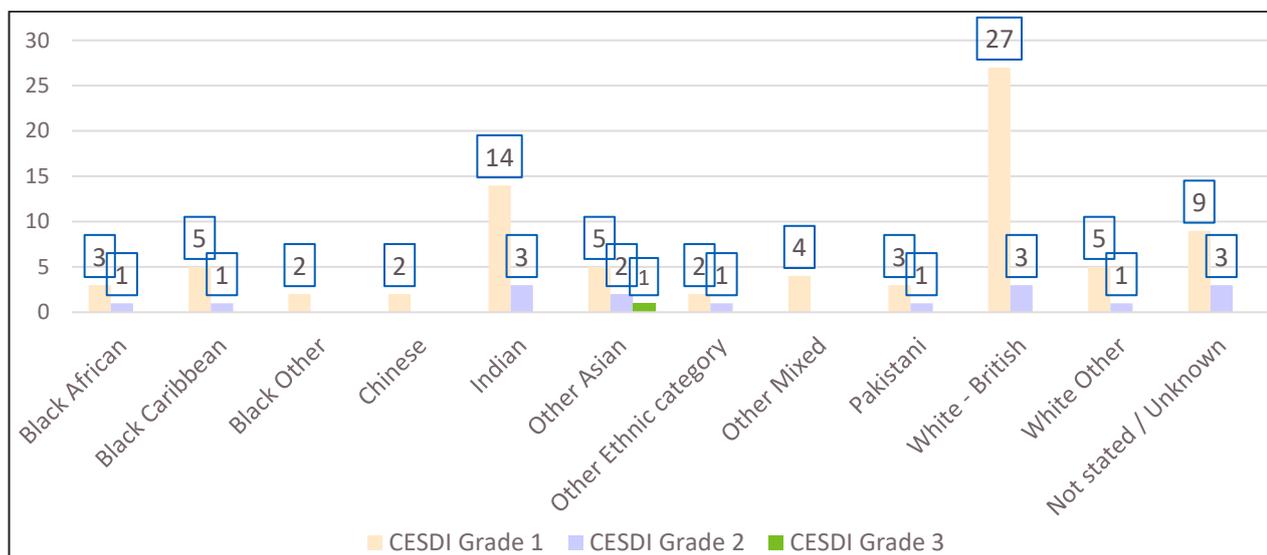


Fig 10: Closed mortality cases by CESDI grade and Ethnicity, January to December 2024

Analysis of CESDI grades by gender indicates the same trend as is the previous 12 month period, that the care of male patients is more likely to have elements of sub-optimal care identified than female patients.

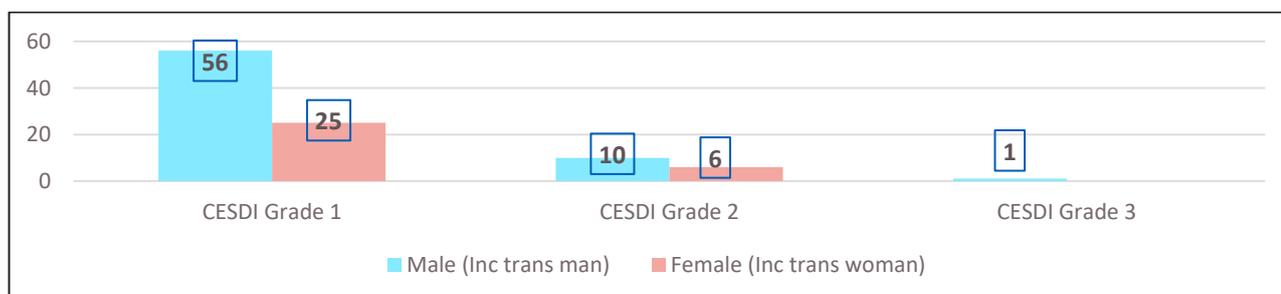


Fig 11: Closed mortality cases by CESDI grade and Gender, January to December 2024

## 6.0 Child Death Overview Panels

**Overview:** There were a total 5 child deaths across Brent, Ealing & Harrow Borough resident children and young people during Q3 2024/25:

**Case 1:** 15-year-old, known to the neurology team, symptom care team at GOSH, and the paediatric team. Background of mucopolysaccharidosis type 3a, respiratory failure, poor feeding, seizures (last 3 years ago), had a seizure at home. Had received Buccal midazolam by parent and LAS were called. On arrival, was found with no pulse and not breathing. Had a DNACPR in place, however parents wanted something done. LAS commenced CPR and discussed DNACPR with parents. Transferred to NPH, as unexpected death, for care after death. Discussed with Medical Examiners who issued Death Certificate stating 1a = MPS type 3a.

- **Challenges:** Delay in patient coming to ED due to ambulance changes. No Kennedy samples taken, as per national guidance. However, given that patient was brought to ED about 4 hours post death, it may not have been possible to get many samples.
- **Improvements Made:** Child death proforma being updated to include information on Kennedy samples and how to take these. Child bereavement support information to be included in the proforma too (being written by the Child Death Review Nurse Team for NWL).
- **Recommendations:** Continue the good collaborative work across the different sites that help manage the children with complex needs and are known to symptom care team.

**Case 2:** 4-year-old, with a background of sickle cell disease, was BIBA. On arrival, was awake, chatting but looking very uncomfortable with a distended abdomen, fever and increased WOB. Mum reported constipation and had stopped all other medication (Folic acid and PenV), whilst trying to get the constipation treated. Was managed as per sepsis protocol, however patient continued to deteriorate rapidly, eventually transferred to St Marys Hospital PICU. Was noted to have ischemic changes on CT head and fixed pupils over the following days. End of life care was discussed, and patient passed away in November. Blood and Urine PCR positive for pneumococcal antigen.

- **Challenges:** Managed well from arrival in ED, some delay in pain relief and IV access was difficult History of poor compliance with prophylactic medication, patient unknown until this attendance. Pneumococcal vaccine at age 2 not received (as per the guidance for SCD).
- **Improvements made:** Discussion at JAR; GP's to check that all patients with sickle cell have had their vaccinations as and when due. Have an altered schedule – with additional vaccines recommended. GP's advised to issue 3 month supply for prophylactic medication to assist with compliance. Instead of the current practice of monthly.
- **Recommendations:** JAR discussion was very informative and identified areas of improvement.

**Case 3:** 20-month-old, run over by a car outside home. Rushed to CMH by parents by car. On arrival, seen by the UCC team, in cardiac arrest, CPR commenced. Some difficulty finding equipment. HEMS arrived; however, was declared dead enroute to St Marys Hospital. Care after death initiated at St Marys with police and safe-guarding involvement. There were some discrepancies in the history initially and difficult to get a clear history, parents only spoke Gujarati.

- **Challenges:** CMH is not equipped to see children with acute deterioration / in extremis, it has an Urgent Care Centre that sees Children. Brought by Parents, may be as unable to call for ambulance? This was not explored.
- **Improvements made:** Discussed with resus team, who are in the process of ensuring that basic equipment is available there.
- **Recommendations:** The team were supported post event, with debrief by the resus team.

**Case 4:** A possibly 24-week gestation baby, born in the A&E department. Mother was unaware of the pregnancy. Baby was delivered, stabilised and transferred to tertiary neonatal unit. The baby passed away a few days later.

- **Challenges:** Unexpected delivery in ED, with not all the equipment on the resuscitator. Lack of overall leadership, with a high number of staff around.
- **Improvements made:** Teams aware of the required equipment and to ensure that it is present on the resuscitator. De-brief held and support discussed. Simulation training to include scenarios like these, to be done in real time and organised regularly.
- **Recommendations:** The team worked well together and there was comprehensive documentation noted by some teams.

**Case 5:** A 13-year-old, known to have asthma was brought to A&E as a OOHCA after having woken up in the night complaining of difficulty breathing and collapsing at home. CPR was commenced and patient was Intubated and ventilated and transferred to PICU, where they passed away a few days later.

- **Challenges:** Difficult managing the ventilation, but managed post initial CPR. Known to have poor asthma control and had missed OPD appointments.
- **Improvements made:** Raised awareness amongst the paediatric team of the need to review all patients with multiple attendances with asthma in the respiratory clinic. Team requesting an Asthma and Allergy nurse specialist to review these patients early and more regularly. Business case written and pending (for 3 years), making the trust an outlier in this aspect.

## 7.0 Perinatal Mortality Review Tool

**Overview:** The Perinatal Mortality Review Tool (PMRT) is a national mandatory monitoring and assurance dataset developed by MBRRACE-UK. It is used to collect very detailed information

about the care mothers and babies have received throughout pregnancy, birth and afterwards. The purpose of the PMRT is to support hospital learn from deaths by providing a standardised and structured review process. The PMRT is designed to support review of:

- All late fetal losses (22 weeks + 0 days to 23 weeks + 6 days).
- All antepartum and intrapartum stillbirths.
- All neonatal deaths from birth at 22 weeks + 0 days to 28 days after birth

During Q3 2024 the following cases were reviewed:

**October 2024:** 1 late fetal loss, 0 stillbirths and 0 neonatal deaths.

**Synopsis of late fetal loss:** Patient booked at another trust but had moved into area, brought in to NPH via London Ambulance Service (LAS) at 22 weeks with twin pregnancy. No pre-alert received from LAS, unit activity was high, and patient transferred to bereavement room as there this was the only room available. Twin 1 birthed within 9 minutes, successfully resuscitated, stabilised, and transferred to a tertiary unit due to severe prematurity, sadly this baby died the next day. Twin 2 was birthed 3 hours 46 minutes later showing no signs of life and was classified as a late fetal loss.

**Challenges:** No pre-alert from the LAS meant that team were not ready and waiting for the ambulance arrival. On review and discussion with LAS it was ascertained that the member of staff who answered the call was new to the position and had called the wrong hospital with the pre-alert, the second call did come to NPH, but the woman was already in the hospital.

When the ward receives a pre alert, they have time to organise the room and equipment for the arrival of the woman and the doctors are made aware and prepared for the woman's arrival.

Acuity on the unit; triage midwife looked after the patient, leaving 1 midwife in triage. All rooms on the delivery suite were in use with labouring women and the manager on call had to attend the unit overnight to assist with maternity care.

**Improvements made:** Learning shared at forums, via safety briefings and in reflective sessions. The Resuscitaires in the bereavement room were not switched on and checked for the imminent delivery of preterm twins. If the unit had received a pre alert this would have been completed and there would not have been a delay with the equipment being ready. LAS have investigated why trust did not receive a pre-alert and a discussion with member of staff involved has been facilitated with a reflective session and training arranged.

**November 2024:** 1 late fetal loss, 1 stillbirth, and 0 neonatal deaths.

**Synopsis of fetal loss:** Patient was 22+4 weeks on attendance at triage with second episode of reduced Fetal Movements. Seen in triage, midwife unable to auscultate fetal heartbeat (FHR). Patient seen by Senior Registrar who performed a bedside scan, on finding no cardiac activity,

another scan was undertaken by Consultant and the Late Fetal Loss (LFL) was confirmed. Patient offered a formal scan, which was performed the next morning and LFL was confirmed.

**Challenges:** Due to the acuity in triage, there was a delay in the patient being seen, waiting 4 hours before the diagnosis of LFL. On investigation, all triage rooms were full. During the antenatal period there was a discrepancy in the baby's centile on scanning and the patient was informed the baby was on the 3rd centile and would need a fetal medicine scan (FMU) but later called by the Radiographer who stated that the baby was on 14th centile and would not require the FMU scan. On review of this decision, it was found that the Radiographer was looking at the estimated fetal weight (EFW) graphs instead of the centile used to ascertain the baby size in accordance with the scan parameters. The scan was reviewed by one of the FMU consultants and was on the 14th centile not the 3rd.

**Improvements:** The Lead Radiographer discussed care with the scan radiographer and a reflective session was held. Scan radiographer made aware of the correct policy where a senior radiographer should have called the patient to explain what had happened, this will now be embedded in future care of patients. The scan was further reviewed by one of the FMU consultants and baby was on the 14th centile. Service is currently auditing the use of the Birmingham Symptom Specific Obstetric Triage System (BSOTS), to review current waiting times. Service has hired a doctor assigned to triage, ensuring that patients are seen within allotted times.

**Synopsis of Stillbirth:** Patient was 30 weeks and 6 days pregnant on attendance in triage with complaints of abdominal pain. This was patients third pregnancy where they had previously developed pre-eclampsia and gestational diabetes. Patient had experienced a fetal loss at 10 weeks with twins in June 2023. While in triage, it was noted that they were oedematous especially in face and feet. It was difficult to secure intravenous access (IV) and take investigative bloods, the midwife and registrar were unable to auscultate the FHR. The patient was becoming hypertensive, clammy and pale and complaining of constant pain.

The Registrar suspected placental abruption and 2222 call was placed and they were transferred to the theatre and category 1 caesarean section (C/S) was carried out under General Anaesthetic (GA). There was a delay in commencing the C/S as there was difficulty to secure IV access, decision was made for femoral line access, this took 3 attempts due to the patient's condition. There was also an emergency case ongoing in theatre 2 therefore a second theatre had to be opened and the staff from the main site had to attend to help with the operation.

**Challenges:** Delay in gaining IV access due to the patient's condition, taking 3 attempts to secure a femoral line. This was escalated appropriately to the anaesthetics and the consultant managed to successfully place the line. A second theatre had to be opened and the team from the main side had to attend to help with the operation as the staff were already dealing with an emergency in the first theatre. On review the patients care, they had been cared for by midwifery staff, an appointment was booked for the consultant, but the patient was abroad at the time, and this had

not been noted or actioned. It was also noted the patient's urine had 2 plus of protein and this was not actioned or associated with pre-eclampsia and referral was not arranged.

**Improvements:** Obstetric consultant training session is planned to highlight the signs and symptoms of pre-eclampsia and when to refer patients to triage or for consultant review. Patient Safety Midwife has raised the missed opportunities with staff at monthly meetings, highlighting the need to be aware of policies on the intranet and the signs & symptoms of pregnancy complications. Case was discussed at the Emerging Incident Review Group and the Patient Safety Team is arranging a multidisciplinary meeting to encourage further learning. It was felt that there was appropriate management of emergency C/S and escalation process regarding gaining IV access prior to anaesthesia.

**December 2024:** 0 Late fetal losses, 1 Stillbirth and 0 Neonatal deaths.

**Synopsis of stillbirth:** Patient attended triage at 38 weeks, 5 days complaining of reduced fetal movements for a few hours. Was seen within 26 minutes, midwife and doctor were unable to auscultate fetal heart rate (FHR), a scan was performed by the Registrar and again by the Consultant, in line with the trust guidelines. Stillbirth confirmed the patient was admitted to the ward with a plan to commence the pregnancy loss pathway. Patient proceeded to go into spontaneous labour and birthed an infant. On review of the notes the patient had a history of 3 term vaginal deliveries and one late miscarriage at 18 weeks at the beginning of the year.

**Challenges:** Language Barriers as English was not the patients first language, and the following trust policies and guidelines to ensure our women are seen appropriately. As this patient had previously had a late miscarriage at 18 weeks and they should have been seen by a Consultant, this does not appear to have been requested. Documentation did not appear to mention the late fetal loss. A review of Cerner notes found that the antenatal summary does document the pregnancies, but it does not appear that the miscarriage had been identified and actioned. Acuity in triage is for all patients to be triaged within the BSOTS timeframe. One of the triage midwives was birthing a patient, on return to triage this patient was seen first due to the reduced FM's

**Improvements made:** ensuring access to interpreting service throughout the maternity unit and community clinics. Service has iPad's on the wards for interpretation and all children centres have the use of telephone interpreters. There were missed opportunities to allocate the patient to the correct pathway and make sure they have the correct appointments with the correct practitioners. This learning will be taken to the different forums to make sure it is cascaded to staff.

## 11.0 Conclusion

The outcome of the Trust's mortality surveillance programme continues to provide a rich source of learning that is supporting the organisations improvement objectives. The Trust continues to be recognised as having a low relative risk of mortality (SHMI) across NHS England.

We can provide assurance to the committee that we are providing safe care for the majority of patients. Where care issues are found, we have robust processes for referral for more in-depth review and these processes are triangulated against other data provided within the trust under the PSIRF framework.

We continue to align and improve our learning from patient death processes, and actively support the alignment across the acute provider collaborative to aid comparison, learning and opportunities for improvement.

## 12.0 Glossary

**Medical Examiners** are responsible for reviewing every inpatient death before the medical certificate cause of death (MCCD) is issued, or before referral to the coroner in the event that the cause of death is not known or the criteria for referral has been met. The Medical Examiner will request a Structured Judgement Review if required or if necessary refer a case for further review and possible investigation through our incident reporting process via the quality and safety team. The ME will also discuss the proposed cause of death including any concerns about the care delivered with bereaved relatives.

**Structured Judgement Review (SJR)** is a clinical judgement-based review method with a standard format. SJR reviewers provide a score on the quality of care provided through all applicable phases of care and will also identify any learning. The SJR will be completed within seven days of referral.

**Structured judgement reviewers** are responsible for conducting objective case note reviews of identified cases. They will seek, when required, specialist input and advice from clinical colleagues, including members of the multi-disciplinary teams to ensure high quality, comprehensive review is undertaken, using the full range of medical records available to them.

**Specialty M&M** reviews are objective and multidisciplinary reviews conducted by specialties for cases where there is an opportunity for reflection and learning. All cases where ME review has identified issues of concern must be reviewed at specialty based multi-disciplinary Mortality & Morbidity (M&M) reviews.

**Child Death Overview Panel (CDOP)** is an independent review aimed at preventing further child deaths. All child deaths are reported to and reviewed through Child Death Overview Panel (CDOP) process.

**Perinatal Mortality Review Tool (PMRT)** is a review of all stillbirths and neonatal deaths. Neonatal deaths are also reviewed through the Child Death Overview Panel (CDOP) process. Maternal deaths (during pregnancy and up to 12 month post-delivery unless suicide) are reviewed by Healthcare Safety Investigation Branch and action plans to address issues identified are developed and implemented through the maternity governance processes.

**Learning Disabilities Mortality Review (LeDeR)** is a review of all deaths of patients with a learning disability. The Trust reports these deaths to the Local integrated care boards (ICBs) who are responsible for carrying out LeDeR reviews. SJRs for patients with learning disabilities are undertaken within the Trust and will be reported through the Trust governance processes.

### Appendix A – Acute Provider Collaborative performance scorecard

	2023-2024	2024-25		
	Q4	Q1	Q2	Q3
No. Deaths	595	560	556	598
No. Adult Deaths	593	555	552	594
No. Child Deaths	2	5	4	4
No. Neonatal Deaths	0	0	2	0
No. Stillbirths	7	3	2	2
ME Reviewed Deaths in Qtr.	595	560	556	598
% ME Reviewed Deaths - Deaths (excluding Stillbirths) in Qtr.	100%	100%	100%	100%
SJR Requested for Deaths in Qtr.	64	83	139	95
% SJRs Requested for Deaths in Qtr. of total deaths in Qtr.	11%	15%	25%	16%
SJR Completed for Deaths in Qtr.	63	78	130	88
% SJRs Completed for Deaths in Qtr.	98%	94%	94%	93%
No. LeDeR Completed	15	9	12	12
Requests made by a Medical Examiner - SJRs Requested for Deaths in Qtr.	17	26	48	10
% Requests made by a Medical Examiner - SJRs Requested for Deaths in Qtr.	27%	31%	35%	11%
Concerns raised by family / carers - SJRs Requested for Deaths in Qtr.	22	16	24	13
% Concerns raised by family / carers - SJRs Requested for Deaths in Qtr.	34%	19%	17%	14%
Patients with learning disabilities - SJRs Requested for Deaths in Qtr.	15	9	12	12
% Patients with learning disabilities - SJRs Requested for Deaths in Qtr.	23%	11%	9%	14%
Patients with severe mental health issues - SJRs Requested for Deaths in Qtr.	2	6	6	7
% Patients with severe mental health issues - SJRs Requested for Deaths in Qtr.	3%	7%	4%	7%
Unexpected deaths - SJRs Requested for Deaths in Qtr.	17	25	51	36
% Unexpected deaths - SJRs Requested for Deaths in Qtr.	27%	30%	37%	38%
Elective admission deaths - SJRs Requested for Deaths in Qtr.	9	7	11	6
% Elective admission deaths - SJRs Requested for Deaths in Qtr.	14%	8%	8%	6%
Requests made by speciality mortality leads/through local Mortality & Morbidity review processes - SJRs Requested for Deaths in Qtr.	3	4	10	1

	2023-2024	2024-25		
	Q4	Q1	Q2	Q3
% Requests made by speciality mortality leads/through local Mortality & Morbidity review processes - SJRs Requested for Deaths in Qtr.	5%	5%	7%	1%
Service or diagnosis alarms as agreed by APC mortality surveillance group - SJRs Requested for Deaths in Qtr.	2	n/a	n/a	n/a
% Service or diagnosis alarms as agreed by APC mortality surveillance group - SJRs Requested for Deaths in Qtr.	3%	n/a	n/a	n/a
CESDI 0 - No suboptimal care - Completed SJRs for Deaths in Qtr.	41	57	94	69
% CESDI 0 - No suboptimal care - Completed SJRs for Deaths in Qtr.	65%	73%	72%	78%
CESDI 1 - Some sub optimal care which did not affect the outcome - Completed SJRs for Deaths in Qtr.	17	14	32	18
% CESDI 1 - Some sub optimal care which did not affect the outcome - Completed SJRs for Deaths in Qtr.	27%	18%	25%	20%
CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death) - Completed SJRs for Deaths in Qtr.	5	7	3	1
% CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death) - Completed SJRs for Deaths in Qtr.	8%	9%	2%	1%
CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death) - Completed SJRs for Deaths in Qtr.	0	0	1	0
% CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death) - Completed SJRs for Deaths in Qtr.	0%	0%	1%	0%

## Appendix B: Ethnicity Q4 2023/24 and Q1, Q2 & Q3 2024/25

	2023-24		2024-25								Community population Brent, Ealing, Harrow
	Q4 n	Q4 %	Q1 n	Q1 %	Q2 n	Q2 %	Q3 n	Q3 %	Total n	Total %	
Bangladeshi	1	0%	1	0%	0	0.00%	1	0.00%	3	0.13%	0.77%
Black African	18	3%	14	3%	18	3.24%	15	3.24%	65	2.82%	6.47%
Black Caribbean	15	3%	14	3%	15	2.70%	25	2.70%	69	2.99%	4.10%
Chinese	1	0%	4	1%	1	0.18%	2	0.18%	8	0.35%	1.10%
Indian	101	17%	128	23%	112	20.14%	147	20.14%	488	21.13%	21.00%
Mixed white and Asian	0	0%	4	1%	1	0.18%	4	0.18%	9	0.39%	1.27%
Mixed white and black African	1	0%	0	0%	2	0.36%	0	0.36%	3	0.13%	0.67%
Mixed white and black Caribbean	3	1%	2	0%	1	0.18%	0	0.18%	6	0.26%	1.07%
Not stated/Unknown	79	13%	64	11%	53	9.53%	56	9.53%	252	10.91%	N/A
Other Asian	64	11%	31	6%	56	10.07%	50	10.07%	201	8.71%	8.90%
Other Black	13	2%	10	2%	15	2.70%	11	2.70%	49	2.12%	1.33%
Other ethnic category	29	5%	14	3%	13	2.34%	17	2.34%	73	3.16%	5.23%
Other mixed	11	2%	1	0%	2	0.36%	4	0.36%	18	0.78%	1.70%
Pakistani	9	2%	12	2%	13	2.34%	15	2.34%	49	2.12%	4.33%
White - British	208	35%	213	38%	204	36.69%	195	36.69%	820	35.51%	20.00%
White - Irish	11	2%	10	2%	9	1.62%	9	1.62%	39	1.69%	2.37%
White - other white	31	5%	38	7%	41	7.37%	45	7.37%	155	6.71%	15.07%
No value	0	0%	0	0%	0	0.00%	2	0.00%	2	0.09%	N/A
<b>Total</b>	<b>595</b>	<b>100%</b>	<b>560</b>	<b>100%</b>	<b>556</b>	<b>100.00%</b>	<b>598</b>	<b>100.00%</b>	<b>2309</b>	<b>100.00%</b>	

NWL Acute Provider Collaborative Quality Committee

29/04/2025

Item number: 4.1.3d

This report is: Public

# The Hillingdon Hospitals NHS Foundation Trust

## Learning from Deaths Quarter three – 2024/25

Author: Paula Perry  
Job title: Clinical Governance Facilitator for Mortality

Accountable director: Victoria Cook  
Job title: Deputy Chief Medical Officer

### Purpose of report (for decision, discussion or noting)

Purpose: Information or for noting only

This report presents the data from the Learning from Deaths programme for Quarter Three (Q3) of 2024/25 for information. It is a statutory requirement for Trusts to present this information to their boards.

### Report history

Outline committees or meetings where this item has been considered before being presented to this meeting.

<b>Trust Quality and Safety Executive Committee</b> 10/02/2025 Q3 Report presented	<b>Mortality Surveillance Group</b> 12/03/2025 Q3 Report presented	<b>Trust Quality and Safety Committee</b> 20/02/2025 Q3 Report presented
--	--	--

### Executive summary and key messages – linked to the section above, please update this to include key discussion points and actions agreed at previous meetings

- 1.1. [To provide the board with an update on the Trust Learning from Deaths programme from 1<sup>st</sup> October 2024 to 31<sup>st</sup> December 2024.
- 1.2. Following the change to a new Hospital Standardised Mortality Ratio (HSMR) methodology the HSMR for August 2024 is 83.3 against the NHS benchmark of 100, the figure therefore shows as below the national average but is not statistically low.

- 1.3. Standardised Hospital Mortality Indicator (SHMI) year to July 2024 is 97.95 and below the NHS benchmark of 100.
- 1.4. 100% of all deaths in Quarter Three were reviewed by the Medical Examiner, 7% of cases were referred for a Structured Judgement Review.
- 1.5. Further work to analyse ethnicity data for deceased patients has been included in this quarter with the inclusion of more demographic details. An update on this work and next steps are provided in full in this paper.
- 1.6. There continues to be focused work with the divisions to ensure that Structured Judgement Reviews are completed within the expected timeframe, monthly meetings have been set up within the divisions to support the SJR process including monitoring and escalation of any delays with SJR completion.
- 1.7. The Mortality Surveillance Group continues to monitor the number of in-patient deaths and the number of Structured Judgement Reviews being triggered and completed.
- 1.8. Where the potential for improvement is identified learning is shared at Divisional Boards/groups and presented by the divisions to the Trust-wide Mortality Surveillance Group; this ensures outcomes are shared and learning is cascaded.

## Impact assessment

Tick all that apply

- Equity
- Quality
- People (workforce, patients, families or careers)
- Operational performance
- Finance
- Communications and engagement
- Council of governors

*Mortality case review following in-hospital death provides clinical teams with the opportunity to review expectations, outcomes and learning in an open manner. Effective use of mortality learning from internal and external sources provides enhanced opportunities to reduce in-hospital mortality and improve clinical outcomes and experience for patients and their families*

## Reason for private submission (For Board in Common papers only)

Tick all that apply [*delete section if not applicable*]

- Commercial confidence
- Patient confidentiality
- Staff confidentiality
- Other exceptional circumstances

If other, explain why

## Strategic priorities

Tick all that apply

- Achieve recovery of our elective care, emergency care, and diagnostic capacity (APC)
- Support the ICS's mission to address health inequalities (APC)
- Attract, retain, develop the best staff in the NHS (APC)
- Continuous improvement in quality, efficiency and outcomes including proactively addressing unwarranted variation (APC)
- Achieve a more rapid spread of innovation, research, and transformation (APC)
- Help create a high quality integrated care system with the population of north west London (ICHT)
- Develop a sustainable portfolio of outstanding services (ICHT)
- Build learning, improvement and innovation into everything we do (ICHT)

## Key risks arising from report

- There has been a change to the Hospital Standardised Mortality Ratio+ (HSMR+) methodology, a more sophisticated comorbidity measure is used to capture more conditions and an adjustment to frailty has also been introduced. This has impacted Hillingdon Hospital with an increase in the HSMR, a deep dive is being carried out in to the impact this will have on the data moving forward which will be fed back and monitored at the Mortality Surveillance Group meeting in May.
- Morbidity & Mortality meetings (M&M) need to be established in Unplanned Care to present and monitor the learning and recommendations identified from Structured Judgement Reviews.

## Main Report

### 2. [Learning and Improvements

- 2.1 Learning from Deaths (LFD) is a standard quarterly agenda item at the Trust Quality & Safety Committee where developments on the LFD agenda and learning is shared and to provide assurance on the Learning from Deaths process.
- 2.2 The Trust Mortality Surveillance Group continues to meet bi-monthly. Data and learning is presented from level 1 reviews, Structured Judgement Reviews, and by way of divisional exception reports following Mortality and Morbidity meetings which have a focus on learning and is then disseminated to all the directorates and throughout the divisions.
- 2.3 Unplanned Care have a Learning Newsletter that is distributed throughout the whole division after each quality and governance forum, this includes learning responses from patient safety incidents and Structured Judgement Reviews.
- 2.4 A Safety Improvement group (SIG) has been established which triangulates learning, themes and action plans from investigations including Structured Judgement reviews.
- 2.5 There have been no prevention of future deaths (PFD) notices issued following an inquest in this quarter.
- 2.6 **Patients with a learning disability/autism:** One completed case received during this quarter was for a patient who had a learning disability/autism and was graded as a CESDI 1 (Some suboptimal care – which did not affect the outcome).
- 2.7 The patient attended the Emergency Department following an absence seizure during a physiotherapy session, sustaining an ankle fracture and staff were in the process of transferring the patient to ED Resus when she lost output. The patient received immediate and appropriate care with response from the team with an appropriate decision taken to cease resuscitation. However, there was no documentation of patient's PMHx and History of presenting problem (i.e., no record of full PMHx,

medication and how the patient was leading up to the cardiac arrest over the last few days). Normally, during CPR efforts a team member would review the patient's past medical history and background and this would be fed back to the team leader. The SJR reviewer concluded that this information must have been gathered by the team but was not documented.

2.8 Review of all our SJRs received in quarter three have highlighted that there was excellent end-of-life care in a number of cases with early involvement from the Palliative Care Team and that families were fully involved in the decision-making process when patients deteriorated;

- Multi-Disciplinary Team Care: Early review by specialist and seniors, excellent initial medical assessment and thorough management plan made to involve the appropriate teams.
- Good communication with next of kin: Involvement of patient (initial contact) and then the family in decisions and provision of updates. Communication with the family was recognised to be difficult, despite this the medical notes document that they were kept fully updated.
- Appropriate care and management of the deteriorating patient: Good End-of-Life care with early palliative team involvement and syringe driver commencement. The Cardiac arrest was run well and is documented with appropriate decision to cease efforts. Good end of life care from palliative inpatient team and Bevan ward nurses.

2.9 Ten further SJR's received this quarter were also graded as 'Some suboptimal care which did not affect the outcome' CESDI 1. Key themes/issues identified include:

- Communication with the family was difficult. It may have affected staff's assessment of the patient & delayed their recognition of how unwell the patient was.
- The need for a pathway for completing death certificates out of hours when no doctor had seen the patient alive.
- Comfort observation to be more clearly visible on Cerner.
- Previous VBG results not visible under the results tab on Cerner. Noted that the scanned paper VBGs were uploaded to Medi-Viewer, approximately a week later.
- Importance of documenting the mortality/morbidity predictive score (NELA or p-possum) in entries discussing if a patient is fit for surgery or not.
- It is important to clearly document how many times and who attempted to insert an NG tube and at what point no further attempts were made, as well as discussions that were had with the patient +/- the family about this.
- Quality of discharge summaries needs improving.

### 3. Key themes

#### 3.1 Mortality rates

3.2 The HSMR Methodology looks at diagnostic groups most associated with in-hospital deaths, with the new methodology looking at 46 diagnostic groups rather than 51. A more sophisticated comorbidity measure is used to capture more conditions and an adjustment to frailty has also been introduced. Stillbirths have been removed from the new metrics. Across the APC, the new methodology has impacted Hillingdon Hospital the most with an increase in the HSMR. A deep dive into the new methodology data and the impact this has on Hillingdon Hospital's data and rates is being carried out to identify if the new methodology is a true reflection on the care provided at Hillingdon Hospital and this will be reported back at the next meeting.

The Hillingdon Hospital HSMR is accepted level rather than low. HSMR for August 2024 is 83.3 against the NHS benchmark of 100, the figure therefore shows as below the national average but is not statistically low. The data is coded correctly, however it shows that the patients at THH are less frail than elsewhere with confirmation received that the North West London population is younger, however the population's BMI is higher. There are ongoing discussions around coding for obesity which may have an impact on the data should this be included.

- 3.3 The SHMI data benchmark is 100 with Hillingdon Hospital showing at 97.95 and consistently improving. Hillingdon Hospital are the 52nd lowest out of 119 providers in the NHS where in 2022 we were the 90th lowest and which shows significant improvement. This data captures in-hospital and 30 days post discharge and looks at the discharging of patients and the quality of post discharge care. The data shows that the performance for the Hillingdon area is very good and consistent.
- 3.4 **Diagnostic Groups reviews**
- 3.5 In line with the agreed process across the Acute Provider Collaborative reviews are completed either because their HSMR is above the national benchmark of 100 (there is a difference between observed and expected deaths) or because their HSMR has been increasing and alerted at CUSUM level (within expected range but there is an increase in the trend).
- 3.6 The Mortality Surveillance Group monitors expected and observed deaths across diagnostic groups and where statistically significant variation is identified the group undertakes coding and care review to identify any themes or potential improvement areas.
- 3.7 There are three diagnosis group alerts in the HSMR data in September 2024 for Allergic Reactions, Appendicitis & Other Appendiceal Conditions and Multiple Myeloma, reviews have commenced for the patients identified. Reviews of Cardiac Arrest & Ventricular Fibrillation and Gout & Other Crystal Arthropathies are also being carried out as they alerted at CUSUM level. Reviews will be completed during quarter four and included in the next Learning from Deaths report.
- 3.8 **Ethnicity**
- 3.9 Work continues to review and develop our data so that we can understand any inequalities in or services.
- 3.10 Local population statistics identify that 42% of 'White British' people make up the resident population for the London Borough of Hillingdon. 16% 'Asian or Asian British – Indian' make up the second largest proportion of the resident population while 'White – Any Other White Background' make up 8% of the identified ethnicity.
- 'White British' remains the most frequently identified ethnicity associated with in-hospital mortality accounting for 60% of deaths occurring during quarter three. This is a noticeable difference to numbers of deaths in this ethnicity and is an increase to analysis in quarter two which identified 46% of in-hospital deaths as 'White British'. 'Asian – or Asian British Indian' was the second largest ethnic group in this quarter associated with in-hospital deaths, which aligns with the demographic composition of our local population and accounting for 9% of deaths.
  - The percentage of deaths where ethnicity is not known has increased from 2% in quarter two to 9% in quarter three.
  - Further analysis by ethnicity is provided in appendix B.

- 3.11 **SJR referrals by ethnicity:**
- The 'White British' group made up the highest number of referrals, 67% in quarter three, again similar to analysis in quarter two which was 72%. All other ethnic groups referred for SJR were small in numbers.
- 3.12 **Ethnicity by CESDI score and gender breakdown**
- 3.13 We have included gender in this quarter's analysis, however as our numbers are small it is still difficult to make meaningful analysis from this. Next steps will be to bring in additional demographic details such as age as well as including ethnicity of deaths in the community to expand our data set. Analysis of the 12-month period April 2024 to March 2025 will be included in the next Learning from Deaths report which may give more meaningful results.
- 3.14 20% of completed SJRs for 'White – British' deaths in quarter three resulted in a CESDI 1 score (one case) and 20% were graded as a CESDI 2 (one case). Both of these cases were for male patients but it is recognised that the numbers are too small for meaningful analysis
- 3.15 **Medical Examiner**
- 3.16 **Overview:**
- 3.17 The Medical Examiner Service in Hillingdon is responsible for scrutinising all deaths in hospital and identifying learning points, or deaths needing to be referred to the Coroner. On 9th September 2024, The Registration of Deaths (Medical Examiner) regulations were enforced. Since the implementation, significant changes have occurred within the system to incorporate the scrutiny of all non-coronial deaths within the borough which has been largely successful. All 45 GP surgeries have referred deaths to the Medical Examiner service and all non-coronial deaths within the borough have been scrutinised by the Medical Examiner team.
- 3.18 From October to December 2024, the Medical Examiners (ME) have scrutinised 437 total deaths within the borough of Hillingdon. 204 (100%) in-hospital deaths (including 3 children) of which 37 adults and 1 child (18.5%) were referred to the Coroner, with the Coroner retaining 22 (10.7%) for investigation: Fourteen were returned for certification with no requirement for further investigation. The Medical Examiners urgently reviewed 13 in-hospital deaths where their faith tradition required urgent registration and burial, including 3 (2 children) making use of the weekend on-call service.
- 3.19 Further scrutiny identified 233 community deaths (200 from GP practices, 33 from the local Hospice). The Trust have received referrals from 100% of local GP practices and assisted with referral of 20 (8.6%) community deaths to the Coroner of which 4 were kept for further investigation. 17 community deaths were urgently reviewed by the Medical Examiners, (including out of hours) where their faith tradition required urgent registration and burial.
- 3.20 **Achievements:**
- 3.21 We continue our excellent working relationships with our referrers, register offices, local funeral directors and the Coroner's office.
- 3.22 **Challenges:**
- 3.23 To Maintain momentum achieved before rollout, with ongoing encouragement of community partners to embrace the new system now that the advantages are becoming clear.
- 3.24 **Next steps:**
- 3.25 We are in a period of consolidation of our achievements and we are now able to focus on those of our partners who could probably achieve more timely referrals to ensure the optimisation of the service for the bereaved.

### 3.26 Structured Judgement Reviews (SJR)

3.27 The 12-month rolling data table below shows the number of adults deaths that have occurred along with the number of level 1 reviews completed, SJRs requested and SJRs returned.

Data pulled on 3<sup>rd</sup> February 2025

	Q4 23/24	Q1 24/25	Q2 24/25	Q3 24/25	Total
Total number adult deaths - (Based on date of death)	216	166	162	201	745
Total number of Levels 1 reviews for adult deaths	216	166	162	201	745
Number of patients referred for SJR- (Based on date of death)	11	23	17	15	66
Number SJRs returned (Based on date of death)	11	23	16	7	57
Number of SJRs awaiting return	0	0	1	8	9

- 3.28 There had previously been a delay around Structured Judgement Reviews being completed for ITU due to resource, which has now been resolved. Clinical work pressure has resulted in some reviews being delayed during December and January. The SJRs are now being monitored at the divisional scope meetings on a weekly basis to ensure that delays do not occur and the appropriate investigation is taken place with meaningful learning identified, all actions are recorded on the Trust GivemeData system to allow for triangulation of actions and evidence to be uploaded that the actions have been implemented.
- 3.29 One case relating to a death in quarter two for Structured Judgement Review was discussed at the Trust's Incident Review Group during this quarter, where it was agreed that as an After-Action Review had already been carried out with lessons learned and there would be no new learning from completing a SJR.
- 3.30 In quarter three 2024/25, Medical Examiners (ME) have scrutinised 201 adult patient deaths within the hospital with level 1 reviews being carried out for all of these cases. There is a consistent monthly 100% compliance rate for level 1 reviews being carried out which provides assurance around the level 1 review Trust process.
- 3.31 The percentage of inpatient deaths referred for a SJR in quarter three, 7% (15 cases), was lower compared to 11%, (18 cases) in quarter two.
- 3.32 'Requests by Medical Examiner' remains the most frequent trigger for Structured Judgment Review, accounting for 40% (n=6) of all referrals in the quarter.
- 3.33 Seven Structured Judgement Reviews relating to deaths occurring during Q3 2024/25 have been undertaken at the time of reporting; 43% (n=3) of which identified no sub-optimal care. Three cases were graded as a CESDI 1 (e.g. level of sub-optimal care identified during hospital admission, but different care or management would NOT have made a difference to the outcome and the death was unavoidable). One case was identified via the mortality review process as a CESDI 2 (Sub-optimal care, different care MIGHT have made a difference to the outcome – possible avoidable death).
- 3.34 Nine Structured Judgement Reviews relating to deaths occurring in previous quarters have been received during Q3 2024/25 which identified no sub-optimal care and eight cases were graded as a CESDI 1 (Some sub-optimal care which did not affect the outcome).
- 3.35 All CESDI 0 and CESDI 1 cases are sent to the divisional leads for oversight and to

- ensure that there is discussion and presentation at appropriate Speciality and Mortality & Morbidity meetings where the learning can be shared.
- 3.36 All cases with a CESDI 2 or 3 outcome automatically trigger escalation to the executive for a decision on appropriate learning response. There have been no common themes identified in the two cases graded as a CESDI 2 in quarter two and quarter three.
- 3.37 Reviews received in this quarter found no cases of Suboptimal care where it would reasonably be expected to have made a difference to the outcome (CESDI 3).
- 3.38 In four cases (n=4) there was found to be poor care during the patient's phase of care:
- Admission and Initial management (n=3)
  - Ongoing care (n=1)
  - Care during procedure (n=1)
  - Perioperative care (n=0)
  - End of Life care (n=0)
- 3.39 Evidence of excellent care has been recognised during patients' phase of care in a number of the reviews completed (n=7):
- Admission and Initial management (n=5)
  - Ongoing care (n=4)
  - Care during procedure (n=4)
  - Perioperative care (n=0)
  - End of Life care (n=7)
- 3.40 There has been introduction of a Mortality & Morbidity meeting in Care of the Elderly, the first one of which is expected to be held in February 2024. Focus will be on cases completed that carry more learning within them rather than review of all deaths within the specialty. Junior Doctors will be involved in presenting the learning and will provide a good teaching opportunity. All deaths are reviewed by the division for their oversight and through the unplanned care Mortality & Morbidity forum.
- 3.41 Trial of a monthly meeting, Divisional Mortality Review Group, (DMRG) with Planned Care took place in January which focused on the outcomes of completed SJRs that had been graded as a CESDI 1 or a CESDI 2. The aim of the meeting was to provide scrutiny to mortality cases and the grades as well as identify themes and escalate any issues of concern. Timely divisional approval of actions would be included in the agenda. The meeting went well and this will be taken to the next Mortality Surveillance Group meeting for discussion of it going forward and consideration of attendees.
- 3.42 Work continues with the all the divisions to review all outstanding SJRs. Regular meetings take place with the Governance Manager for planned care with escalation to the division. Consideration is being given as to who would be best placed to support a regular meeting in unplanned care, although it should be noted that cases are always highlighted to the Interim Director of unplanned care and the division.
- 3.43 **PMRT**
- 3.44 **Overview:**
- There were five stillbirths in quarter three.
  - The crude stillbirth rate is 3.42 per 1000 births.
  - There were no neonatal deaths in quarter three.
  - There were no terminations of pregnancy in quarter three.
- 3.45 **Challenges:**
- All five stillbirths were of Indian ethnicity, only one mother had identified language needs. Although on investigating, a translator had been provided for two mothers.

- There were two stillbirths where the Fetal Growth Restriction (FGR) guideline was not followed at booking.
- Two mothers were diabetic and care was given following the diabetic pathway.
- Out of three stillbirths, two were diagnosed on admission for Induction of Labour and one was diagnosed on a routine growth scan.

3.46 **Improvements made:**

- Following the stillbirth review the Trust now has a dedicated PMRT Midwife who will put the PMRT reviews on Give Me Data and this sends a prompt to staff to update any actions assigned to them. There is regular monitoring of this and actions are reviewed accordingly.
- There were previously discrepancies surrounding the use of aspirin in high risk pregnancies which not all North West London trusts were using. We now have sector wide guidance on updating the FGR guideline to align with Saving Babies Lives v3. The new guideline ensures that we are all following the same pathway.

3.47 **Recommendations:**

- The FGR Guideline is not always followed at booking. This appears to be a common theme and we are collaborating with the Digital Midwives and the Antenatal Manager on strong actions aiming to ensure that this is identified at booking. Currently there is a Cerner freeze preventing this from being implemented online.
- A peer review audit of measurement quality in scans as per British Medical Ultrasound Society (BMUS) Guidelines is due to take place by the Lead Sonographer to ascertain the discrepancies between estimated fetal weight and actual birth weight.
- An audit is currently in progress of the use of the partogram, a labour monitoring tool, during labour for stillbirths.

3.48 **LeDeR**

3.49 **Overview:**

3.50 As a Trust we follow the LeDeR programme to improve healthcare for people with Learning Disabilities and Autism. From January 2022, LeDeR reports have included deaths of autistic people without a learning disability. In response to this change and following stakeholder engagement, the new name for the LeDeR programme is 'Learning from Life and Death Reviews – people with a learning disability and autistic People'.

3.51 The LeDeR programme seeks to co-ordinate, collate and share information about the deaths of people with learning disabilities and autistic people so that common themes, learning points and recommendations can be identified and taken forward at both local and national levels. The Trust is committed to ensuring deaths of patients with known/pre-diagnosed learning disabilities and/or autism are reported to the LeDeR programme and reviewed accordingly.

3.52 For an autistic adult to be eligible for a LeDeR review, they must have had a confirmed diagnosis of autism reported in their clinical records before their death. LeDeR does not include those who self-identify as autistic or anyone who has not received a clinical diagnosis from a qualified health professional.

3.53 Two patients who died in quarter three and identified as having a learning disability/autism have been notified on the LeDeR portal for review. There has also been one referral received from the community for an adult with learning disability who died in October 2024. The patient was known to the hospital and palliative care and notified to LeDeR for review by the Learning Disability Nurse here.

### 3.54 **Challenges**

3.55 There are multiple codes being used on Cerner. The Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT) supposedly provides an efficient way to highlight patients with a learning disability and/or autism with comprehensive high quality clinical content in patients electronic health records. However, there are multiple problem lists and SNOMED term for the same medical condition. The reasonable adjustment flag remains inactive on Cerner which helps to identify patients with a learning disability and/or autism who may require more support and reasonable adjustments made for them.

3.56 External LeDeR reviewers staffing changes constantly, there is no continuity and with different reviewers requesting for different records. Once a death is notified to LeDer, the reviewer now not only request for the Structural judgement review completed, but also require full comprehensive medical records from admission to events leading up to the patient's death. This has an impact on team time completing these requests.

### 3.57 **Improvements made:**

3.58 Having established a good working network with the community and North West London, deaths are being reported and reviewed more promptly than before.

### 3.59 **Good Practice within Hillingdon Hospital**

3.60 Learning Disability awareness training has been carried out at both Hillingdon and Mount Vernon hospital. Autism awareness has been provided by Hillingdon Autistic Care and Support (HACS) which received positive feedback from staff. There is also mandatory training which includes Autism awareness and there continues to be increased staff awareness of reasonable adjustments that may be needed for any patients with a learning disability and/or autism.

3.61 Linking in with the HATS (patient transport) team and Hillingdon Hospital Outpatients for patients who may require support or reasonable adjustments made when attending their appointment.

### 3.62 **CDOP**

#### 3.63 **Overview:**

3.64 During this quarter there were four deaths in children who had received direct care at The Hillingdon Hospital, two of which were out of the area. In addition there were a further two deaths of children at other Trusts, who were Hillingdon residents. Both of these children were premature babies born at tertiary hospital.

3.65 The four children who had received care at The Hillingdon Hospital:

- 14-month with metabolic encephalopathy and life limiting illness, passed away from Flu A and overwhelming sepsis.
- 8-month Sudden Unexpected Death in Infancy (SUDI) having been found between two mattresses.
- 9-year old poorly controlled asthma.
- 6-year old non curable brain malignancy with likely acute intracranial event and RSV infection.

#### 3.66 **Challenges:**

3.67 Asthma Deaths: There have been two deaths of children with asthma within North West London during this quarter. Common factors have been poorly controlled asthma, multiple attendances to GP/UCC/A&E, multiple reliever prescriptions and missed appointments. There is a lack of consistent Paediatric Asthma provision across all the North West London Trusts, and lack of consistent Paediatric Asthma provision across all the NWL Trusts, and lack of clear pathways of identifying high risk children.

3.68 Safer sleeping: There was another likely SUDI due to unsafe sleeping arrangements despite ongoing safer sleeping advice. Advice had been given to this particular family,

but the sleeping environments had not changed.

### 3.69 **Recommendations:**

3.70 There will be a review of all recent asthma deaths within North West London which will be presented at the next NWL Child Death Review Team Strategic meeting. Findings and recommendations will be shared with the Integrated Care Board (ICB).

## 4. **Areas of focus**

### 4.1 **Cerner EPR**

4.2 As highlighted in the quarter two report there is still a discrepancy with some of the mortality data being captured by the Digital Services Team and we need to ensure our mortality data accurately reflects the correct figures. Issues identified around deaths are still currently:

- Patients are not discharged off Cerner – These are then not counted in reporting.
- Patients are discharged with an incorrect discharge method (should always be 4-Died or 5-Stillbirth) – These are then not considered deaths.
- Patients not discharged on the day they died (the date of death is different to the discharge date) – These deaths are reported in different week of the month/month but only surface once discharged.
- Confirmation of Death Form is not always recorded – This is more of a workflow issue and is still being reviewed to assess the impact it has on reporting.

4.3 A weekly Mortality Data Quality report which includes each of the issues identified is sent to the Divisional Directors and Chief Nurse Information Officer for dissemination to the affected areas and there is continued work with the Cerner 'Super Users' on the wards.

### 4.4 **Monitoring of compliance, learning and actions**

4.5 The Trust does not currently have a digital platform for mortality. As outlined in previous reports we are still exploring, and in discussion with the Acute Provider Collaborative, different systems that will support with monitoring compliance, triangulation of data and learning from incidents, audit, complaints and mortality for us all. This will support with improving the completion of SJRs and monitoring and evidencing the learning that is identified as part of the Structured Judgement Review. There is currently no progress to be able to report on this.

### 4.6 **Specialty Mortality and Morbidity meetings**

4.7 Work is ongoing with Specialty Mortality and Morbidity (M&M) meetings in Planned Care. Planned Care are now using the standardised slide deck template at all their M&M meetings, however we will continue to support them to ensure that any learning identified and actions are captured in the presentations.. A new M&M meeting within Care of the Elderly is commencing from February 2024 with uptake of this standardised slide deck template.

4.8 Divisional exception reports following M&M meetings are being presented and discussed at the Mortality Surveillance Group meeting (MSG). This provides an overview of learning with the opportunity for any case discussion, actions being taken and escalation for MSG to take forward.

### 4.9 **Mortality Leads**

4.10 As previously reported there remain vacant posts for a mortality lead in Medicine and Surgery.

### 4.11 **Completion of SJR and learning from deaths**

4.12 Expectation is that SJRs are completed with two weeks and that the current process we have will remain at present. There had previously been a delay around Structured Judgement Reviews being completed for ITU due to resource, which has now been resolved and clinical work pressure has resulted in some reviews being delayed during

December and January. The SJRs are now being monitored at the divisional scope meetings on a weekly basis to ensure that delays do not occur and the appropriate investigation is taken place with meaningful learning identified, all actions are recorded on the Trust GivemeData system to allow for triangulation of actions and evidence to be uploaded that the actions have been implemented. This work has oversight from the Trust Mortality Surveillance Group.

- 4.13 Trial of a monthly meeting, Divisional Mortality Review Group, (DMRG) with Planned Care took place in January which focused on the outcomes of completed SJRs that had been graded as a CESDI 1 or a CESDI 2. The aim of the meeting was to provide scrutiny to mortality cases and the grades as well as identify themes and escalate any issues of concern. Timely divisional approval of actions would be included in the agenda. The meeting went well and this will be taken to the next Mortality Surveillance Group meeting for discussion of it going forward and consideration of attendees.

## 5 Conclusion

- 5.1 The outcome of the Trust's mortality surveillance programme continues to be a rich source of learning that is supporting the organisation's safety improvement objectives.
- 5.2 The Trust is committed to delivering a just, open and transparent approach to investigations that reduces the risk and consequences of recurrence. We can provide assurance to the committee that we are providing safe care for the majority of patients. Where care issues are found, we have robust processes for referral for more in-depth review and these processes are triangulated within the Trust under the PSIRF framework.
- 5.3 Work continues to align and improve our learning from patient death processes, and actively support the alignment across the acute provider collaborative to aid comparison, learning and opportunities for improvement. However, the current process will remain at present due to funding.
- 5.4 We are continuing to explore different systems with the Acute Provider Collaborative that will support with monitoring SJR compliance rate, learning and triangulation of data from SJRs, incidents, audit, and Complaints.

## 6. Glossary

- a. **Medical Examiners** are responsible for reviewing every inpatient death before the medical certificate cause of death (MCCD) is issued, or before referral to the coroner in the event that the cause of death is not known or the criteria for referral has been met. The Medical Examiner will request a Structured Judgement Review if required or if necessary refer a case for further review and possible investigation through our incident reporting process via the quality and safety team. The ME will also discuss the proposed cause of death including any concerns about the care delivered with bereaved relatives.
- b. **Structured Judgement Review (SJR)** is a clinical judgement based review method with a standard format. SJR reviewers provide a score on the quality of care provided through all applicable phases of care and will also identify any learning. The SJR will be completed within seven days of referral.
- c. **Structured judgement reviewers** are responsible for conducting objective case note reviews of identified cases. They will seek, when required, specialist input and advice from clinical colleagues, including members of the multi-disciplinary teams to ensure high quality, comprehensive review is undertaken, using the full range of medical records available to them.

- d. **Specialty M&M** reviews are objective and multidisciplinary reviews conducted by specialties for cases where there is an opportunity for reflection and learning. All cases where ME review has identified issues of concern must be reviewed at specialty based multi-disciplinary Mortality & Morbidity (M&M) reviews.
- e. **Child Death Overview Panel (CDOP)** is an independent review aimed at preventing further child deaths. All child deaths are reported to and reviewed through Child Death Overview Panel (CDOP) process.
- f. **Perinatal Mortality Review Tool (PMRT)** is a review of all stillbirths and neonatal deaths. Neonatal deaths are also reviewed through the Child Death Overview Panel (CDOP) process. Maternal deaths (during pregnancy and up to 12 month post-delivery unless suicide) are reviewed by Healthcare Safety Investigation Branch and action plans to address issues identified are developed and implemented through the maternity governance processes.

**Learning Disabilities Mortality Review (LeDeR)** is a review of all deaths of patients with a learning disability. The Trust reports these deaths to the Local integrated care boards (ICBs) who are responsible for carrying out LeDeR reviews. SJRs for patients with learning disabilities are undertaken within the Trust and will be reported through the Trust governance processes.

**Author:** Paula Perry, Clinical Governance Facilitator for Mortality

**Date:** 03/02/2025

### **List of appendices**

Appendix 1 – Performance Scorecard

Appendix 2 – Ethnicity

Appendix 3 – Flow Chart referral to LeDeR

## Appendix 1 – Performance Scorecard

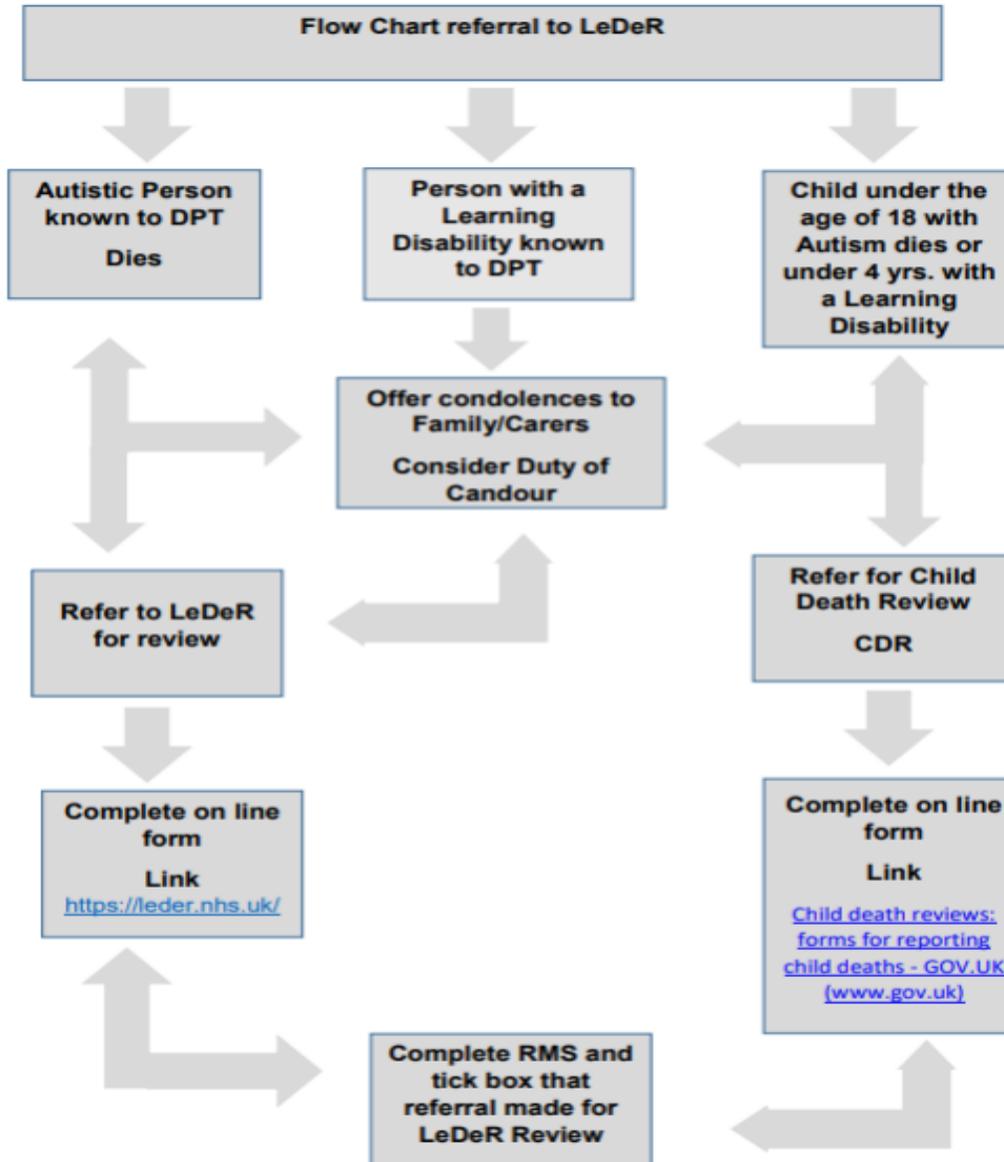
	Q4	Q1	Q2	Q3	Comments	National LfD minimum requirement?
<b>Summary data</b>						
Total no. deaths (adult and children, including neonatal and excluding stillbirths)	218	167	164	204	Inpatient deaths only	
Total no. adult deaths	216	166	162	201	Inpatients over 18 years age	Y
No. adult deaths per 1,000 non-elective bed days	TBC	TBC	TBC	TBC		
Total no. child deaths	1	1	1	3	Inpatients over 28 days and less than 18 year only	
Total no. neonatal deaths	1	0	1	0	Inpatients livebirths under 28 days of age	
Total no. stillbirths	5	1	3	5	Inpatient not live births	
<b>Review summary</b>						
Deaths reviewed by Medical Examiner	218	167	164	204		
% Deaths reviewed by Medical Examiner	100%	100%	100%	100%	% of total deaths	% of row 1
Deaths referred for Level 2 review	11	23	17	15		
% Deaths referred for Level 2 review	5%	14%	10%	7%	% of total adult deaths	% of row 2
Level 2 reviews completed	11	23	16	7		
% Level 2 reviews completed	100%	100%	94%	47%	% of total referrals this quarter	Y
Total Deaths Reviewed Through the LeDeR Methodology	0	4	1	2		
<b>Level 2 referral reason breakdown</b>						
Requests made by a Medical Examiner	(1) 9%	(6) 26%	(9) 50%	(6) 40%	% of total referrals	
Concerns raised by family / carers	(7) 64%	(9) 39%	(3) 17%	(5) 33%	% of total referrals	
Patients with learning disabilities	(0) 0%	(4) 17%	(1) 6%	(2) 13%	% of total referrals	

Patients with severe mental health issues	(3) 27%	(2) 9%	(2) 11%	(3) 20%	% of total referrals	
Unexpected deaths	(0) 0%	(5) 22%	(1) 6%	(1) 7%	% of total referrals	
Elective admission deaths	(1) 9%	(1) 4%	(1) 6%	(0) 0%	% of total referrals	
Requests made by speciality mortality leads / through local Mortality and Morbidity review processes	(0) 0%	(1) 4%	(1) 6%	(0) 0%	% of total referrals	
Service or diagnosis alarms as agreed by APC mortality surveillance group	(0) 0%	(0) 0%	(0) 0%	(0) 0%	% of total referrals	
Random selection of deaths for SJR review	(0) 0%	(0) 0%	(3) 17%	(0) 0%		
<b>Level 2 review outcomes</b>						
CESDI 0 - No suboptimal care	9	11	8	3	% of cases reviewed	Total Figure
CESDI 1 - Some sub optimal care which did not affect the outcome	2	12	7	3	% of cases reviewed	Total Figure
CESDI 2 - Suboptimal care – different care might have made a difference to outcome (possible avoidable death)	0	0	1	1	% of cases reviewed	
CESDI 3 - Suboptimal care - would reasonably be expected to have made a difference to the outcome (probably avoidable death)	0	0	0	0	% of cases reviewed	Y
<b>SHMI and HSMR</b>						
SHMI 12-month rolling					Provided by Telestra Health UK	
HSMR 12-month rolling					Provided by Telestra Health UK	
Palliative Care SHMI 12-month rolling					Provided by Telestra Health UK	
Palliative Care HSMR 12-month rolling					Provided by Telestra Health UK	

## Appendix 2 – Ethnicity

	Total	2023/24	2024/25			2023/24	2024/25		
		Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
<b>Asian - Any Other Asian Background</b>		8	11	11	13	3.67%	6.58%	6.71%	6.47%
<b>Asian or Asian British - Bangladeshi</b>		0	0	0	1	0.00%	0.00%	0.00%	0.50%
<b>Asian or Asian British - Indian</b>		20	22	27	19	9.17%	13.17%	16.46%	9.45%
<b>Asian or Asian British - Pakistani</b>		1	0	1	4	0.46%	0.00%	0.61%	1.99%
<b>Black - Any Other Black Background</b>		0	2	0	0	0.00%	1.20%	0.00%	0.00%
<b>Black or Black British - African</b>		3	6	2	1	1.38%	3.59%	1.22%	0.50%
<b>Black or Black British - Caribbean</b>		4	3	1	3	1.83%	1.80%	0.61%	1.49%
<b>Mixed - Any Other Mixed Background</b>		0	0	1	1	0.00%	0.00%	0.61%	0.50%
<b>Mixed - White and Asian</b>		0	0	1	1	0.00%	0.00%	0.61%	0.50%
<b>Mixed - White and Black African</b>		0	0	1	2	0.00%	0.00%	0.61%	0.99%
<b>Mixed - White and Black Caribbean</b>		0	0	1	1	0.00%	0.00%	0.61%	0.50%
<b>Other - Any Other Ethnic Group</b>		18	4	3	11	8.26%	2.39%	1.83%	5.47%
<b>Other - Chinese</b>		1	1	0	0	0.46%	0.60%	0.00%	0.00%
<b>Other - Not Known</b>		0	0	3	19	0.00%	0.00%	1.83%	9.45%
<b>Other - Not Stated</b>		0	0	0	0	0.00%	0.00%	0.00%	0.00%
<b>White - Any Other White Background</b>		44	24	37	3	20.18%	14.37%	22.56%	1.49%
<b>White - British</b>		117	91	75	121	53.67%	54.50%	45.73%	60.20%
<b>White - Irish</b>		2	3	0	1	0.92%	1.80%	0.00%	0.50%
<b>Total</b>		218	167	164	201	100.00%	100.00%	100.00%	100.00%

**APPENDIX 3 – Flow Chart  
referral to LeDeR**



## 5.1. COLLABORATIVE DATA AND DIGITAL COMMITTEE REPORT - NWL ICB CYBER SECURITY STRATEGY

---

### REFERENCES

Only PDFs are attached

-  5.1b. Cyber security strategy - NWL ICB Cyber Security Strategy - v4.5 final draft.pdf

# NORTH WEST LONDON INTEGRATED CARE BOARD CYBER SECURITY STRATEGY

Final draft

# CONTENTS

EXECUTIVE SUMMARY .....	4
STRATEGY TIMELINES .....	7
KEY .....	7
INTRODUCTION .....	11
CYBER SECURITY STRATEGY .....	18
STRATEGY GOVERNANCE .....	21
KEY CYBER STRATEGY DATES .....	65
RESOURCING THE STRATEGY .....	66
KEY STAKEHOLDERS .....	67
APPENDIX A – DSPT / CAF – STRATEGIC OUTCOMES .....	70
APPENDIX B - LIST OF NATIONAL SERVICES AND RESOURCES .....	71
APPENDIX C - REFERENCES .....	73
APPENDIX D - CHECKLIST FOR BOARD ASSURANCE .....	75
APPENDIX E - CHECKLIST FOR STRATEGY AUTHORS .....	76
APPENDIX F – OUTCOME 1 – ORGANISATIONAL RACI FOR ADOPTING THE CYBER SECURITY STRATEGY PILLARS .....	77
APPENDIX G – OUTCOME 2 – ORGANISATIONAL RACI FOR THE NHSE CYBER RISK INVESTMENT .....	81
APPENDIX H – OUTCOME 3 – ORGANISATIONAL RACI FOR STAFF AWARENESS AND CULTURE .....	86

APPENDIX I – OUTCOME 4 - ORGANISATIONAL RACI FOR CAF  
ALIGNED DSPT..... 87

APPENDIX J – OUTCOME 1 – ADOPTING THE CYBER SECURITY  
STRATEGY PILLARS GANTT CHART ..... 89

APPENDIX K – OUTCOME 2 – NHSE CYBER RISK INVESTMENT  
GANTT CHART ..... 91

APPENDIX L – OUTCOME 3 – STAFF AWARENESS AND  
CULTURE .....93

APPENDIX M – OUTCOME 4 – CAF-ALIGNED DSPT GANTT  
CHART..... 94

APPENDIX N – OUTCOME 2 – NW LONDON ICS CYBER RISK  
INVESTMENT – ASSESSMENT TOOL ..... 99

ABBREVIATIONS.....108

DOCUMENT CONTROL.....111

## Executive Summary

Integrated Care Boards (ICBs) are accountable to NHS England for risk management across their healthcare provider organisations, including for cyber security risk management. This North West London ICB Cyber Security Strategy outlines the overall approach for each Trust to take to incorporate into their Trust specific cyber security strategy to ensure the protection of sensitive data, the resilience of their healthcare services and compliance with legal and regulatory obligations.

The NHS, as part of the UK Critical National Infrastructure (CNI) and a processor of large volumes of highly sensitive information, faces additional legal obligations to secure services and data. While digital adoption has improved administrative processing response times, patient outcomes, and overall efficiency, it has also increased exposure to cyber threats. In the last six months, cyber incidents have disrupted major trusts like Guys and St Thomas, Kings College Hospital, and Alder Hey.

This Cyber Security Strategy offers a framework (the “what”) for Trusts to develop localised Cyber Security Strategies (the “how”). This strategy follows the national published guidance for the [NHS in March 2023 Cyber security strategy for health and social care: 2023 to 2030](#). While NHS England may fund some elements of cyber security through nationally procured products and services, each Trust is ultimately responsible for financing its strategy and meeting its compliance obligations.

No level of investment can guarantee security, but the majority of attacks can be avoided by implementing the tools, protections and preparation outlined in this strategy. Senior Executive support is vital for success.

### Scope

NW London ICB Trusts and organisations in scope of this strategy are;

1. Central London Community Healthcare NHS Trust
2. Central and North West London NHS Foundation Trust
3. West London NHS Trust
4. Imperial College Healthcare NHS Trust
5. Chelsea and Westminster Hospital NHS Foundation Trust
6. London North West University Healthcare NHS Trust
7. The Hillingdon Hospitals NHS Foundation Trust
8. NW London Integrated Care Board, including NW London Primary Care.

## Funding and Accountability

Each Trust in the ICB remains accountable for ensuring the resilience of their services and the security and integrity of their data. There is nothing in this document which alters those obligations. This document, based on NCSC and NHS published guidance, is intended to assist Boards to prioritise proven risk-reducing investments, develop mitigation plans to strengthen service resilience in the event of disruption, and set out a road map of improvements for risk mitigation and management of cyber across the ICB.

There is currently no identified central funding from the ICB or NHSE for implementing the strategy. Organisations must use their own resources. If central funds become available, the ICB will distribute them. NHSE offers free resources like threat monitoring tools and risk assessments, which Trusts should deploy and use thereby freeing up local money to focus on capabilities not provided by the national team.

The implementation timeline outlines *minimum* achievements for the next two - three years. Trusts are encouraged to exceed these milestones where possible.

## Recommendations

We have aligned the strategy to achieve four key strategic outcomes, which are aligned to business goals, regulatory and NHSE requirements:

- **Outcome 1** - Adopt the [NHSE Five Cyber Security Strategy Pillars](#)
- **Outcome 2** - Assess compliance with the [NHSE Cyber Risk Investment](#) requirements, and develop a roadmap for investment and implementation
- **Outcome 3** – Assess [Staff Awareness and Culture](#), using NHSE guidance and develop a roadmap to enhance
- **Outcome 4** - We will adopt [A Strategy to Adopt the CAF Aligned DSPT](#)

In addition to setting out the timeline for adoption and implementation of core cyber security defensive and restorative capabilities, the strategy also makes four other key recommendations to aid the ICB in managing the overall risk.

1. Develop a standard Board reporting framework for cyber security risk and activity reporting, including Emergency Preparedness, Resilience and Response (EPRR) preparedness and planning for long duration digital disruption
2. Standardise on a methodology for cyber risk scoring across Trusts in the ICB using an evidence based methodology
3. Implement an information sharing agreement, covering all Trust's in the ICB, to share cyber security risk scoring data.
4. Each Trust to develop a financial model showing the cost of disruption from a long duration cyber security outage so that the potential financial impacts are understood. Suggested time horizon for the model is 12 weeks.

Supporting the recommendations in this strategy will reduce the likelihood of service disruption and lessen the impact when disruption occurs.

This document, once approved, is intended to be used as a basis for developing localised cyber security strategies. Each localised strategy will need to take into account the NHSE What Good Looks Like guidance and well as NIS and GDPR requirements.

The strategy envisions a secure healthcare system where patient data is safeguarded, and services remain uninterrupted. The primary objectives of this strategy include:

- Protecting patient data from unauthorised access and breaches.
- Ensuring continuous healthcare service availability and integrity.
- Maintaining compliance with relevant cyber security regulations and standards.
- Encourage and support innovation and collaboration in Cyber Security, across ICS organisations and external partners.
- Foster a culture of continuous learning and improvement; leveraging industry best practices.

### **Key Initiatives and Activities**

To achieve these objectives, we will implement several key initiatives:

- Deploying advanced security technologies to detect and prevent cyber threats.
- Enhancing cyber security awareness and training programs for all staff.
- Strengthening incident response capabilities to quickly address and mitigate cyber incidents.

### **Governance and Accountability**

The strategy will report into existing Digital and Data governance structures. The requirements set out in the strategy will be incorporated into each Trusts annual planning cycles and delivered through existing teams, resources and governance structures.

The ICB will monitor overall progress with achievement of the strategy and deploy any available centralised funding to Trusts to assist with implementation.

Members from all NWL ICS organisations and the NHSE Regional Security Lead were involved in reviewing the strategy to ensure all factors were considered. Feedback indicated that the ICS Cyber Security Strategy provided clear direction on initiatives. The agreed strategic timelines are summarised below:

# Strategy Timelines

## Key

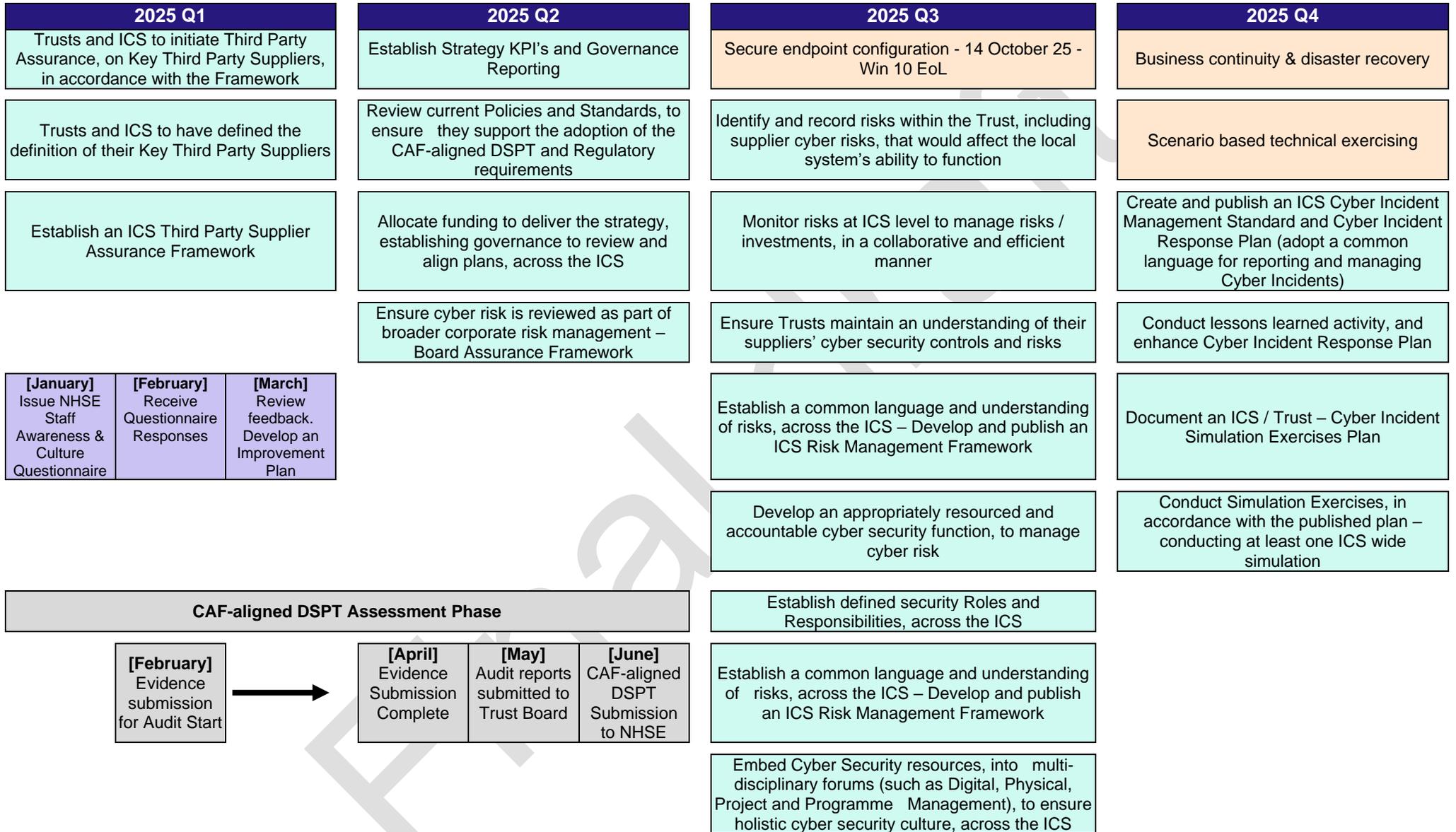


## 2024

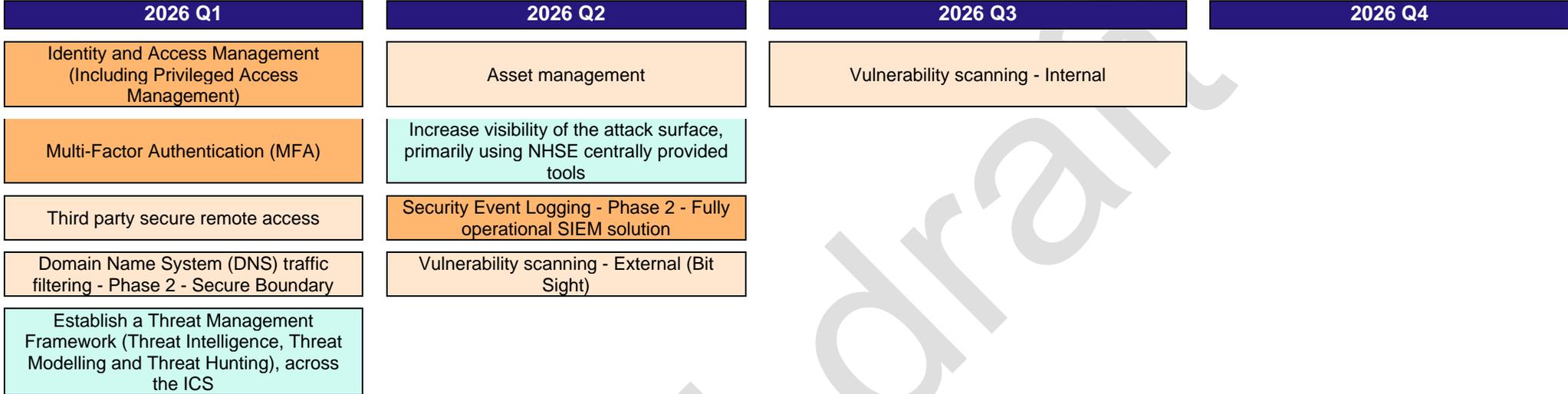
2024 Q1	2024 Q2	2024 Q3	2024 Q4
-	-	-	Interim Baseline Assessment - 31 Dec 24
			<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 2px;"> <b>[October]</b>                      'NW London ICS Cyber Risk Investment – Assessment Tool' issued                 </div> <div style="border: 1px solid black; padding: 2px;"> <b>[November]</b>                      'NW London ICS Cyber Risk Investment – Assessment Tool' returned                 </div> </div> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <b>[October]</b>                      Submit Cyber Risk Reduction Funding Form (FY24-25)                 </div>

## 2025

2025 Q1	2025 Q2	2025 Q3	2025 Q4
Practice Secure by Design, on new projects and programmes, across the ICS	Malware Detection	Vulnerability Management	Backups
Document an ICS level Secure by Design Assurance / Certification Process (3LOD model)	Perimeter Protection	Cyber Risk Management	Security Event Logs - MVP Phase 1 - Log Retention / Minimum Viable Logs (Critical Logs)
Document and publish guidance and training on Secure by Design	Cyber Strategy & Governance	Domain Name System (DNS) traffic filtering - Phase 1 - PDNS Deployment	Cyber Incident Management



2026



2027



Figure 1

### **Risk Management**

We will adopt a proactive and standardised approach to risk management, including regular risk assessments and the implementation of robust mitigation strategies. This will help us identify and address potential vulnerabilities before they can be exploited.

### **Performance Metrics and Evaluation**

The success of our cyber security strategy will be measured using key performance indicators (KPIs) such as the number of incidents detected and resolved, staff training completion rates, and compliance audit results. Regular evaluations will be conducted to ensure continuous improvement.

### **Conclusion**

This strategy underscores our commitment to maintaining robust cyber security measures to protect patient data and ensure the resilience of our healthcare services. By implementing these four outcome initiatives, we aim to create a secure environment that supports the delivery of high-quality care.

Final draft

# Introduction

## North West London Integrated Care System

The North West London Integrated Care System (ICS) is responsible for contracting healthcare services locally and the oversight of the local NHS budget. NW London ICS is a collaborative partnership that brings together health and care organisations to improve the overall health and care services for the population of North West London. The ICS encompasses a wide range of partners, including NHS bodies, local authorities, community and voluntary organisations, and primary care networks. It has an extensive role in primary, secondary and community care, some of which are sole responsibilities, others in a joint or shared function with NHS England (NHSE). The NW London ICS focuses on working collaboratively to address challenges like health inequalities, demand for emergency services, and long-term conditions, ensuring that care is more coordinated across the region. The NW London ICS includes the following healthcare providers:

### Acute Trusts:

- Imperial College Healthcare NHS Trust
- Chelsea and Westminster Hospital NHS Foundation Trust
- London North West University Healthcare NHS Trust
- The Hillingdon Hospitals NHS Foundation Trust

### Community and Mental Health Trusts:

- Central and North West London NHS Foundation Trust (CNWL)
- West London NHS Trust (WLNT)

### Community Healthcare Trusts:

- Central London Community Healthcare NHS Trust (CLCH)

### Primary Care:

- 360 GP Practices
- 44 Primary Care Networks
- The Integrated Care Board is responsible for systems (including cyber security) in Primary Care and also in its own head office and programme teams.

NW London ICS covers the following London boroughs: Brent, Ealing, Harrow, Hammersmith & Fulham, Hillingdon, Hounslow, Westminster, and the Royal Borough of Kensington and Chelsea. Local Authorities' Cyber Security Strategies span all their services (including social care) and are therefore outside the scope of this document.

## Security in Healthcare

Healthcare is becoming increasingly dependent on digital solutions for the prompt, safe and effective delivery of data and information to those that need it. Cyber incidents present a real risk to business functions, organisational objectives, and patient safety. This risk is prominent for systems and data

that are hosted and/or consumed by ICS member organisations. A cyber incident is commonly a trigger to the realisation of other organisational risks.

Ensuring the Confidentiality, Availability and Integrity of the data that we process and store, required for operational functions on behalf of our patients, is fundamental. There are legal, regulatory, and ethical obligations that ICS member organisations must fulfil.

**Confidentiality** – Only those authorised and with a valid business need can access information and systems, ensuring data is only disclosed to others in line with the policy and process.

**Integrity** – Information and systems are protected against unauthorised change and data can be deemed precise and factual.

**Availability** - Information and systems are available and accessible when required and can sufficiently deter or resist attacks.

This strategy outlines how the NW London ICS will collaboratively deliver long term cyber security direction and objectives, based on a decision horizon covering the 2025-2027 financial years. This strategy outlines how to achieve the following objectives, aligned to the five pillars in the *Cyber Security Strategy for Health and Social Care: 2023 to 2030*, as detailed in the 'Guidance for Developing an ICS Cyber Security Strategy':

**Objective 1** – Identifying and Managing Risk

**Objective 2** – Strengthening Governance

**Objective 3** – Embedding Cyber Awareness and Culture

**Objective 4** – Critical Systems and suppliers

**Objective 5** – Prediction, Prevention, Detection, Response and Recovery

The objectives are aligned to underpin the overall NW London ICS operational strategy, and empower the digital strategy. Supporting direction to enrich healthcare objectives and manage risk to enable the overall delivery of secure, sustainable, and safe services to the local population in a timely manner, aligned with the NHS long term plan.

Senior level ICS stakeholder understanding and support is fundamental to achieving this strategy, coupled with sufficient skilled and/or specialised resourcing to deliver the outlined objectives.

## Current Landscape

Cyber security remains a priority for the ICS and its member organisations. It requires considerable time and resources to maintain an acceptable level of risk. NHS Trusts and Integrated Care Boards are identified as Network and Information Systems (NIS) Regulations 2018, Operators of Essential Service (OES), which ultimately outlines that any services provided by them (including the making of arrangements for the provision of services by others) are deemed as essential services.

Nationally funded services are available from NHS England and are already embedded in some areas. ICS member organisations have varying cyber maturity, posture, and risk appetites. There is a range of technologies deployed across the ICS. Where finances have been constrained for IT investment in some Trusts, this has led to some assets being used beyond their 'end of life' support arrangements and increased the risk of a cyber-incident.

Each Trust within the ICB is responsible for ensuring the NHSE Self-Assessment Tools (DSPT and CAF) are completed annually and that targets set by the toolkit archive a 'standards met' level of compliance. With the exception of the NHSE Cyber Risk Investment funding, this Cyber Security Strategy is not funded centrally, therefore, appropriate management of budget allocations is critical to ensure successful implementation and reducing cyber risk.

## Cyber Threat Landscape

At October 2024, the Espionage and Terrorism Threat Level across the UK is 'SUBSTANTIAL'. This means that an 'Attack is Likely'. The National Cyber Security Centre (NCSC), have confirmed that the UK Cyber Security Threat Level is 'Heightened', following the Russian invasion of Ukraine, and escalation in the Middle East, between Israel, Palestine, Lebanon, and Iran. The NCSC is calling on UK organisations, to strengthen their digital defences. As detailed by the NCSC, in its 'Cyber Threat to the UK Health and Social Care Sector' document:

- Ransomware almost certainly remains the largest and most likely disruptive threat to the UK health and social care sector.
- The primary threat from nation states towards the UK health and social care sector is almost certainly cyber espionage, for the purposes of intelligence gathering to support their own strategic goals.
- Cyber actors will almost certainly continue to target the UK health and social care sector supply chain, in order to facilitate their cyber operations and access a large number of potential victims.
- It is highly likely that the UK health and social care sector is considered an attractive target to a range of threat actors because of the quantity and sensitivity of health data available; including, intellectual property, big data and personal information held about UK citizens.
- Due to a more adversarial geopolitical environment including the ongoing war in Ukraine, the rise of state-aligned groups from around the globe, and an observed rise in more aggressive cyber activity, it is highly likely that the cyber threat to the UK Critical National Infrastructure (CNI) has increased in the last year.

The NCSC Annual Review [2024](#), is linked in the [References](#) Section, below.

## Challenges

As detailed in the Cyber Security Strategy for Health and Social Care 2023 – 2030, the main challenges below are experienced by the UK NHS:

### High operational pressures

In a sector with varying working environments, high operational demand with many systems required to run 24/7, it can be challenging to prioritise finite resources to address competing risks, priorities and pressures. This challenge has been exacerbated by the unprecedented pressures placed on healthcare systems by the COVID-19 pandemic. We must ensure that organisations have the necessary insights and understanding to appropriately dedicate the right types of funding at the right time to cyber security, acknowledging the competing priorities and challenging work environments.

### **Large, complex and autonomous sector**

The size and diversity of the sector makes it challenging to set standards that can apply to all, which is a critical issue where sensitive and personal data is being shared across organisations. Some parts, such as primary, community and adult social care, face distinctions which require a balanced approach. We must account for specific requirements and varying cyber capabilities while defending as one.

### **Supply chain vulnerabilities**

The health and social care supply chain is complex as providers each use multiple suppliers. These suppliers in turn have their own supply chains, creating multiple layers of risk. This complexity makes it challenging to assure against supply chain risk, where our central visibility has less coverage, and where there is likely wide variance in cyber maturity. We must work with colleagues in procurement and supply chain to ensure that suppliers meet our cyber security standards.

### **Unclear accountability and ability to influence**

Where accountability for cyber risk is unclear, health and social care leaders may find it challenging to dedicate time and resources to their organisation's cyber security. We must be clear on the accountability that boards and leaders have for their organisations' cyber security and the responsibility that cyber professionals have for delivering in this space.

### **Limited cyber workforce**

A UK-wide shortfall of cyber professionals makes it challenging to hire and retain the experts we need to support leaders and staff in improving their organisations' cyber security. A comprehensive hiring, training and retention plan will be crucial to increasing the cyber workforce across health and social care.

### **New digital, data and technology**

The pace of growth and development in the digital, data and technology space makes it challenging to assure new products' cyber security. Standards-based practices and architectures that can accommodate new technologies will enable the sector to safely benefit from new and developing technology.

### **Legacy technology**

As new technology is developed, it can be challenging to monitor and replace older technology as it becomes outdated and more vulnerable to cyber attacks. We must ensure that such a large, busy

and diverse sector is able to keep ahead of outdated technology by promoting practices and architectures that support redundancy, maintenance and replacement of individual parts. This approach should be seen as an investment, rather than a cost, to assure technology can be used more safely and securely.

## External Factors

There are some factors that are ‘out of our hands’, uncontrollable aspects that may affect the risks the organisation maintains, this strategy ensures we are prepared for these and can be reactive to those changes.

These are grouped and outlined as the acronym **PESTLE**:

- Political
- Economic
- Social
- Technological
- Legal and Environmental

Below outlines the areas we believe may present a prevalent risk to the successful execution and outcome of this strategy:

Table 1

Factor / Issue / Risk	Group (PESTLE)
The change of Labour Government in July 24, may have delayed projects and programmes, during the period of transition. Across the wider Public Sector there have been funding cuts announced in the Autumn Financial Budget.	Political
ICB's and ICS's were expecting financial contributions from NHS England, to support with the delivery of their Cyber Security Strategies. This funding was not released, as at October 24. Further central initiatives may be impacted, as a result of the change in Government (see above).	Economic
NHS are competing with a global market demand for digital skills, in particular cyber security. This may result in the UK Public Sector not being able to find, develop and retain cyber resources, to successfully deliver the outcomes in this strategy.	Economic
The NHS is an easy target from foreign nation states, organised crime and other malicious threat actors. A significant cyber event, which results in an outage or data breach, may significantly reduce the ability to fund the execution of the cyber security strategy, within planned timescales.	Legal and Environmental
Deep rooted longer-term contracts, with key suppliers, may make it difficult for the some Trusts to adapt quickly to constantly evolving requirements and needs.	Legal and Environmental
Some Trusts are made up of internal teams, which may make it easier to influence / access investment in Digital, IT and Cyber	Economic

OFFICIAL-SENSITIVE

<p>Programmes. Where Trusts do not have this capability / influence (particularly Mental Health), it may delay their ability to define their requirements and ascertain funding.</p>	
<p>Modernising IT systems and ensuring cybersecurity are vital. The NHS must invest in technology to improve patient care, data management, and operational efficiency while protecting against cyber threats. This is difficult across a diverse range of legacy / current technology landscape.</p>	<p>Technical</p>
<p>Addressing the impacts of climate change and reducing the NHS's carbon footprint are crucial for long-term sustainability. This includes managing waste, reducing emissions, and preparing for the health impacts of climate change, which may take precedence over future cyber security programmes.</p>	<p>Social</p>
<p>Compliance with regulatory requirements and adapting to policy changes are ongoing challenges. The NHS must stay updated with regulations to avoid penalties and ensure high standards of care.</p>	<p>Legal and Environmental</p>

Final draft

## Learning from the Past – Previous Healthcare Incidents

Table 2

Incident	Type	Details
WannaCry (May 2017)	Ransomware	The WannaCry ransomware attack in May 2017 exploited a vulnerability in Microsoft Windows, affecting numerous organisations worldwide, with the NHS being one of the hardest hit. This cyberattack led to significant disruptions in healthcare services, including cancelled surgeries and appointments, as many NHS systems became inaccessible due to encrypted data, highlighting severe cybersecurity vulnerabilities within the organisation
Ireland Health Service Executive ransomware attack (May 2021)	Ransomware	Ireland's Health Service Executive was hit by a significant attack using Conti ransomware, that crippled its IT systems, causing 80% of the HSE IT environment to become encrypted, disrupting healthcare services nationwide. The attack led to delayed treatments, cancelled appointments, and a months-long recovery process
Advanced Systems – Third Party Software Services Provider (June 2022)	Ransomware	A sophisticated ransomware attack, took seven customers of Advanced Systems offline for months, in 2022. Advanced is a key supplier across the NHS, which resulted in patient check-in and medical notes services, resorting to pen and paper. The impact caused more than six months backlog, with hundreds of thousands of paper records, to rectify.
Dumfries and Galloway NHS (February 2024)	Data Breach	Involved the exfiltration approximately three terabytes of sensitive data by the group INC Ransom, which included personal health information of NHS staff and patients. The attackers threatened to release this stolen data on the dark web, raising significant concerns about privacy and data security within the NHS
Synnovis (June 2024)	Ransomware	A ransomware attack targeted Synnovis, a pathology service provider for NHS trusts in South East London, resulting in the postponement of over 10,000 outpatient appointments and 1,700 elective procedures at major hospitals like King's College Hospital. The attack caused significant disruptions to healthcare services, with many affected departments struggling to regain full functionality for weeks
Change Healthcare (February 2024)	Ransomware and Data Breach	Change Healthcare is a clearing house of payment and other information between thousands of healthcare organisations, processing 15 billion transactions p.a. The highly sensitive records of 190 million individuals were stolen. Provision of healthcare and pharmacy services were impacted for weeks across the US. A number of smaller providers went into bankruptcy as they were unable to be paid. There are hundreds of legal cases being developed against Change Healthcare. Change Healthcare estimates the costs of the attack will be in the order of \$3 billion

# Cyber Security Strategy

As detailed in the below sections, the ICS shall adopt a multi-outcome strategy, in order to comply with NIS regulations, NHSE requirements, and to build a resilient organisation, fit for the future. To summarise, the below outcomes will be achieved, as part of this strategy:

- **Outcome 1** - Adopt the [NHSE Five Cyber Security Strategy Pillars](#)
- **Outcome 2** - Assess compliance with the [NHSE Cyber Risk Investment](#) requirements, and develop a roadmap for investment and execution
- **Outcome 3** - Assess [Staff Awareness and Culture](#), using NHSE guidance and develop a roadmap to enhance
- **Outcome 4** - We will adopt [A Strategy to Adopt the CAF Aligned DSPT](#)

The following sections provide further details of what these include, and how we will achieve these outcomes.

## North West London ICS Core Organisational Objectives

As defined in the '[October 2024 North West London Board Meeting in Public](#)', the below core objectives are defined by the ICS:

1. Improve outcomes in population health and healthcare
2. Prevent ill health and tackle inequalities in outcomes, experience and access
3. Enhance productivity and value for money
4. Support broader economic and social development

This cyber security strategy directly supports each of the above objectives, as without an affective security posture, the ICS and Trusts cannot operate effectively and efficiently.

Board Assurance 25 September 2024

No	Risk Description	Risk Owner(s)	Responsible Committee(s)	Previous Risk Score (July 24)	Current Risk Score	Target	ICS/ICB
1	<b>ICB People</b> Failure to recruit, retain and develop the right people with the right skills	Director of People & OD	People & Rem Com Performance	16	20	12	ICB
2	<b>Collaboration and Engagement</b> Failure of the ICB to hear from, listen to, engage and influence our major stakeholders (residents; patients; staff and LA, NHS and third sector partners)	Director of Communications & Involvement	Strategic Commissioning Performance	12	12	8	ICB & ICS
3	<b>ICB Strategic Delivery</b> Failure to develop a prioritised, financially robust and deliverable ICB strategy and associated delivery plans that improve the health and wellbeing of NWL's residents and deliver our statutory duties	Director of Strategy & Population Health	Strategic Commissioning	12	16	8	ICB
4	<b>ICB and ICS Resilience</b> Failure to ensure we have the ability to respond appropriately, timeously and effectively to foreseeable major risks, events and potential disruptions (e.g. cyber/pandemic)	Chief Information Officer Chief Medical Officer Chief Financial Officer	Performance	16	16	12	ICB & ICS
5	<b>ICS Finance</b> We are unable to deliver the required levels of activity and quality within a recurrent cost base that ensures long term sustainability for all NWL ICB organisations to allow for the delivery of the NWL ICS strategy	Chief Financial Officer	Performance Contracting & Finance	20	20	10	ICS
6	<b>ICB Governance</b> Failure to ensure that the governance arrangements in place are fit for purpose and provide line of sight across the operating model	Chief Financial Officer	Audit & Risk	12	12	8	ICB
7 NEW	<b>ICS Performance and Quality</b> Failure to have effective oversight of ICS performance and quality	Chief Medical Officer Chief Nursing Officer	Performance	N/A	12	8	ICS

Figure 2

## Our Vision

Digital transformation is at the heart of NW London ICS's vision; and in alignment with the NW London ICS Digital and Data Strategy Vision, which is broken down through a series of seven steps, detailed in the graphic below:

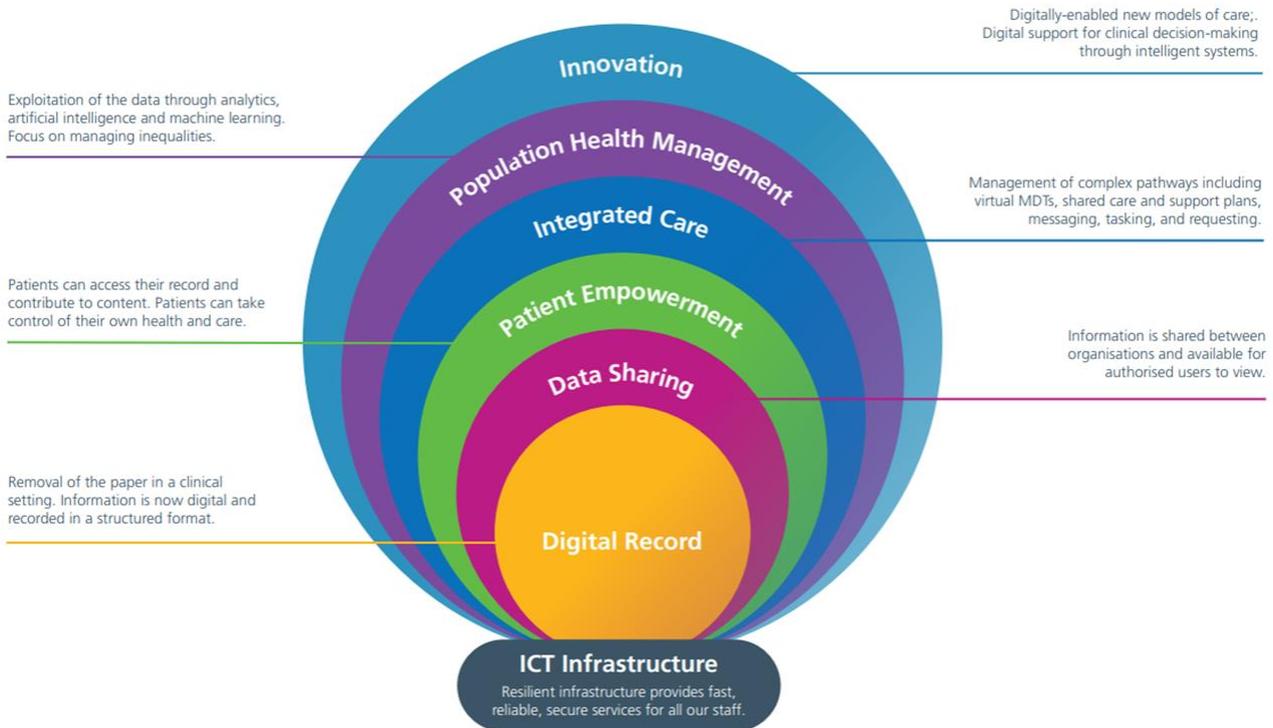


Figure 3 - NW London ICS Digital and Data Strategy – Vision

- **Infrastructure:** Staff will have seamless and reliable access to key clinical and business systems via a high-performing IT infrastructure that meets statutory and regulatory standards for security and information governance, while reducing infrastructure costs through system rationalisation and IT support services, and enabling ongoing productivity and efficiency improvements through corporate systems like Robotic Process Automation (RPA).
- **Digital Record:** Clinical systems will be consistent across care settings, enabling uniform workflows, access, and experience for staff and patients, with accurate patient information shared seamlessly between Primary Care, Community, and Mental Health systems to support integrated care. The single Oracle Health Cerner Electronic Patient Records (EPR) system across all 12 hospitals will be optimised for common pathways, and systems, processes, and staff skills will be continuously enhanced during and after implementation to ensure they are fit for purpose.
- **Data Sharing:** Shared records will support integrated care by securely and reliably informing care professionals of previous care activities and enabling digital care transfers, while the national Federated Data Platform, building on the local Care Co-ordination Solution (CCS), will bring together data from acute providers at ICS, regional, and national levels to ensure that data used for decision-making and measuring organisational performance more accurately reflects actual system activity.

- **Patient Empowerment:** People, along with their caregivers, will be able to access and manage their health and care information consistently through minimal apps, with the NHS App as a common interface, while also being able to input their own details into clinical systems (e.g., self-referrals and symptom tracking), and ensuring that those at risk of digital exclusion are supported with non-digital alternatives.
- **Integrated Care:** The national NHSE Federated Data Platform, building on our local CCS, will provide data to enable top-down management of demand, capacity, and patient flows across the ICB and Borough Based Partnerships, support clinical and service decision-making, and facilitate multi-disciplinary integrated care pathways spanning health and social care settings through shared digital care records, tasks, and plans.
- **Population Health Management:** Create a single, secure dataset of timely, granular health and care information as a "source of truth," fully leveraged for direct care, population health management, and identifying inequalities, while also being appropriately de-identified for research. This initiative will help organisations transform by making better use of Whole Systems Integrated Care (WSIC) and other available data tools, supported by a modern IT platform for storage and reporting, and aligned with the pan-London strategy for a sub-national Secure Data Environment.
- **Innovation:** Innovative technologies, such as learning systems and Artificial Intelligence (AI), will be regularly applied to support clinical decision-making, while digital innovations like ambient documentation will enable new, transformational models of care.

## Cyber Security Vision

Our vision is to identify and maintain the confidentiality, integrity, and availability of all NW London ICS healthcare data and systems proportionately, boost resilience, and protect from cyber incidents or unauthorised access in line with industry best practice and guidance.

Our vision is to support a transition to the Cyber Assessment Framework (CAF)-Aligned Data Security Protection Toolkit (DSPT), which is aligned to the NCSC Cyber Assessment Framework.

## Our Mission

Our Cyber Security Mission is to identify, manage, and report system cyber risk transparently to senior management and local member stakeholders ensuring they understand the underlying risk posture and can direct cyber risk appetite.

Strengthening and aligning governance across the ICS to ensure the ICB and all member organisations understand and discharge cyber roles, responsibilities, and activities in a joined up and systemic security function.

To lead and drive security culture improvements at a system level, supporting staff and patients in achieving good outcomes.

Embrace innovative technologies and collaboration across the ICS organisations and with external partners; leveraging support from the Cyber Associates Network (CAN), engagement with NHSE forums, and regional cyber workshops to deliver an enhanced cyber security posture. To ensure

reliable and secure delivery and retention of data in line with expectations and regulatory requirements and to exceed these where possible.

Preventing security incidents occurring and impact to systems, with the ability and experience to respond in a managed, measured, and proportionate way when they do; including exercising response and simulating realistic incidents and impacts.

## Strategy Governance

### Establishing Governance

By incorporating the below governance elements into the Cyber Security Strategy, we will ensure that objectives have appropriate support, momentum, and ownership, while also effectively managing and accounting for deliverables:

#### Strategy Governance Framework

**Senior Leadership Involvement:** Senior stakeholders, including the board and executive team, shall be actively involved in the development and oversight of the cybersecurity strategy through existing Digital and Data governance structures.

**Defined Roles and Responsibilities:** Clear lines of who is responsible for various aspects of the strategy shall be documented, ensuring there is accountability at all levels. Refer to Sections [Roles and Responsibilities](#) and [Outcome 1-4 RACI Appendices](#), below.

#### Documented Governance for Objectives

**Strategic Alignment:** Cyber security objectives shall align with the broader goals of the ICS. These can be discussed, agreed and documented, at the Section [Discussed and Approved at Board Level Meeting](#).

**Ownership and Accountability:** Specific objectives shall be assigned to senior stakeholders, making them responsible for the progression and success of these goals. Roles and responsibilities for this Strategy are defined at Section [Roles and Responsibilities](#) and Outcome [1-4 RACI Appendices](#), below.

**Regular Reviews and Updates:** Regular reviews shall be established, to assess progress of objectives and make necessary adjustments, maintaining momentum and relevance.

#### Governance for Deliverables

**Project / Programme Management:** Use of existing project and programme management approach and resources will direct and manage strategy deliverables.

**Performance Metrics:** Clear metrics to evaluate the effectiveness and impact of cybersecurity initiatives, shall be defined and agreed. Refer to Section [Board Reporting and Key Metrics](#).

**Risk Management:** Risk management processes shall be defined, to identify, assess, and mitigate cyber risks, ensuring continuous alignment with the strategy. Refer to Section [Board Reporting and Key Metrics](#).

**Effective Communication**

**Transparent Reporting:** Regularly communications shall be established, to highlight progress, challenges, and successes to all stakeholders, fostering an environment of transparency.

**Awareness and Training:** Provide ongoing cybersecurity awareness and training for all employees, ensuring organisational preparedness and resilience. A communications resource shall be included (refer to [Roles and Responsibilities](#)), for this to be successful. NHSE have provided guidance on questions, to gauge the cyber culture, which are documented at Section [Staff Awareness and Culture](#).

**Strategy Sign Off**

NHS England issued a guidance document for development, authorisation and submission of the ICB Cyber Security Strategy which set out key milestones below.

Table 3

Milestones	Date	Description
Initial draft	30 September 2024	A copy of this draft should be submitted to your Regional Security Lead (RSL) and confirmation provided that the strategy is on track for completion within these milestones
Final draft	18 December 2024	ICs will obtain assurances required for system-level approval and sign-off for the strategy as outlined in this guidance
Formal sign-off and submission of strategy by ICB Board as the statutory body	31 March 2026	Strategy to be fully approved and endorsed by the ICS. Information on protocol for submission to NHS England (NHSE) will be made available to ICs by RSLs.

NWL ICB submitted the draft Cyber Security Strategy to NHSE on Wednesday 18th December.

The work schedule part of the strategy will be reviewed again with ICT Cyber and Operational leads during 2025 to confirming their local plans for achieving the Year 1 target position following local business planning cycle outcomes.

During 2025 (February, March and April), the Cyber Security Strategy will be submitted for approval to:

OFFICIAL-SENSITIVE

- **The Board in Common:** For approval on behalf of Central London Community Healthcare NHS Trust (CLCH), Central and North West London NHS Foundation Trust (CNWL), Central and North West London NHS Foundation Trust (CNWL)
- **The Acute Provider Collaborative Board:** For approval on behalf of Imperial College Healthcare NHS Trust, Chelsea and Westminster Hospital NHS Foundation Trust, London North West University Healthcare NHS Trust, The Hillingdon Hospitals NHS Foundation Trust
- **ICS Digital Transformation Board:** On behalf of The Integrated Care Board, which is responsible for systems (including cyber security) in 360 GP Practices, 44 Primary Care Networks and also in its own head office and programme teams.

Final draft

## Board Reporting and Key Metrics

To support the overarching Governance and routine monitoring of the Cyber Security Strategy, the below KPIs have been identified, which should be highlighted and documented at the formal Cyber Security Governance Meetings, identified at the [Governance](#) Section. The below KPIs are recommended to be reported, on a regular basis:

Table 4

Key Performance Indicator	Description	Who (Reporter / Recipient)	Frequency	Related Outcome (1 – 4)
Cyber Security Risk Reporting	At the organisational level, report on the number of Business as Usual (BAU) Cyber Security Risks (Inherent and Residual) and their Risk Rating	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 1)
Strategy Risks Reporting	From Section 'Strategy Risk Management' – Report to the Governance Board where any Risks, which may affect the execution of the strategy, have been realised	Organisation Security Lead ----- NW London Cyber Security Governance Board	Monthly	Outcome 1 (Pillar 1)
Incident Management	At the organisational level, report on the number of incidents / data breaches, including their impact rating	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 1)
Vulnerability Management	At the organisational level, report on the security vulnerabilities, identified across the organisation, through security tooling or dedicated vulnerability scans. Include vulnerability impact level (CVSS score, or Defender score) Identify number of assets at End of Life (EoL) and End of Vendor Support (EoVS)	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 1)
Threat Management	Report, where possible: Threat Management initiatives - where Threat Intelligence, has been qualified and the organisation has	Organisation Security Lead -----	Monthly	Outcome 1 (Pillar 1)

Key Performance Indicator	Description	Who (Reporter / Recipient)	Frequency	Related Outcome (1 – 4)
	conducted Threat Hunting activities against qualified Indicators of Compromise (IoC) / Threat Actors. Report where IoC's have / have not realised a real threat. Note – this activity may be provided by a Managed Detection Response service	Organisation Security Working Group (Exec Sponsor)		
Security Operations Centre (SOC) / Managed Detection and Response (MDR) Reporting	Where a SOC / MDR service is established, it is recommended that the below areas are reported on, to ensure good governance and monitoring: <ul style="list-style-type: none"> <li>• Security Incidents, and Severities</li> <li>• Number of incidents escalated</li> <li>• Mean Time to Detect (MTTD)</li> <li>• Analysts Mean Time to Assignment (MTTA)</li> <li>• Analysts Mean Time to Triage (MTTT)</li> <li>• Service Requests – Mean Time to Fulfilment (MTTF)</li> <li>• Performance against SLA's</li> <li>• Service Availability</li> </ul>	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 2)
Security Awareness and Culture	At the organisational level, report on the levels of compliance against Mandatory Security / Data Protection training. Note - Organisations shall report against their Target Appetite Levels (xx% target)	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 3)
Roles and Responsibilities	Report on whether the required roles, as listed at Section 'Resourcing the Strategy', have been filled. These roles are essential, to support the successful adoption and execution of the Security Strategy. Note – where the organisation has not met these roles, a Strategy Risk shall be raised (see Section 'Strategy Risk Management')	Organisation Security Lead ----- NW London Cyber Security Governance Board	Monthly	Outcome 1 (Pillar 3)

Key Performance Indicator	Description	Who (Reporter / Recipient)	Frequency	Related Outcome (1 – 4)
Third Party Suppliers	Report on: <ul style="list-style-type: none"> <li>Number of Key Suppliers within the organisation</li> <li>Number of Key Suppliers which have undergone Third Party Supplier Due Diligence (within documented timescales – i.e. per annum)</li> </ul>	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 4)
Secure by Design	Report on: <ul style="list-style-type: none"> <li>Number of projects / programmes, applicable for Secure by Design process</li> <li>Number of projects which have completed / undertaking Secure by Design process</li> </ul>	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 4)
Security Policies and Standards	Report on: <ul style="list-style-type: none"> <li>Security Policies and Standards available and published</li> <li>Policies and Standards are current within their review / update cycle (have not expired)</li> </ul>	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Monthly	Outcome 1 (Pillar 4)
Cyber Resilience Planning and Testing	Report on: <ul style="list-style-type: none"> <li>Business Continuity Plan Published (per organisation)</li> <li>Business Continuity Test Plan published (includes planned Cyber Incident Simulation Tests / Exercise)</li> <li>Business Continuity / Cyber Incident Tests completed, against the plan (successful / not successful)</li> <li>Cyber Incident Response Plan Documented and Published</li> </ul> <p>Note – by not having the above documented and published, a formal risk shall be raised, as defied at Section ‘Strategy Risk Management’.</p>	Organisation Security Lead ----- Organisation Security Working Group (Exec Sponsor)	Quarterly	Outcome 1 (Pillar 5)

Key Performance Indicator	Description	Who (Reporter / Recipient)	Frequency	Related Outcome (1 – 4)
Cyber Risk Investment Foundational Priorities	<p>Report at the organisational level, on whether the below Foundation Priorities are in place:</p> <ul style="list-style-type: none"> <li>• Identity and Access Management (including PAM)</li> <li>• Multi Factor Authentication</li> <li>• Malware Detection</li> <li>• Perimeter Protection</li> <li>• SIEM</li> <li>• Vulnerability Management</li> <li>• Backups</li> </ul> <p>Note – Refer to the Strategy Outcome 2 – NHSE Cyber Risk Investment Assessment Tool</p> <p>Note – RAG Status:</p> <ul style="list-style-type: none"> <li>• Red – Not available and no plan to remediate</li> <li>• Amber – Not available, but plan / funding available to remediate</li> <li>• Green – Available / funded / resourced</li> </ul>	<p>Organisation Security Lead ----- NW London Cyber Security Governance Board</p>	Monthly	Outcome 2
Staff Awareness and Culture	<p>Report on:</p> <ul style="list-style-type: none"> <li>• Staff Awareness Survey (see Section ‘Outcome 3 – Staff Awareness and Culture’) has been distributed across organisation</li> <li>• Returns Received</li> <li>• Corrective Action / Improvement Plan established</li> </ul>	<p>Organisation Security Lead ----- NW London Cyber Security Governance Board</p>	Monthly	Outcome 3
CAF-aligned DSPT	<p>At an organisational level, report on:</p> <ul style="list-style-type: none"> <li>• Number of Essential Functions / Services Identified</li> <li>• Independent Assessor Assigned</li> <li>• December 24 - Baseline Assessments – Started / Scoped / Not Started</li> </ul>	<p>Organisation Security Lead ----- NW London Cyber Security Governance Board</p>	Monthly	Outcome 4

Key Performance Indicator	Description	Who (Reporter / Recipient)	Frequency	Related Outcome (1 – 4)
	<ul style="list-style-type: none"> <li>• January – May 25 – Independent Assessments initiated – Started / Scoped / Not Started</li> <li>• 30 June 25 – Self Assessment Submitted – Yes / No</li> <li>• Self-Assessment - Passed / Failed</li> </ul> <p>Note – this only applies to Category 1 Organisation (see Section ‘NHS Category Organisation Types’)</p>			

## Strategy Risk Management

Risks identified and captured at this section, may affect the successful adoption and implementation of the Cyber Security Strategy.

Once a risk has been identified, it is important to consider whether it falls within the agreed risk appetite for the Trust. However, as the Cyber Strategy is managed at the ICS level, the ICS may have a direct input into appetite and wider risk remediation activities.

As part of this process, the risk's basic causes are considered and the impact and likelihood of it materialising are assessed in line with the requirements of the Trust risk Matrix.

After the level of risk is determined following the risk appetite levels, the most appropriate risk response must be agreed as outlined below:

- **Tolerate:** if the risk falls within Trust risk appetite levels, there is usually no need for further action and the risk can be tolerated as it is.
- **Treat:** when a risk is outside the Trust risk appetite, a number of mitigations should be implemented to bring the risk to a tolerable level.
- **Transfer:** there are certain risks that the organisation decides to transfer to a third body. This usually occurs through insurance or external resourcing and it often applies to part of the risk.
- **Terminate:** if the impact of the risk on organisational objectives and core services is too high, and it goes well outside the risk appetite and tolerance boundaries set by the Board, consideration should be given to terminating the activity that causes the risk.

### Risk Appetite Levels

For the purpose of the ICS Cyber Strategy, there are three main levels to describe its risk appetite to correspond with the definitions used in the 'Risk Appetite for NHS Organisations' by the Good Governance Institute. The description of these levels are:

Table 5

Risk Appetite Level		Description
<b>Avoid/ Minimal</b>	<b>Low</b>	Strives to avoid risk and uncertainty. Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential
<b>ALARP (As little as reasonably possible)</b>		Works to minimise unavoidable risk.
<b>Cautious</b>	<b>Medium</b>	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
<b>Open</b>		Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)

Risk Appetite Level		Description
<b>Seek/ Mature</b>	<b>High</b>	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk). Confident in accepting or setting high levels of risk because controls, forward scanning and responsiveness systems are robust.

The below statements are a reflection of the organisations current position in relation to its primary risks:

Table 6

Risk Area	Risk Appetite	Target Risk Score	Risk Response
<b>Patient Safety</b>	Low Avoid / Minimal	4 – 6	Treat – Changing the likelihood
<b>Operational Performance</b>	Medium (Cautious)	8 – 12	Treat – Changing the likelihood
<b>Data Quality</b>	Low (ALARP)	6 – 9	Treat – Changing the likelihood
<b>Regulatory Compliance and Compliance With Other Standards Set by Regulators</b>	Low (Avoid / Minimal)	4 – 8	Treat – Changing the likelihood
<b>Data Security and Protection (Confidentiality, Integrity and Availability)</b>	Low (ALARP)	8 – 12	Treat – Changing the likelihood
<b>Finance</b>	Medium (Cautious)	8 – 12	Treat – Changing the likelihood
<b>Legal Compliance and Operational Impact</b>	Low (ALARP)	6 – 9	Treat – Changing the likelihood
<b>Reputational</b>	Low (ALARP)	6 – 9	Treat – Changing the likelihood
<b>Innovation</b>	Medium (Open)	8 – 12	Tolerate – Or increasing the risk in order to pursue an opportunity
<b>Research</b>	High (Mature)	8 – 12	Tolerate – Or increasing the risk in order to pursue an opportunity
<b>Workforce Safety and Wellbeing</b>	Low (Avoid / Minimal)	6 – 9	Treat – Changing the likelihood
<b>Sustainable Workforce</b>	Medium (Open)	6 – 9	Treat – Changing the likelihood
<b>Estates</b>	Low (ALARP)	12 – 15	Treat – Changing the likelihood

Risk Area	Risk Appetite	Target Risk Score	Risk Response
Redevelopment	High (Mature)	8 – 12	Tolerate – Or increasing the risk in order to pursue an opportunity
New Patient Pathways	Medium (Open)	6 – 9	Tolerate – Or increasing the risk in order to pursue an opportunity

### Risk Scoring – Likelihood and Consequences

Risk registers are used to document the risks identified; level of severity and probability, ownership and mitigation measures for each risk. Risks must be entered onto the Trust's risk management system by anyone who has completed the Trust's Risk Management e-learning module and has the agreed permission in accordance with the locally agreed governance arrangements for their area.

Risks level of severity and probability will be scored using a local 5x5 risk matrix, assessing the likelihood and consequence of each risk.

Whilst taking into consideration the trust risk appetite level, risks will be scored as below:

Table 7

		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequence	5 Catastrophic	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	4	6	8	10
	1 Negligible	1	2	3	4	5

$$\text{Risk Scoring} = \text{Consequence} \times \text{Likelihood} (C \times L)$$

**Definition of Likelihood:**

The below table can be used to determine the Likelihood score:

Table 8

Descriptor	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost Certain
<b>Frequency: How often might it / does it happen</b>	This will probably never happen / recur. Not expected to occur for years	Do not expect it to happen / recur but it is possible it may do so; at least annually	Might happen or recur at least monthly	Expected to happen / recur but it is not a persisting issue	Will undoubtedly happen / recur, possibly daily
<b>Probability: Will it happen or not?</b>	≤ 4%	5-19%	20-59%	60 - 89%	>90%

**Definition of Consequence:**

The below table can be used to determine the Consequence score:

Table 9

Descriptor	1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
<b>Impact on the Safety of Patients</b>	Minimal injury requiring no / minimal intervention or treatment.	Minor injury or illness, requiring minor intervention. Increase in length of hospital stay by 1 - 3 days Recognised (consented) complication of a procedure	Moderate injury requiring professional intervention Increase in length of hospital stay by 4 - 15 days. An event which impacts on multiple patients	Major injury leading to long-term incapacity / disability Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects An event which has a serious impact on multiple patients	Incident leading to death Multiple permanent injuries or irreversible health effects. An event which has a serious impact on a large number of patients.

Descriptor	1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
<b>Impact on the Safety and Wellbeing of Staff</b>	No time off work.	Requiring time off work for ≤3 days	Requiring time off work for 4 - 14 days.	Major injury leading to long-term incapacity / disability	Incident leading to death
<b>Quality / Audit</b>	Assessment of compliance against Trust priority audits or NICE guidance failing to meet relevant internal timescales Delayed response to NICE guidance	National audit submissions failing to meet relevant timescales Single failure to meet internal standards. Minor implications for patient safety if unresolved.	Repeated failure to meet internal standards.	Non-compliance with national standards with significant risk to patients if unresolved. Major patient safety implications if findings are not acted upon.	Critical report as a result of national audit Gross failure of patient safety if findings not acted upon.
<b>Human Resources / Organisational Development / Staffing / Competence</b>	Short-term staffing level that temporarily reduces the service quality (<1 day)	Low staffing level that reduces the service quality	Late delivery of key objective / service due to lack of staff. Unsafe staffing level or competence (>1 day). Low staff morale. Poor staff attendance for mandatory / key training	Uncertain delivery of key objective / service due to lack of staff. Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale, impacting on productivity and turnover. High level of agency staff use. No staff attending mandatory / key training. Limited capacity to develop people, impacting turnover	Non delivery of key objective / service due to lack of staff. Ongoing unsafe staffing levels or competence. Loss of several key staff. High level of agency staff use. No staff attending mandatory / key training on an ongoing basis. Limited capacity to develop people, impacting on turnover.
<b>Statutory Duty / Inspections</b>	No breach of statutory duty or regulatory requirement Regulator provides only guidance for improving; no action is set for the Trust to take	Breach of statutory duty or regulatory requirement is minimal / minor Action set by the regulator for the Trust to take is minimal / minor	Breach of a statutory duty or regulatory requirement which is moderate to serious. Regulator issues a requirement notice to the Trust for action to be taken	Multiple breaches of statutory duties or regulatory requirements which are each moderate to serious. Regulator issues a requirement notice or	Multiple breaches of statutory duties or regulatory requirements which are each Serious. Regulator takes civil enforcement action

Descriptor	1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
	Performance rating is not adversely impacted	Performance rating is not adversely impacted	Performance rating is adversely impacted	takes civil enforcement action against the Trust Performance rating is adversely impacted Critical inspection report published	against the Trust, which may include restriction, suspension or closure of a service, or placement of the Trust in Special Measures Regulator takes criminal enforcement action against the Trust, i.e. financial penalty or prosecution Performance rating is Inadequate Severely critical inspection report published
<b>Adverse Reputation to Organisation / Loss of Trust</b>	Rumours in circulation Social media comments	Local media inquiries / low level coverage Local councillors inquiries Potential for public concern - – Trust response manages the issue	Local media coverage / several outlets MPs inquiries to the Trust Short term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation MPs questions / statements in Parliament Request to attend local council scrutiny committee NHSE/I involvement Medium term reduction in public confidence	National media coverage with >3 days service well below reasonable public expectation DHSC involvement Government statement in Parliament Long term loss of public confidence
<b>Finance</b>	Small loss risk of claim remote	Loss of 0.1 - 0.5% of budget	Loss of 0.5% - 2% of budget	Uncertain delivery of key objective / loss of 2% - 5% of budget	Increase in cost, loss of income or non-delivery of objectives which is $\geq 5\%$ of budget
<b>Service Interruption (which focusses on IT systems)</b>	Loss of a minor system for 1 day	Loss of a major system for over 1 hour.	Loss of a major system for 1 > 3 days.	Loss of a major system for 3 days to a week	Loss of a major system for > 1 week.

Descriptor	1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
<b>Information Security (impact on Confidentiality, Integrity or Availability)</b>	Loss of confidentiality has minimal effect on the organisation or patient care: <10 patient records or sensitive data, such as passwords are compromised, or <10 patient records are maliciously modified, or <10 patients records become inaccessible	Loss of confidentiality has minor effect on the organisation, or patient care: >10 - 1000 patient records or sensitive data, such as passwords are compromised, or >10 - 100 patient records are maliciously modified, or >10 - 1000 patients records become inaccessible	Loss of confidentiality has moderate effect on the organisation or patient care: >1000 – 10000 patient records or sensitive data, such as passwords, are compromised, or >100 – 1000 patient records are maliciously modified, or >1000 – 5000 patients records become inaccessible	Loss of confidentiality has serious effect on the organisation, or patient care: >10000 – 100000 patient records, or sensitive data, such as passwords, are compromised, or >1000 – 10000 patient records are maliciously modified, or >5000 – 10000 patients records become inaccessible	Loss of confidentiality, impact on integrity and availability are severe: Records are greater than those stated left

## Cyber Security Strategy Risks

Table 10

ID	Title	Risk Description	Likelihood	Consequence	Risk Score
SR-1	Strategy Resourcing	<p>In the event that the Trust cannot fulfil the roles defined at Section 'Resourcing the Strategy', it is unlikely that the strategy will be successfully deployed and implemented. These roles have also been called out by NHSE, as fundamental, to support the adoption of the new CAF-aligned DSPT.</p> <p>Without the specialist capabilities, it is unlikely that the organisation will have an awareness of their cyber threats, issues and weaknesses, or will be able to scope, finance or implement the Outcomes of this strategy. This, will ultimately lead to inappropriate cyber measures and controls being in place, to deal with current / evolving threats.</p> <p><b>Target Appetite Risk Score = 6 – 9</b></p>	4 - Likely	4 - Major	16  Treat – Changing the likelihood
SR-2	Funding the Cyber Security Strategy	<p>In the event that the ICS and individual Trusts do not secure and receive appropriate funding, to execute on the multi-year cyber security strategy, it will lead to inappropriate cyber measures and controls being in place, to deal with evolving threats.</p> <p>Cyber Risk Investment is being provided by NHSE, which shall be consumed by March 25. Failure to identify the investment requirements, and draw-down funding this FY, may lead to funding not being made available, and alternative funding of the strategy will be required.</p> <p><b>Target Appetite Risk Score = 8 - 12</b></p>	5 - Almost Certain	4 - Major	20  Treat – Changing the likelihood
SR-3	Board / Executive Sponsorship	<p>In order to commission the cyber security strategy, Board / Executive Level Approval is required, at a formal Board Level Meeting.</p> <p>It is essential that Board Level representatives across the ICS and Trusts are actively engaged in the Cyber Security Strategy, and appropriate Governance is established, to monitor adherence to the Outcomes and roadmap.</p> <p>Governance has been defined at the 'Governance' section of this document.</p>	4 – Major	4 - Major	16  Treat – Changing the likelihood

ID	Title	Risk Description	Likelihood	Consequence	Risk Score
		<p>Lack of senior level involvement, will likely result in the outcomes, investment and deadlines being successful.</p> <p><b>Target Appetite Risk Score = 8 - 12</b></p>			
SR-4	Third Party Support	<p>In the event that key third parties are not notified and engaged, in supporting the execution of the strategy, that timescales will not be met.</p> <p>This risk may be amplified, across the ICS, as each trust will have a separate reliance on Third Party Support.</p> <p>Examples where third party support is required, includes:</p> <ul style="list-style-type: none"> <li>• Independent Auditors (for assessing the CAF-aligned DSPT by June 25)</li> <li>• NHSE (funding, guidance and DSPT submission)</li> <li>• IT systems providers</li> </ul> <p>Recent guidance from NHSE has determined that Category 2 suppliers (such as IT providers / operators of essential services) do not need to complete the new CAF-aligned DSPT (version 7), but will continue to complete V6 DSPT. This may result in IT service providers not adapting systems and processes, to support the Trust in achieving the new requirements, including within the CAF-aligned DSPT, by the June 25 deadline.</p> <p>Further delays from NHSE, releasing funding, to support the Cyber Risk Investment and Cyber Security Strategy, will undoubtedly prohibit the ICS from executing the outcomes, detailed in this strategy.</p> <p><b>Target Appetite Risk Score = 8 - 12</b></p>	4 – Major	4 - Major	16 Treat – Changing the likelihood
SR-5	Managing the Supply Chain and Third Party Provider Risk and Assurance	<p>Failure to identify Key Third Party Suppliers, can expose the organisation to various risks, including:</p> <ul style="list-style-type: none"> <li>• Inability to understand which key third parties play a pivotal role in the management, and compliance of operating Essential Functions, which are within scope of the CAF-aligned DSPT. Therefore, being unable to document the required artefacts, to evidence compliance, or maintain appropriate measures on critical systems.</li> </ul>	4 – Major	4 – Major	16 Treat – Changing the likelihood

ID	Title	Risk Description	Likelihood	Consequence	Risk Score
		<ul style="list-style-type: none"> <li>If key suppliers are not known/documented, then it is not possible for the organisation to conduct appropriate Third Party Supplier Due Diligence. Failure to do so may leave the organisation vulnerable to threats (Supply Chain is identified as the number one threat to UK, by the NCSC), as well as meeting Regulatory requirements (GDPR / UK DPA), and requirements outlined in the NIS and CAF-aligned DSPT.</li> </ul> <p><b>Target Appetite Risk Score = 4 - 8</b></p>			
SR-6	<b>Staff Awareness and Culture</b>	<p>Staff Awareness and Culture within Cyber Security, is fundamental for the organisation to function securely.</p> <p>Staff Awareness, has been specifically documented in Outcome 1 (Pillar 3), Outcome 3 (NHSE culture assessment) and Outcome 4 (CAF-aligned DSPT).</p> <p>This highlights the importance of assessing the current levels of Cyber Awareness Maturity, across the organisation, and producing an appropriate programme to improve.</p> <p>Regulatory requirements, such as GDPR / DPA18, expect to see staff mandatory annual cyber security and data protection training levels at ~95% compliance.</p> <p><b>Target Appetite Risk Score = 4 - 8</b></p>	<b>3 – Possible</b>	<b>4 – Major</b>	<p><b>12</b></p> <p><b>Treat – Changing the likelihood</b></p>

Where the below risks materialise, the risk can be extracted from the strategy document and captured within the organisation Risk Register. Any identified risks, should be escalated at the formal Cyber Security Governance Meetings, and outcomes / remediations agreed and documented.

## Strategy Outcome 1 - Cyber Security Strategy Pillars

As referenced in the DHSC Policy Paper, "A Cyber Resilient Health and Adult Social Care System in England: Cyber Security Strategy to 2030," introduces five collaboratively developed pillars to guide organisations toward a cyber-resilient health and social care sector. These pillars provide a framework for prioritising long-term cyber security improvements.

A national implementation plan will support these pillars, detailing activities and metrics to build resilience over the next 2–3 years. This plan, based on current assumptions about cyber security threats to 2030, will be kept under review and updated every 2-3 years, to enable us to address a range of future scenarios. A complementary roadmap will outline priority services and resources through 2030. The five pillars are as follows:

### Pillar 1 - Focus on the Greatest Risks and Harms

The health and social care system is vital for public wellbeing, with certain organisations, assets, and services critical to avoid significant harm from disruptions. The health sector is designated as requiring high security for its network and information systems, governed by the NIS Regulations to ensure essential services have adequate cyber protections. NHS trusts, foundation trusts, ICBs, and specific independent providers in England are designated as operators of essential services (OESs).

### Desired Outcome for pillar 1 by 2030

By 2030, the health sector aims to establish a shared understanding of varying risks, enhance visibility of the attack surface, and implement cybersecurity measures proportionate to threats and potential harm. NIS regulatory powers will be clearly understood and applied appropriately to mitigate cyber risks and strengthen resilience.

### How This Will be Achieved

To achieve this, the regional cyber security teams will:

Regional cybersecurity teams will establish a common language for assessing cyber risks, leverage national data to create a system-wide threat picture, and define proportionate mitigations for key risks. They will analyse the impact of cyber incidents on patients and services, regularly update standards to address evolving risks, and set clear minimum requirements for critical areas, aligned with NIS regulations and legislative changes. Additionally, they will review NIS implementation to ensure adequate coverage of essential services and use insights from regulatory actions to enhance overall resilience.

To achieve this, the ICS will:

Trusts should identify and document risks, including supplier cyber risks that could impact local system operations. They must engage in ICS-level risk mitigation plans, track investments, and monitor progress. Cyber risks should be integrated into broader corporate risk management, with providers maintaining oversight of suppliers' cybersecurity controls and vulnerabilities.

## **Pillar 2 - Defend as One**

The NHS has made strides in leveraging its scale, such as through the NHS England Cyber Security Operations Centre (CSOC) and sector-wide security technology deals. However, more must be done to capitalise on its size and interconnectedness to combat evolving cyber threats. This includes sharing knowledge to enhance skills, consolidating data to understand threats, and using NHS capabilities to improve resilience across the health and social care sector.

A more integrated approach is needed, with stronger national direction and centralised platforms to avoid silos, while allowing local organisations autonomy to implement strategies based on their needs. National teams should focus on enforcing impactful controls while delegating risk decisions to local leaders, enabling a tailored approach, including in adult social care.

### **Desired Outcome for pillar 2 by 2030**

Health and social care organisations collaborate on cyber security by sharing data, resources, and learning to strengthen sector-wide resilience. Threat intelligence and detection are nationally coordinated for swift response, while national teams set clear accountability expectations for leaders and boards regarding organisational risks and their wider sector implications. Leaders are encouraged to utilise available services to address the most significant risks and harms effectively.

### **How This Will be Achieved**

To achieve this, the regional cyber security teams will:

Define clear roles and responsibilities for cyber risk, foster collaboration across government, care, academia, and commercial partners, and offer centralised support for initiatives aligned with national priorities. Enhance NHS-wide cyber monitoring with automation where feasible, and establish a health technology assessment and remediation service.

To achieve this, the ICS will:

Develop an ICS-wide cyber security strategy with allocated funding and governance to review and align plans, ensuring involvement from all members and partners. The strategy should align with established cyber security standards for both existing and new cross-organisational systems.

## **Pillar 3 – People and Culture**

Managing cyber risk requires a collective effort across all organisations, with leaders ensuring staff are equipped with the skills and resources to address threats. A "just culture" of learning and collaboration is essential to foster ownership and continuous improvement. To achieve cyber resilience, we must increase the number and expertise of cyber professionals at all levels through hiring, training, and career pathways. Additionally, we need to offer cyber basics training for the broader workforce and senior leaders, ensuring they understand the relevance to patient and service user safety. Efforts to grow the cyber workforce will also extend to adult social care, while acknowledging its unique challenges.

### **Desired Outcome for pillar 3 by 2030**

Cyber security is recognised as a crucial profession in health and social care, with the NHS attracting and retaining a diverse workforce. A 'just culture' for cyber regulation is promoted across the system, ensuring that everyone understands their role in maintaining good cyber security and acts accordingly.

### **How This Will be Achieved**

To achieve this, the regional cyber security teams will:

Clearly define roles and responsibilities for managing cyber risk, emphasising its importance to patient and service user safety. Integrate cyber security into national and regional forums to foster a holistic culture. Implement a plan to grow the cyber workforce and establish career pathways across health and social care. Ensure accessible cyber basics training for all, while building a community of shared learning through platforms like the CAN and digital social care website. Lead by example in promoting a "just culture" at the national level when addressing cyber vulnerabilities.

To achieve this, the ICS will:

Develop a well-resourced and accountable cyber security function to manage risks, supported by ICS and organisational resources. Integrate cyber security decisions into multi-disciplinary forums to foster a holistic culture, with the ICP promoting collaboration, sharing best practices, and addressing gaps. Encourage cross-organisational cooperation, ensuring accountability for key priorities, and lead by example in adopting a 'just culture' to address cyber vulnerabilities at the ICS level.

### **Pillar 4 – Build Secure for the Future**

The health and social care system was not originally designed with cyber security in mind, contributing to many current vulnerabilities. As we develop future systems, we have the chance to integrate security into organisational structures and technologies from the outset, setting standards for emerging technologies and governance, such as in ICSs. Additionally, cyber security must be a key focus in the supply chain, from procurement to contract management, to ensure a more secure system overall.

### **Desired Outcome for pillar 4 by 2030**

Organisations must understand and manage emerging risks, ensuring resilience across the critical health and social care supply chain. New services, support, and standards should be secure by design, with clear, aligned standards underpinned by the CAF.

### **How This Will be Achieved**

To achieve this, the regional cyber security teams will:

Adapt flexibly to emerging threats by developing horizon-scanning functions and engaging with critical suppliers to ensure their cyber security. Improve communication with suppliers during cyber events and share guidelines for embedding security into contracts. Make the CAF the primary cyber standard in the DSPT, ensuring compliance through collaboration with the CQC and local government. Set minimum IT lifecycle management expectations and secure architecture patterns

while empowering organisations to tailor their cyber security to their needs within mandated standards. Engage with teams implementing new technologies to ensure security is prioritised and provide clarity on upcoming cyber guidance.

To achieve this, the ICS will:

Build systems and services with cyber security by design, ensuring supplier alignment with national standards. Regularly engage organisations on compliance with standards and frameworks, and develop a cyber security program that supports the strategy's objectives, with clear milestones and metrics.

### **Pillar 5 – Exemplary Response to Recovery**

Cyber-attacks are inevitable, and the health and social care system must be prepared to minimise their impact and recovery time. National teams, including the NHS England CSOC, should develop response capabilities and promote best practices across organisations. Regular cyber response exercises at all levels, coupled with lessons learned, will improve incident handling. Business continuity is key, ensuring that critical services can continue at an acceptable level during a cyber-attack, with leaders at all levels responsible for ensuring preparedness within their areas.

#### **Desired Outcome for pillar 5 by 2030**

National, regional and local responses to a cyber incident minimise the impact of a cyber-attack on patient and service user care.

#### **How This Will be Achieved**

To achieve this, the regional cyber security teams will:

Publish expectations for incident response and reporting, and lead national "dry run" exercises to develop and apply cyber attack response plans. Collaborate with the NCSC on managing technical responses to sector-wide attacks, and deploy Cyber Security Incident Response teams to support local organisations as needed. Investigate and report on lessons learned from cyber events, driving improvements and remediation. Develop national resilience by understanding the impact of critical system failures and agreeing on mitigations, while integrating cyber response into broader emergency preparedness and response planning.

To achieve this, the ICS will:

Outline the responsibilities of member organisations and a central accountable function for cyber response and recovery. Ensure the ICS and its members have a rehearsed plan for managing and recovering from a cyber attack. Engage with dry-run exercises and post-incident reviews to identify and address common themes, leading ICS-wide incident response drills. Develop ICS resilience by understanding the impact of critical system unavailability and agreeing on mitigations.

As part of the Cyber Security Strategy, we have mapped the pillar outcomes, within the NHS CAF and DSPT, at Section [Appendix A – DSPT / CAF – Strategic Outcomes](#).

## Outage Cost Modelling

In order to support the justification and execution of the Cyber Security Strategy, particularly Pillar 5 (of Outcome 1), it may be beneficial for key stakeholders, to calculate and document an outage cost model, to determine the true impact of not implementing the outcomes of the strategy. This exercise will allow each organisation to calculate the total cost / impact, in the event of a loss of key digital systems and processes, across their organisation.

Calculating the outage cost for an NHS organisation due to a loss of digital systems involves several steps. This involves financial impact assessment, operational assessment, risk management, and future mitigation strategies. Below outlines some recommended steps, which can be used, to capture an outage cost model:

- Define the Scope and Objectives:
  - Determine the specific systems and services that are critical for operations.
  - Clarify the timeframe for which the outage costs need to be assessed (e.g., per hour, day, or overall event).
- Identify Critical (Essential) Systems and Services:
  - Make a list of IT systems and digital services essential to clinical and administrative operations.
  - Include patient record systems, appointment scheduling, lab/specialist systems, etc.
- Assess Direct Costs, such as::
  - Staffing Costs: Calculate the cost of unproductive staff time during system downtime.
  - Overtime Costs: Account for overtime if extra hours are needed to catch up after the outage.
  - Alternative Resources: Cost of temporary solutions or manual processes put in place.
- Evaluate Indirect Costs:
  - Patient Impact: Estimate costs related to cancelled appointments, delayed treatments, and potential patient harm.
  - Litigation and Penalties: Consider potential legal consequences or regulatory fines.
  - Reputation Damage: Assess potential loss of future revenue due to damaged reputation.
- Assess Long-term Operational Impact:
  - Analyse the potential impact on patient throughput and service delivery capabilities.
  - Consider increased workload post-outage due to rescheduling and backlog.
- Conduct a Risk Assessment:
  - Identify vulnerabilities in current IT systems and processes.
  - Evaluate the probability of different types of outages and their potential impact.
- Estimate Recovery and Mitigation Costs:
  - Include costs for recovering systems, such as IT support, hardware replacement, and software reinstallation.
  - Consider investments in resilience, such as backup systems and disaster recovery plans.
- Implement a Contingency Plan:
  - Develop a plan for maintaining operations during outages, including manual backups and alternative communication methods.
  - Train staff on contingency workflows to minimise disruptions.

- Engage Stakeholders:
  - Work with clinical leadership, IT departments, finance teams, and external consultants to gather comprehensive data.
- Develop and Validate the Cost Model:
  - Use historical data and simulations to estimate prospective outages' financial and operational impact.
  - Validate the model by comparing it with similar previous incidents where possible.
- Report and Communicate Findings:
  - Create detailed reports that can be used for internal briefings and external communications.
  - Develop and execute a communication plan to inform relevant stakeholders quickly in case of an actual outage.
- Review and Update Periodically:
  - Regularly review the cost model and update it according to changes in technology, healthcare services, and organisational processes.

By following these steps, we can better understand potential financial losses from digital/IT outages and prioritise resilience measures to minimise disruption.

#### **Outcome 1 - Roles and Responsibilities**

A Roles and Responsibilities (RACI) Matrix is available at the following section - [Appendix F – Outcome 1 – Organisational RACI for adopting the Cyber Security Strategy Pillars](#)

#### **Outcome 1 - Timescales**

A full Gantt Chart against Outcome 1 initiatives, is available at - [Appendix J – Outcome 1 – Adopting the Cyber Security Strategy Pillars Gantt Chart](#).

## Strategy Outcome 2 - NHSE Cyber Risk Investment

To execute the cyber security strategy for health and social care to 2030, NHSE launched the Cyber Improvement Programme (CIP), which is a cyber-risk reduction investment across the NHS system. NHSE's CIP has allocated ICSs and ALBs cyber capital and revenue investment to strengthen their cyber security posture, and therefore reduce risk at a local level. The current CIP funding (applications submitted October 2024), is to be used by March 2025.

NHSE has provided guidance documents (Appendix C) to support NHS organisations in prioritising where the investment could be spent; to achieve the greatest cyber risk reduction.

A cyber risk quantification analysis was conducted by NHSE to identify which cyber defence capabilities will likely deliver the greatest quantifiable risk reduction for organisations, by reducing the likelihood and impact of cyber-attacks to the organisation. The methodology and approach for this analysis is set out in the aforementioned guides.

NHS organisations, including Trusts, ICBs and ALBs, have ultimate autonomy for capital and revenue investment decisions, with the guide recognising that every organisation has differing levels of cyber maturity and capability requirements.

A gap analysis tool was created by NW London ICS, '[NW London ICS Cyber Risk Investment – Assessment Tool](#)', and was shared with the organisations of the NW London ICS, week commencing 14<sup>th</sup> October 2024, to assess their current cyber maturity and cyber defence capabilities against the cyber capabilities outlined in 'Cyber Risk Investment Decision Making – Annex A' (Appendix C). This enabled organisations to determine their level of compliance and identify cyber capability areas for improvement/investment. The graphic below displays the overall ICS compliance against the foundational/cyber capabilities detailed in 'Cyber Risk Investment Decision Making – Annex A' (Appendix C).

The graphic below shows the overall ICS compliance responses against both the foundational, and other cyber capabilities

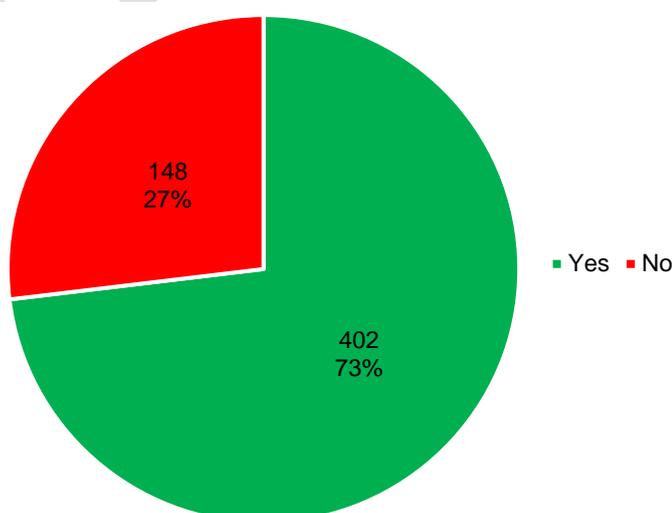


Figure 4 – Answer totals for the 'NW London ICS Cyber Risk Investment – Assessment'

The table below displays the current status for each ICS organisations' cyber capability and the associated Cyber Risk Reduction Funding request against the Foundational Priorities and cyber capabilities. Where any component of the foundational capability or other cyber capabilities were not met in the assessment tool, the whole capability is marked as not being met, for the purposes of this analysis.

- **Green** – Requirement met (from Assessment Tool returns)
- **Amber** – Requirement not met; funding requested through NHSE
- **Red** – Requirement not met; no funding requested/available/approved
-  - National services are provided and should be considered before an individual investment is undertake

Final draft

Table 11

	Organisation / Foundational Priority	Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	Identity and Access Management (Including Privileged Access Management)	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Multi-Factor Authentication (MFA)	Red	Yellow	Red	Red	Green	Green	Green	Green	Green
	Malware Detection	Green	Green	Green	Green	Green	Red	Red	Red	Red
	Perimeter Protection	Green	Green	Green	Green	Red	Green	Red	Red	Red
	Security Event Logging	Yellow	Red	Red	Red	Red	Green	Red	Red	Red
	Vulnerability Management	Yellow	Green	Green	Green	Red	Green	Red	Red	Red
	Backups	Red	Red	Red	Red	Red	Red	Green	Green	Red
	Third party secure remote access	Red	Green	Green	Green	Red	Red	Green	Green	Red
	Network segmentation	Red	Red	Red	Red	Red	Red	Yellow	Red	Red
	Domain Name System (DNS) traffic filtering	Green	Red	Red	Red	Green	Red	Green	Green	Green
	Secure endpoint configuration	Red	Green	Green	Green	Green	Green	Yellow	Green	Green
	Cyber Incident Management	Red	Red	Red	Red	Red	Red	Red	Red	Red

OFFICIAL-SENSITIVE

	Organisation / Foundational Priority	Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	Cyber Strategy & Governance	Green	Green	Green	Green	Red	Yellow	Green	Green	Green
	Cyber Risk Management	Green	Red	Red	Red	Red	Red	Yellow	Green	Green
	Scenario based technical exercising	Red	Red	Yellow	Yellow	Red	Red	Red	Red	Red
	Asset management	Yellow	Green	Green	Green	Green	Red	Green	Red	Red
	Business continuity & disaster recovery	Red	Green	Red	Red	Red	Red	Green	Red	Red
	Vulnerability scanning	Green	Red	Red	Green	Red	Yellow	Red	Red	Red

## ICS Cyber Risk Reduction Funding Applications

The following table displays a summary of the Capital and Revenue funding requests from the ICS organisations, submitted for FY24-25 on **17<sup>th</sup> October 2024**.

Table 12

Type	Organisation	Capability	
Capital	London North West University Hospitals NHS Trust	Malware Detection /Vulnerability Management	Acquisition and deployment of NISSUS Expert Deep Scanning – for endpoint scanning/network attached devices
Capital	London North West University Hospitals NHS Trust	Secure Endpoint Protection	Acquisition and deployment of ManageEngine Device Plus – endpoint port/configuration device control management
Capital	London North West University Hospitals NHS Trust	Secure Endpoint Protection	Acquisition and deployment of AppCheck – conduct penetration testing and detection on all network devices, OS, and web applications
Capital	The Hillingdon Hospitals NHS Foundation Trust	Malware Detection /Vulnerability Management	Acquisition and deployment of NISSUS Expert Deep Scanning – for endpoint scanning/network attached devices
Capital	The Hillingdon Hospitals NHS Foundation Trust	Secure Endpoint Protection	Acquisition and deployment of AppCheck – conduct penetration testing and detection on all network devices, OS, and web applications
Capital	Chelsea and Westminster Hospital NHS Foundation Trust	Strong Authentication (MFA), Privileged Access Management	Procure and implement new MFA and PAM solution for admin accounts; replacing current EoS PAM solution
Capital	London Ambulance Service NHS Trust	Privileged Access Management	Procure an additional 50 perpetual PAM licenses to onboard 3rd party suppliers on to Delinea; enabling zero trust for any suppliers required to connect to internal resources to provide support
Capital	Imperial College Healthcare NHS Trust	Asset Management	Acquisition and deployment of IHealth Assurance Dashboard to maintain an asset inventory which exceeds MDE capabilities and compliance with NHS England cyber alerts and high severity alerts (HSAs)
Capital	Imperial College Healthcare NHS Trust	Privileged Access Management	Acquisition and deployment of 'SpecOps Password Policy' to ensure AD password/passphrases are strong - banning words from custom dictionary lists (eg. London100) and known compromised passwords from being used
Revenue	London North West University Hospitals NHS Trust	Cyber Strategy & Governance	Purchase and implement Trustwide mandatory Cyber awareness Training 'Know2Be'; Additional Cyber Security Training for Staff who required enhanced knowledge as specified in DSPT / CAF

Type	Organisation	Capability	
Revenue	London North West University Hospitals NHS Trust	Scenario Based Technical Exercising	Conduct physical cyber security review – ‘Dionach Red Team’; Use of onsite scenario based exercises (e.g. purple teaming) to assess the effectiveness of technical security controls across the layers of defence
Revenue	The Hillingdon Hospitals NHS Foundation Trust	Cyber Strategy & Governance	Purchase and implement Trustwide mandatory Cyber awareness Training ‘Know2Be’; Additional Cyber Security Training for Staff who required enhanced knowledge as specified in DSPT / CAF
Revenue	The Hillingdon Hospitals NHS Foundation Trust	Scenario Based Technical Exercising	Conduct physical cyber security review – ‘Dionach Red Team’; Use of onsite scenario based exercises (e.g. purple teaming) to assess the effectiveness of technical security controls across the layers of defence
Revenue	West London NHS Trust	Privileged Access Management, Secure Endpoint Protection	Acquisition and deployment of ManageEngine Device Plus – endpoint port/configuration device control management to Manage active directory & users on a more consistent basis, including vulnerability management.
Revenue	West London NHS Trust	Vulnerability Scanning, Malware Detection, Vulnerability Management	Acquisition and deployment of NESSUS Expert Deep Scanning for vulnerability and malware detection
Revenue	West London NHS Trust	Cyber Strategy & Governance	Develop a Trust Cyber Security Strategy as a managed service through partner.
Revenue	West London NHS Trust	Vulnerability Scanning	DSPT View for audit, gap analysis and vulnerability identification
Revenue	London Ambulance Service NHS Trust	Cyber Risk Management	Creation and deployment of CIS Benchmark Level 1-compliant gold builds for Windows 10, Windows Server, and iOS. This includes configuration, testing for security and performance, deployment, detailed documentation, and a formal handover with training and support to the BAU team for ongoing maintenance.
Revenue	Imperial College Healthcare NHS Trust	Security Event Logging	Uplift current Splunk core license to Splunk Enterprise Security – enable correlation and enrichment of logs along with User and Entity Behaviour Analytics (UEBA)
Revenue	Imperial College Healthcare NHS Trust	Vulnerability Management	Implementation of Power BI and Automate capabilities with MDE Vulnerability management to create an automated notification directly to system owners/admins and tracking of vulnerabilities (eg. PHP/JRE). Vulnerability management to create an automated notification

Type	Organisation	Capability	
Revenue	Central London Community Healthcare NHS Trust	Privileged Access Management, Network Segmentation, Secure Endpoint Protection, Web Application Firewall (WAF)	Conduct Architecture review and improvement plan to align to best practice and Implement nationally funded NHSE tools (MDE, MS Defender, Secure Boundary)
Revenue	NHS North West London Procurement, hosted by Central London Community Healthcare NHS Trust	Cyber Strategy & Governance	Develop a Third Party Risk Management (TPRM) framework to enhance cyber resilience and mitigate risks across 13,000 suppliers for NHS North West London ICS. This includes delivering immediate risk controls, implementing a federated model across 7 Provider Trusts and the ICB, enhancing TPRM processes and technology for continuous monitoring, and aligning with regulations and the national NHSE supplier risk approach.
Revenue	NHS North West London Procurement, hosted by Central London Community Healthcare NHS Trust	Cyber Risk Management	Implement a Third Party Risk Management (TPRM) framework to strengthen cyber resilience and mitigate risks across 13,000 suppliers for NHS North West London ICS. Led by NWLPS, this involves scaling a federated model across 7 ICS Provider Trusts and the ICB, aligning resources, automating due diligence, and integrating global intelligence for continuous monitoring, all while adhering to UK, international, and NHSE standards.

**Outcome 2 - Roles and Responsibilities**

A Roles and Responsibilities (RACI) Matrix is available at the following section - [Appendix G – Outcome 2 – Organisational RACI for the NHSE Cyber Risk Investment](#).

**Outcome 2 - Timescales**

A full Gantt Chart against Outcome 2 initiatives, is available at - [Appendix K – Outcome 2 – NHSE Cyber Risk Investment Gantt Chart](#).

**Strategy Outcome 3 - Staff Awareness and Culture**

It is recommended, that as part of the cyber security strategy, each organisation conducts a staff awareness survey, to gauge staff understanding of data security. The results from the assessments will allow the Trusts/ICS to gauge general levels of cyber culture and awareness, and to generate a plan for future remediation.

The below timescales have been agreed (Cyber Security Strategy Workshop, dated 8 November 2024), as part of the Security Strategy, for Outcome 3:

- Issue the below NHSE Staff Awareness and Culture Questionnaire (17 questions), across the ICS and Trusts – **January 2025**
- Receive responses to NHSE Staff Awareness and Culture Questionnaire – **February 2025**
- Review feedback at ICS level, and develop a future Staff Awareness and Culture Improvement Plan – **March 2025**

2025 Q1		
[January]	[February]	[March]
Issue the NHSE Staff Awareness and Culture Questionnaire (17 questions), across the ICS and Trusts	Receive responses to NHSE Staff Awareness and Culture Questionnaire	Review feedback at ICS level, and develop a future Staff Awareness and Culture Improvement Plan feedback.

Figure 5

The following statements have been recommended by [NHSE](#), to be incorporated into training programmes, allowing personnel to “agree” or “disagree”. Not all statements are seeking an ‘agree’ response, however, it should support the organisation in identifying gaps or areas to focus future improvement:

Table 13

Question Number	Domain	Question
1	Leadership	I feel data security and protection are important for my organisation.
2	Policies	I know the rules about who I share data with and how.
3	Policies	I know who to ask questions about data security in my organisation.
4	Use of Data	I am happy data is used legally and securely in my organisation
5	Sharing data securely	I know how to use and transmit data securely.
6	Using data legally and securely	I feel that patient confidentiality is more important than sharing information for individual care.
7	Processes	The tools and processes used by my organisation make it easy to use and transmit data securely.
8	Raising concern	I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination.
9	Laws and principles	I understand the important laws and principles on data sharing, and when I should and should not share data.
10	Data sharing questions	If I have a question about sharing data lawfully and securely I know where to seek help.
11	Personal responsibility	I take personal responsibility for handling data securely.
12	Training	The data security training offered by my organisation supports me in understanding how to use data lawfully and securely.
13	Access to Information	The level of access I have to IT systems holding sensitive information, is appropriate.
14	Reporting	I know how to report a data security breach.
15	Incidents	When there is a data security incident my organisation works quickly to address it.
16	Learning Lessons	When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again.
17	Contingency Plan	If a data security incident was to prevent technology from working in my organisation, I know how to continue doing the critical parts of my job.

Once the assessment has been completed, each organisation shall discuss and agree a 'Staff Awareness and Culture' improvement plan, if deemed necessary.

### Outcome 3 - Roles and Responsibilities

A Roles and Responsibilities (RACI) Matrix is available at the following section - [Appendix H – Outcome 3 – Organisational RACI for Staff Awareness and Culture](#).

### Outcome 3 - Timescales

A full Gantt Chart against Outcome 3 initiatives, is available at - [Appendix L – Outcome 3 – Staff Awareness and Culture](#).

## Strategy Outcome 4 - A Strategy to Adopt the CAF-Aligned DSPT

### Overview of the new CAF-aligned DSPT – Independent Assessment Framework

The [Data Security and Protection Toolkit](#) (DSPT) changed in September 2024 for NHS Trusts (Acute, Foundation, Ambulance and Mental Health), ICBs, Commissioning Support Units, and Department of Health and Social Care (DHSC) ALB's (Category 1 Organisation Types), to align with the NCSC CAF. This was a commitment made in the DHSC cyber security strategy for Health and Social Care to 2030, to enhance the cyber security assurance of government organisations, which underpins the five pillars of the Strategy.

The CAF-aligned DSPT approach is geared towards using principles and expert judgment to guide competent decision-making, with a focus on achieving key outcomes. This new approach will affect the way that people, processes and technology are evaluated and assured in cyber security and information governance. This evaluation will be evidenced through indicators of good practice for each outcome, and will be required to meet expected achievement levels.

Cyber security plays a critical role in all sectors, but its importance is amplified in the healthcare industry, where sensitive patient data and even lives are at stake. In the NHS, a cyberattack could compromise confidential medical records, disrupt critical medical equipment, or even delay life-saving treatments. Information governance takes centre stage in the NHS as patients trust their health and care providers with sensitive information. A breach of information governance could lead to added stress for patients and staff alike, disrupting care and leading to a loss of trust.

The NHS CAF was developed by NHS Digital in alignment with the principles and structure of the NCSC CAF; previously deployed across Central Government and Defence. It aims to help NHS/Category 1 ([NHS Category Organisation Types](#)) organisations manage and assess cybersecurity risks by providing structured guidance across key areas such as risk management, data protection, incident response, and system resilience.

The CAF-aligned DSPT is specifically tailored to healthcare settings, ensuring that essential health services remain secure and operational in the face of cyber threats. The NHS CAF consists of five Objectives:

- **Objective A:** 'Managing Risk'
- **Objective B:** 'Protecting against cyber-attacks and data breaches'
- **Objective C:** 'Detecting cyber security events'
- **Objective D:** 'Minimising the impact of incidents'
- **Objective E:** 'Using and sharing information appropriately'

Large NHS organisations, including NHS Trusts, ICBs, ALBs, and Commissioning Support Units (CSUs) (Category 1 organisations), must complete the **DSPT against the CAF rather than the National Data Guardian's 10 data security standards**. All other organisations will continue to complete the Toolkit measured against the National Data Guardian's standards.

The DSPT 2024-2025 (version 7) standard, is applicable for NHS Trusts, ALBs, ICBs and CSUs until the DSPT deadline, 30 June 2025 - [DSPT Toolkit – CAF Summary Audit Guide v7 24-25 V1.0](#). Further guidance will be released by NHSE in November 2024, via the [DSPT News website](#).

For the June 2025 DSPT deadline, the requirement is only to establish a baseline with the initial submission; there is not a requirement for full compliance with the CAF at that point.

DHSC, as the competent authority for the health and care sector under the NIS Regulations, may access information from the CAF-aligned DSPT to fulfil its regulatory purpose.

### Goals of moving to the CAF-Aligned DSPT:



#### Enhanced Risk Management

Emphasise good decision-making over compliance, with better understanding and ownership of information risks at the local organisation level, where those risks can most effectively be managed.



#### Foster a Continuous Improvement Culture

Support a culture of evaluation and improvement, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes – and expend effort on what works, not what ticks a compliance box.



#### Improve Threat Management

Create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks.

### The Independent Assessment Framework

#### Benefits of the Independent Assessment Framework

The CAF-aligned DSPT harnesses a less prescriptive approach in the response to each outcome, and therefore warrants its own guidance to reflect the changes in the toolkit. This updated guidance is intended to provide the following benefits to Health and Social Care organisations, independent assessment providers, and the Health and Social Care system as a whole:

- **Health and Social Care organisations:** As the focus of DSPT shifts from verifying the implementation of specific controls mandated by evidence items, to assessing adherence to the desired outcomes under the CAF-aligned DSPT independent assessments, organisations will receive an opinion over the effectiveness of their control environments, to adhere to the specified outcomes. This would ultimately support them in identifying cyber security and information governance gaps between the organisation's self-assessment and the assessment result, that should be mitigated to improve the posture of the organisation. In addition, the increased insight that national bodies will have into the cyber security and information governance posture of multiple organisations across the sector will enable them to support individual organisations in improving their controls.
- **Independent assessment providers:** In recent times, independent assessment providers have been expected to provide an increased level of assurance, over a wider range of data security and protection controls (including more technical cyber-related controls introduced in the CAF-aligned DSPT). The guidance is not designed to replace the existing expertise, knowledge and professional judgement of independent assessment providers, but should instead support them in identifying how to effectively assess the organisation against the objectives of the CAF-aligned DSPT. It will also help inform the work of cyber security and information governance professionals that are new to the health and social care system, helping them to understand assessor's requirements to validate the posture of the organisation during the assessment.
- **National Bodies/Health and Social Care system:** When followed and widely used across the system, the CAF-aligned DSPT framework and guide should provide national bodies with greater insight into the effectiveness of Health and Social Care organisations' cyber security and information governance control environments, as well as their alignment to regulations such as NIS 2018. This will enable new national data security services and guidance to align to known areas of weakness and support shared learnings across the sector from examples of good practice, as well as provide additional support to organisations that may have issues in this area. DHSC, as the competent authority for the health and care sector under the NIS Regulations, may access information from the CAF-aligned DSPT to fulfil its regulatory purpose.

### What is the Independent Assurance Framework

The NHSE CAF-aligned DSPT Independent Assessment Framework is a resource created by NHSE, for independent assessors of Health and Care organisations. The framework is the resource that the assessor should use to assess the organisation against the requirements of the CAF-aligned DSPT. It can act as the basis of scoping the terms of reference for each CAF-aligned DSPT assessment, the approach that the assessor could take during their review, and inform the type of evidence that the assessor could request and review as part of their work. Further detail on the framework, and how to navigate it, will be provided in the framework itself.

There are five objectives (A-E) within the CAF-aligned DSPT. The CAF-aligned DSPT independent assessment framework outlines the principles that make up each objective, highlighting the area of scope for each principle. Each principle contains several outcomes, which can be "Achieved", "Partially Achieved" or "Not Achieved", depending on the results of their respective indicators of good practice. Each organisation will be assigned a profile, which will be based on the type and size of

the organisation. This profile will be used to identify the expected achievement levels for each outcome.

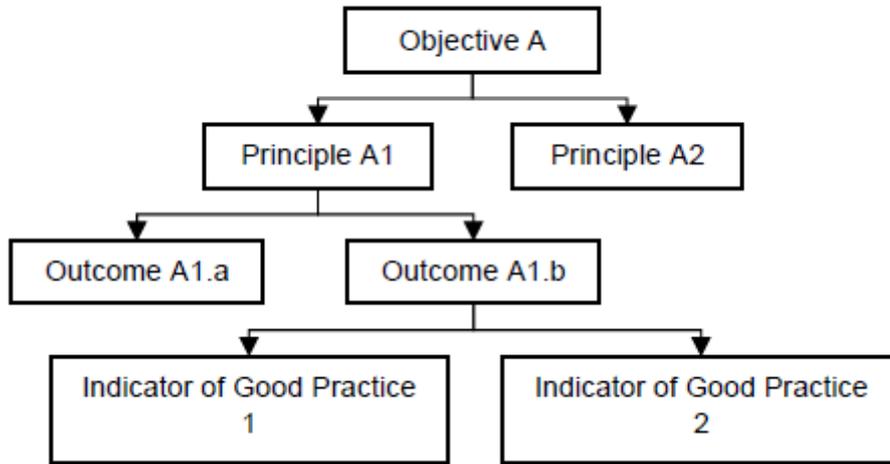


Figure 6

The framework details the control objective of each outcome and Indicator of Good Practise (IGP), and provides guidance on how to assess the organisation’s control environment against the IGPs. It provides an indication of the on-site tests that could be performed, and documents what the assessor should typically request and review, as part of their work. It also includes details on whether or not the IGP is required for this year’s assessment for each category of Health and Social Care organisation.

The framework is designed to be used by independent assessment providers. It will enable independent assessment providers to carry out their assessments in an efficient and consistent manner. It is advised that independent assessment providers have experience in reviewing cyber security and information governance control environments, and the assessment approach is not intended to be exhaustive or overly prescriptive, though it does aim to promote consistency of approach. Assessors are expected to use their professional judgement and expertise in further investigating and analysing the specific control environment, and associated risk, of each health and social care organisation.

### CAF-Aligned DSPT Independent Assessment Programme Timelines

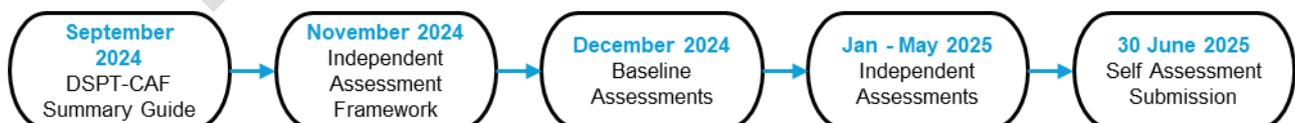


Figure 7

A Project Gantt Chart has been produced at [Appendix M – Outcome 4 – CAF-Aligned DSPT Gantt Chart](#), which outlines the timescales before, during, and post review, and who should be involved.

A defined RACI matrix has also been produced, at [Appendix F – Outcome 1 – Organisational RACI for adopting the Cyber Security Strategy Pillars](#)

Planning for the review by the organisation:

- **Understand Requirements** – Discuss with an independent assessor the timelines and requirements for an independent assessment to be conducted between January and May 2025, including requirements for financial resourcing.
- **Understand CAF Profile** – Review the CAF Profile as set out for your organisation.
- **Understand Expected Achievement Levels** – Review the Objectives, Principles, Outcomes, IGP’s and expected achievement levels for the assessment of your organisation, set out in [Cyber Assessment Framework \(CAF\)-aligned Data Security and Protection Toolkit \(DSPT\) guidance - NHS England Digital](#).
- **Update Leadership** - Provide an update to the Board and Audit Committee of your organisation, indicating expected timelines, scope of assessment and the results of the self-assessment.

There are a total of 47 outcomes in the CAF-aligned DSPT, which will all be assessed over a multi-year period. Each year, a selection of outcomes from across the five objectives will be tested by independent assessment providers. NHSE will mandate a common core set of outcomes to be assessed for all organisations that undertake the CAF-aligned DSPT, while a further number will be selected by individual organisations. These outcomes should be approved by the Board of each organisation, and will reflect areas of concern that warrant additional assurance over the controls in place during that audit period.

More information will be made available in the NHS England (NHSE) DSPT Independent Assessment Framework, to be published in November 2024. Further updates will be provided on the [DSPT News website](#).

**NHS Category Organisation Types**

The 2024-2025 DSPT includes changes to organisation categories, reintroducing the previously discontinued Category 2. This category now includes IT Suppliers and Operators of Essential Service (OES) Independent Providers. IT Suppliers and Independent Providers, who have been designated as OES, **will not** be required to submit a CAF aligned DSPT for the 2024-2025 year. However, NHS organisations, which fall into Category 1, are required to submit their response, by June 2025. Refer to [Appendix M – CAF Aligned DSPT Gantt Chart](#), for a detailed plan for pre, during and post submission actions.

The Categories are shown below:

Table 14

Category 1	Category 2	Category 3	Category 4
NHS Trusts	IT Suppliers	Local Authorities Dentists	General Practitioners (GP’s)

Category 1	Category 2	Category 3	Category 4
Commissioning Support Units (CSU's) Arms Length Bodies (ALB's) Integrated Care Boards (ICB and CCG)	Operators of Essential Service (OES) Independent Providers	Opticians Pharmacies Other in-scope organisations (Charities) Social Care Providers Universities	

The CAF-aligned DSPT approach is geared towards using principles and expert judgment to guide competent decision-making, with a focus on achieving key outcomes. It will affect the way that people, processes and technology are evaluated and assured in cyber security and information governance.

The CAF-aligned DSPT is organised into:

- **Objectives:** Overarching goals of your organisation's cyber security and information governance activities
- **Principles:** Concepts which underpin your organisation's cyber security and information governance 'objectives'
- **Contributing outcomes:** Key markers against which your organisation will judge the effectiveness of your cyber security and information governance practices. These are the key element of the toolkit which you will be prompted to record results against. The combination of all recorded 'contributing outcome' results will determine whether your organisation has achieved 'standards met'
- **Indicators of good practice:** Concrete examples of procedures and processes which help inform your organisation's decision about whether it has achieved a contributing outcome

For each contributing outcome, you will be shown indicators of good practice and the option to select 'Not achieved', 'Partially achieved' or 'Achieved'.

The goals of moving to the CAF-aligned DSPT are to:

- Emphasise good decision-making over compliance, with better understanding and ownership of information risks at the local organisation level where those risks can most effectively be managed
- Support a culture of evaluation and improvement, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes – and expend effort on what works, not what ticks a compliance box
- Create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks

The following groups of health and care organisations will be moving to the CAF-aligned DSPT in 24-25, and will see a new user interface when they log in to file their submission. These organisations are:

- NHS trusts and foundation trusts

- Commissioning support units (CSUs)
- Arm's length bodies (ALBs) of the Department of Health and Social Care (DHSC)
- Integrated care boards (ICBs)

### Scoping Essential Functions

Before starting your CAF-aligned DSPT submission, a scoping exercise is necessary to determine the essential functions, systems, and networks that support critical healthcare services. Essential functions include critical business processes, statutory purposes, and services under NIS regulations.

The CAF-aligned DSPT should cover all essential functions and critical systems, with some elements of the DSPT return also requiring consideration of non-essential functions; for example data protection considerations which apply to any service, and underlying information, systems or networks, where personal data is handled.

A scoping exercise should document the essential functions and the information, systems and networks supporting them. A clear, demonstrable, and risk-based justification of the scope should be maintained, which should be considered an evolving document that will change over time in response to increased knowledge, changes in operating systems, or following incidents.

Scoping activities should include multi-disciplinary stakeholders, representative of your whole organisation, who have a deep understanding of your services and systems and any wider touch points. Third party dependencies which support your essential function should also be identified within your scope.

### Defining Essential Functions

Your essential functions are all the parts of your organisation that are necessary to deliver your organisation's services. Where relevant, this will include consideration of:

- Any essential services for operators of essential services designated under the NIS Regulations
- Any statutory purposes for statutory organisations
- The purposes for which your organisation is constituted

In practice, your essential functions may equate to all your critical business processes.

### Example of Essential Functions for NHS Trusts and Foundation Trusts

Essential services include, but are not limited to, for example, elective care, urgent and emergency care, mental health care and community care. This may be further broken down, for example, diagnostics, surgery and rehabilitative care. Critical systems may include those supporting, for example, access to medical records and imagery, sterilisation, patient transportation, laboratory, administration, finance, HR and payroll services. Each system plays a vital role in ensuring smooth healthcare delivery within the organisation.

**Example of how Essential Functions and Systems may be broken down**

Essential service (example for NHS trusts and foundation trusts):

- healthcare services

Essential functions:

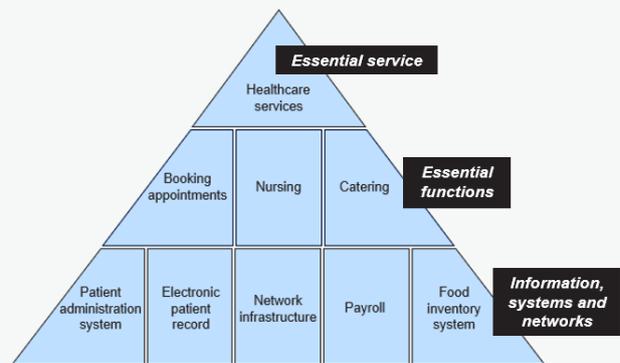
- booking appointments
- nursing
- catering

Systems that support the operation of essential functions:

- patient administration system
- electronic patient record
- network infrastructure
- payroll
- food inventory system

**Criteria for your DSPT ‘essential functions’ scope**

- Does it support the provision of your essential service(s)?
- OR**
- Does it hold personal data?
- OR**
- If compromised by an incident, could it have a cascading impact across your other systems and networks?



*This is an example and may contain many more elements in each segment*

**If ANY of the above apply, the information / asset / system / network should be included in the scope of your DSPT assessment**

Figure 8

## DSPT CAF - Essential functions

- The 24/25 DSPT references “essential functions” and “information systems and networks” within the indicators of good practice.

All assets relevant to the secure operation of essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. This includes maintaining an information asset register (IAR) which is reviewed and kept up to date.

Key roles and responsibilities for the security and governance of information, systems and networks supporting your essential function(s) have been identified. These are reviewed regularly to ensure they remain fit for purpose.

Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function(s), as set by senior management.

You understand the general risks suppliers may pose to your essential function(s).

Your risk assessments are informed by an understanding of the vulnerabilities in the systems and networks supporting your essential function(s), as well as your other data processing activities.

Your organisational process ensures that security and wider Information Governance (IG) risks to information, systems and networks relevant to essential function(s) are identified, analysed, prioritised, and managed. This includes incorporating data protection by design and default into your process.

Direction set at board level is translated into effective organisational practices that direct and control the security and governance of information, systems and networks supporting your essential function(s).

Regular board discussions on the security and governance of information, systems and networks supporting the operation of your essential function(s) take place, based on timely and accurate information and informed by expert guidance.

You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential function(s).

A scoping exercise may need to be conducted to identify what your organisations “essential functions” and “information systems and networks” are.

Figure 9

The Trusts must own and manage the process of scoping essential functions and critical systems. To do this, you need to undertake a scoping exercise which identifies:

- What your essential functions are** – the phrasing of whether it is an essential function, service or critical business process should not matter, it is the fact that the compromise or failure of that function, service or process would lead to unacceptable consequences
- All information, systems and networks which support your essential functions** - and which could result in a significant impact on the continuity of an essential service if compromised by an incident

It is expected that each organisation can evidence that workshops have taken place or provide evidence of activity conducted to define their essential functions, inclusive of multi-disciplinary teams, which includes: Cyber, IT, EPRR, and Operational.

The information required for your scoping assessment is likely to already exist in business continuity impact assessments, [information assets and flows registers](#), asset registers, network architecture diagrams, and similar internal documentation which has been required under previous iterations of the DSPT.

Further guidance on Scoping Essential Functions, is available at the [Appendix C - References](#).

To review compliance against Part A – Part E of the DSPT / CAF, please refer to [Appendix A – DSPT / CAF – Strategic Outcomes](#).

### Interim Baseline Assessment

As per the guidance released by NHSE on 8<sup>th</sup> November ([link](#)), NHS Trusts, ICB’s, DHSC Arm’s Length Bodies and Commissioning Support Units are required to publish an interim (baseline) CAF-aligned DSPT assessment, by 31 December 2024.

Note – other sectors are not required to publish the interim assessment.

The interim assessment indicates that your self-assessment is under way and that you understand your position in December 2024. It may also highlight to your organisation, areas which need particular focus ahead of the full assessment deadline of 30 June 2025.

The interim assessment is not formally assessed by NHS England and the Department of Health and Social Care (DHSC) as part of performance management, but it allows NHS England and DHSC to understand the current position of organisations against the DSPT CAF profile across the different outcomes, review interim responses to outcomes and determine whether further guidance or support is required.

### **What is expected to be included in the interim assessment?**

You should record your organisation's current achievement level (Not achieved/Partially Achieved/Achieved) against each outcome in the DSPT.

It would be helpful to us if you included any evidence or supporting statements to provide context to the achievement levels, but this is not mandatory.

For outcomes that have a policy question (A2.b Assurance, B2.a Identity verification, authentication and authorisation and B4.d Vulnerability management) you will not be able to select any achievement level other than Not Achieved if you have not confirmed that you are meeting the policy question.

### **How to publish an interim assessment**

You cannot currently publish an interim assessment as the functionality is not yet available. An Interim assessment section followed by a 'Start Now' button will go live on the assessment screen late **November 2024** and you can then publish an interim assessment by following the 'publish interim assessment' link on the assessment page. You will receive an email confirmation once you have published your interim assessment.

There are no minimum expectations for each outcome before you can publish your interim assessment as it is a snapshot of current progress.

Details of your interim assessment are not shared in the public domain, only confirmation that you have completed an interim assessment and the date it was published.

Your interim assessment shall be submitted by **31 December 2024**, via the below portal:

<https://www.dsptoolkit.nhs.uk/News/www.dsptoolkit.nhs.uk/Account/Login>

### **Outcome 4 - Roles and Responsibilities**

A Roles and Responsibilities (RACI) Matrix is available at the following section - [Appendix I – Outcome 4 - Organisational RACI for CAF Aligned DSPT](#).

## Outcome 4 - Timescales

A full Gantt Chart against Outcome 4 initiatives, is available at [Appendix M – Outcome 4 – CAF-Aligned DSPT Gantt Chart](#).

## Strategy Timeline

The full strategy Timeline can be found in

*Figure 1.*

A full breakdown of each Outcome Timeline, is available at the below Sections:

- **Outcome 1** - [Appendix J – Outcome 1 – Adopting the Cyber Security Strategy Pillars Gantt Chart](#)
- **Outcome 2** - [Appendix K – Outcome 2 – NHSE Cyber Risk Investment Gantt Chart](#)
- **Outcome 3** - [Appendix L – Outcome 3 – Staff Awareness and Culture](#)
- **Outcome 4** - [Appendix M – Outcome 4 – CAF-Aligned DSPT Gantt Chart](#)

## Key Cyber Strategy Dates

The below key dates have been identified, as part of the Cyber Security Strategy:

Table 15

Milestone	Date	Description
Strategy Initial Draft	November 2024	Initial creation of Cyber Strategy, discussed with Regional Security Lead (RSL)
Submit Strategy to ICB for signoff	December 2024	-
Submit Strategy to NHSE for review/approval	18 December 2024	-
NHSE confirm strategy is compliant with guidance	January 2025	-
Submit Strategy for Board approval (7 organisations)	February 2025 – March 2026	-
Formal sign-off and submission of strategy by ICB Board, as the statutory body	30 April 2024	Strategy to be fully approved and endorsed by the ICS, and information on protocol for submission to NHSE, will be made available to ICS's, by RSL
New CAF-aligned DSPT released	September 2024	Release of the NHSE guidance
North West London ICS Cyber Risk Investment – Assessment Tool	October 2024	Released w/c 14 October, for all Trusts to complete and return
Further Guidance on Independent Assessment Framework released by NHSE	November 2024	Further guidance released by NHSE
NHSE Cyber Risk Investment Deadline (NHS Cyber Improvement Programme)	March 2025	Funding to be used by date
Compile responses, with Independent Assessors	Jan – May 2024	CAF-aligned DSPT baseline response completed
DSPT Submission	30 June 2025	CAF-aligned DSPT baseline response to be submitted

# Resourcing the Strategy

## Capacity

Dedicated cyber security functions within the ICS are being developed, including agreements with member organisations with stronger staffing and resource capacities to provide these at a system level. Throughout this strategy life, and as a need for capacity rises, the ICS will consider schemes to free up investment for resources and prioritise funding to manage those greatest risks and harms.

## Resource Availability

The ICB Chief Information Security Officer (CISO) and CIO will work with dedicated local resources to bring together the ICS/Trust members to deliver this strategy. The CISO shall be supported in all cases by the CIOs, DPOs, Caldicott Guardians, Executive Directors and IT/Information Security/Information Governance Teams.

In order to successfully execute on this strategy, and to align with the CAF-aligned DSPT, the below roles shall be established, as a minimum:

Table 16

Role	Employed
<a href="#">Chief Information Security Officer</a>	Yes / No
<a href="#">Senior Information Risk Owner</a>	Yes / No
<a href="#">Caldicott Guardian</a>	Yes / No
Executive Directors - Sponsor	Yes / No
Chief Finance Officer	Yes / No
<a href="#">Data Protection Officer</a>	Yes / No
<a href="#">Information Governance Lead</a>	Yes / No
<a href="#">Information Security/Cyber Security Lead</a>	Yes / No
Risk & Assurance Manager	Yes / No
IT Lead	Yes / No
Project / Programme Management Resource	Yes / No
Communications Representative	Yes / No
Procurement Representative	Yes / No
Human Resources Representative	Yes / No

Where the above roles are not available, the organisation should consider raising a risk on their Risk Register, as per the guidance at [Section - Risk Management](#).

# Key Stakeholders

Table 17

Name	Role	Description	Contact Details
Kathy Lanceley	ICH CISO / Deputy SIRO		07795838734 <a href="mailto:k.lanceley@nhs.net">k.lanceley@nhs.net</a>
Peter Hartley	London Region Security Lead		<a href="mailto:peter.hartley2@nhs.net">peter.hartley2@nhs.net</a>
	SIRO		
	Organisation CIO - need to list all these		
Steve Bloomer	ICS CFO	ICS CFO	
	7 Trust CFO's to be included		
	Communications Team		
Steve Anthony	Role to be added by Stakeholder	Imperial College Healthcare NHS Trust	steve.anthony@nhs.net
David Everett	Role to be added by Stakeholder	Imperial College Healthcare NHS Trust	davideverett@nhs.net
Kevin Jarrold	Role to be added by Stakeholder	Imperial College Healthcare NHS Trust	<a href="mailto:kevin.jarrold@nhs.net">kevin.jarrold@nhs.net</a>
Emma Cowen	Role to be added by Stakeholder	Chelsea and Westminster Hospital NHS Foundation Trust	emma.cowen@nhs.net
James Warden	Role to be added by Stakeholder	Chelsea and Westminster Hospital NHS Foundation Trust	james.warden@nhs.net
Andrew McEwan	Role to be added by Stakeholder	West London NHS Trust	andrew.mcewan@westlondon.nhs.uk
Sam Marshall	Role to be added by Stakeholder	West London NHS Trust	<a href="mailto:sam.marshall@westlondon.nhs.uk">sam.marshall@westlondon.nhs.uk</a>
Omer Moghraby	Role to be added by Stakeholder	West London NHS Trust	omermoghraby@nhs.net
Asim Mir	Role to be added by Stakeholder	Central London Community Healthcare NHS Trust	asim.mir2@nhs.net
Andrew Chronias	Role to be added by Stakeholder	Central London Community Healthcare NHS Trust	andrew.chronias@nhs.net
John Keating	Role to be added by Stakeholder	London North West University Healthcare NHS Trust	john.keating@nhs.net
Abhilash Abraham	Role to be added by Stakeholder	NHS North West London ICB	abhilash.abraham@nhs.net

OFFICIAL-SENSITIVE

Name	Role	Description	Contact Details
Andrew Wright	Role to be added by Stakeholder	The Hillingdon Hospitals NHS Foundation Trust	andrew.wright24@nhs.net
Gary Elvin	Role to be added by Stakeholder	Central and North West NHS Foundation Trust	<a href="mailto:gary.elvin@nhs.net">gary.elvin@nhs.net</a>

Final draft

## Strategy Approval

Executive support and board sponsorship is fundamental to the success of this strategy. Priorities being driven and supported from senior leadership across our ICS will ensure that the strategic objectives outlined will be delivered to support and enable the wider operational objectives.

## Strategy Author

Name	Role	Date
Kathy Lanceley	CISO	

## Strategy Sponsor

Name	Role	Date
Kevin Jarrold	ICB CIO	

## Executive Approval

Name	Role	Date
TBC		

## Discussed and Approved at Board Level Meeting

Meeting Name	Date
Insert name of Board Level Meeting	

## Appendix A – DSPT / CAF – Strategic Outcomes

As identified at Section ‘ Strategy Outcome 4 – A Strategy to Adopt the CAF-aligned DSPT’, an Interim Baseline Assessment is required to be submitted via the [DSPT Portal](#), by **31 December 24**.

To support the organisation, a CAF-aligned DSPT Gap Analysis Tool has been developed, which can be used to collect and document appropriate evidence, to submit to the portal.

Insert the Tool

### ***CAF-aligned DSPT Tool***

The tool has been created, following the NHSE guidance, which is available [here](#).

Final draft

## Appendix B - List of National Services and Resources

Table 18

National Offering	Description	Strategic Pillars
<a href="#">BitSight</a>	A central platform that uses externally observable events, data sinkholes and 3 <sup>rd</sup> party data to continuously assess cyber security ratings for NHS and partner organisations. The service provides organisations with a security rating to help them measure their security, risks and plan remediation activities.	Defend as One Build Secure for The Future Focus on the Greatest Risks and Harms
<a href="#">Cyber Associates Network</a>	Future NHS-hosted cyber specific group for NHS/DHSC and general cyber updates, knowledge-sharing, professional development and networking with peers in health and care.	People and Culture Defend as One
<a href="#">Cyber Assurance Service</a>	External and internal vulnerability testing to identify areas of weakness and recommended remediation.	Focus on the Greatest Risk and Harms Build Secure for the Future
<a href="#">Cyber Incident Response Exercises</a>	Realistic scenarios and resource-based service that aims to develop and test understanding of how incident response should be carried out in a health and social care setting and context.	People and Culture Exemplary Response and Recovery Defend as One
<a href="#">Immersive Labs</a>	Training platform which helps users to improve their cyber security skills, judgement and knowledge, increasing cyber resilience in the workforce. Suitable for all roles, it's easy to use and offers bitesize activities that fit into busy schedules.	People and Culture Build Secure for The Future Exemplary Response and Recovery
<a href="#">Keep I.T. Confidential Awareness Resources</a>	Security awareness campaign resources to help protect NHS organisations from cyber threats and keep unauthorised people away from sensitive or confidential information such as patient data, health care records or details of NHS IT systems.	People and Culture
<a href="#">Microsoft Defender for Endpoint</a>	NHS-wide, enterprise endpoint security platform designed to prevent, detect, investigate, and respond to advanced threats with system wide visibility and analytics.	Focus on the Greatest Risks and Harms Exemplary Response and Recovery Defend as One
<a href="#">NCSC Assured Cyber Board Training</a>	Cyber training that is tailored to NHS board members with their understanding of the evolving threat landscape and what this means to them.	People and Culture Defend as One
<a href="#">NCSC Assured Cyber SIRO Training</a>	Supporting Senior Information Risk Owners (SIROs) and their deputies to improve their knowledge about cyber security risks and obligations.	People and Culture Focus on the Greatest Risks and Harms Build Secure for The Future

National Offering	Description	Strategic Pillars
<a href="#">Secure Boundary</a>	Next generation firewall and Web Application firewall to protect internet traffic from digital and cloud-based threats.	Defend as One Exemplary Response and Recovery Build Secure for The Future
<a href="#">Simulated Phishing Exercises</a>	Simulated phishing platform to provide capability to test cyber awareness within local organisations or wider ICS contingent. Available upon request to NHS organisations using NHSmail and NHS.uk domains.	People and Culture Defend as One
<a href="#">Technical Remediation</a>	Catalogue of assessment discovery and remediation services to help identify risks/issues and address technical exposures to reduce cyber security risk. E.g. Active Directory and backup assessments to identify weaknesses and deviations from best practice.	Focus on the Greatest Risk and Harms Build Secure for the Future
<a href="#">Vulnerability Monitoring Service</a>	A regular non-intrusive external vulnerability scan to assess NHS stakeholder's public facing vulnerabilities, helping organisations to identify and prioritise which actions to take to improve cyber security levels.	Focus on the Greatest Risks and Harms Defend as One Build Secure for The Future
<a href="#">NCSC Cyber Exercise in a Box</a>	A free resource which helps organisations find out how resilient they are to cyber attacks and practise their response.  Available to all organisations, for free, from the NCSC	Exemplary Response and Recovery Focus on Greatest Risks and Harms
<a href="#">NCSC Active Cyber Defence</a>	Active Cyber Defence (ACD) seeks to reduce the harm from commodity cyber attacks by providing tools and services that protect from a range of attacks.  Available to UK Public Sector organisations, for free, by the NCSC	Defend as One Focus on Greatest Risks and Harms
<a href="#">NCSC CiSP</a>	CiSP is a platform for cyber security professionals in the UK to collaborate on cyber threat information in a secure and confidential environment. It is managed by the NCSC and membership is free,	Defend as One Defend as One Focus on Greatest Risks and Harms

## Appendix C - References

Table 19

Reference	Link / Document
A plan for digital health and social care	<a href="https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care">A plan for digital health and social care - GOV.UK (www.gov.uk)</a>
Board Assurance Toolkit	<a href="https://nhsproviders.org/media/1182/board-assurance-a-tool-kit.pdf">https://nhsproviders.org/media/1182/board-assurance-a-tool-kit.pdf</a>
Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT) guidance	<a href="https://www.nhs.uk/healthcare-technology/cyber-security/cyber-assessment-framework-CAF-aligned-data-security-and-protection-toolkit-DSPT-guidance">Cyber Assessment Framework (CAF)-aligned Data Security and Protection Toolkit (DSPT) guidance - NHS England Digital</a>
Cyber Associates Network (CAN)	<a href="https://www.nhs.uk/healthcare-technology/cyber-security/cyber-associates-network">Cyber Associates Network - NHS England Digital</a>
Cyber Risk Investment Decision Making – Annex A (FY 2024/25)	This document has a protective marking of OFFICIAL-SENSITIVE, and is not published externally. Please request a copy, from Kathy Lanceley.
Cyber Risk Investment Decision Making Guide (FY 2024/25)	This document has a protective marking of OFFICIAL-SENSITIVE, and is not published externally. Please request a copy, from Kathy Lanceley.
Cyber Security Strategy for Health and Social Care to 2030	<a href="https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030">https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030</a>
Data Saves Lives Strategy	<a href="https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data">Data saves lives: reshaping health and social care with data - GOV.UK (www.gov.uk)</a>
Digital Care Hub	<a href="https://www.digitalcarehub.co.uk/dspt/">https://www.digitalcarehub.co.uk/dspt/</a>
DSIT Cyber Resilience Policy	<a href="https://www.gov.uk/government/publications/cyber-resilience">Cyber resilience - GOV.UK (www.gov.uk)</a>
DSPT 2024-2025 for IT Suppliers and Independent Providers who are designated Operators of Essential Services – Category Organisation Types	<a href="https://www.dsptoolkit.nhs.uk/Help/Org-Types">https://www.dsptoolkit.nhs.uk/Help/Org-Types</a>
DSPT 24-25 Interim (Baseline) Assessment Update – 8 November 2024	<a href="#">News</a>
DSPT Toolkit – CAF Summary Audit Guide v7 24-25 V1.0	<a href="https://www.dsptoolkit.nhs.uk/StaticContent/Attachment/827">https://www.dsptoolkit.nhs.uk/StaticContent/Attachment/827</a>
Guidance for developing an ICS cyber security strategy 2022 – 2030	This document is not published externally. Please request a copy, from Kathy Lanceley.
Just Culture	<a href="https://www.nhs.uk/healthcare-technology/cyber-security/just-culture">NHS England » A just culture guide</a>
NCSC Annual Review 2024	<a href="https://www.ncsc.gov.uk/annual-review-2024">NCSC Annual Review 2024 - NCSC.GOV.UK</a>
Network and Information Systems (NIS) Regulations security duties. Through the Health and Care Act 2022, ICBs were designated as Operators of Essential Services (OES) for the health sector from the NIS regulations	<a href="https://eur-lex.europa.eu/eli/dir/2022/2555">https://eur-lex.europa.eu/eli/dir/2022/2555</a>
NHS England – DSPT 2024/2025 (version 7) standard	<a href="https://www.dsptoolkit.nhs.uk/News/131">https://www.dsptoolkit.nhs.uk/News/131</a>

Reference	Link / Document
NHSE DSPT Frequently Asked Questions (FAQ)	<a href="https://dsptoolkit.nhs.uk">Help (dsptoolkit.nhs.uk)</a>
NW London ICS Board Meeting in Public	<a href="#">Board Meeting in Public</a>
Scoping essential functions	<a href="https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/2024-25-caf-aligned-dspt-guidance/overview/scoping-essential-functions">https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/2024-25-caf-aligned-dspt-guidance/overview/scoping-essential-functions</a>
Scoping Essential Functions (NHS CAF)	<a href="#">Scoping essential functions - NHS England Digital</a>
The 2022 Health and Care Bill amended the 2004 Civil Contingencies Act (CCA) to designate Integrated Care Boards (ICBs) as “Category 1 responders”, which means that they are at the core of an emergency response	<a href="https://publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/114844/health-and-care-act-2022-summary-and-additional-measures-impact-assessment.pdf">health-and-care-act-2022-summary-and-additional-measures-impact-assessment.pdf (publishing.service.gov.uk)</a>

## Appendix D - Checklist for Board Assurance

Table 20

Topic	Yes / No
Is the cyber strategy aligned with the ICS-wide vision and mission?	Yes
Have all relevant ICS-wide organisations reviewed and agreed the strategy direction and timescales?	Yes
Is there governance outlined to direct, manage and account for deliverables in cyber strategy?	Yes
Does the strategy establish clear roles and responsibilities for cyber security within ICS and member organisations?	Yes
Does the strategy make provision for monitoring and reporting cyber security performance data across the ICS, and facilitate sharing between member organisations and NHS England?	Yes
Does the strategy outline a need to manage supply chain and 3 <sup>rd</sup> party provider risk and assurances.	Yes
Does the strategy establish the key performance indicators and metrics for measuring the effectiveness and efficiency of the cyber strategy?	Yes
Are the strategic objectives, Specific, Measurable, Achievable, Relevant and Time-Bound in the cyber strategy?	Yes
Does the strategy align, both in relation to objectives and timescale, with the ICS risk appetite and tolerance?	Yes
Does the strategy foster a culture of learning and continual improvement, and leverage the best practices and standards in the industry?	Yes
Are you, as a collective board assured and confident of the strategy and its delivery?	Yes / No

## Appendix E - Checklist for Strategy Authors

Table 21

Topic	Yes / No
Does the strategy comply with the relevant legal, regulatory and ethical obligations for cyber security in Health & Care?	Yes
Is the strategy sponsored at an executive level, to ensure it is understood and embedded from the top down?	Yes
Is there documented governance to ensure that objectives have appropriate support, momentum and ownership by senior stakeholders in the strategy?	Yes
Does the strategy delineate a roadmap for the ICS to foster and advance the cyber security function and embed this as part of the organisational culture, promoting heightened awareness among all stakeholders?	Yes
Does the strategy encourage and support innovation and collaboration in cyber security across ICS organisations and with external partners?	Yes
Does the strategy support the overall operational strategic objectives of the ICS?	Yes
Is the strategy document structured to ensure that strategic objectives and their priorities are clear?	Yes
Does the strategy outline the desired methodology for identifying and managing cyber risks?	Yes
Do the strategic objectives address challenges and risks that may affect the delivery of ICS-wide critical services?	Yes
Does the strategy align with the ICS risk appetite and tolerance?	Yes

## Appendix F – Outcome 1 – Organisational RACI for adopting the Cyber Security Strategy Pillars

For each task to be completed during the adoption of the Cyber Security Strategy Pillars, the indicative RACI table below sets out the people responsible and accountable for the completion, as well as anyone who may be consulted during the task, and who should be informed when the task is being undertaken, and when it has been completed:

Table 22

Task	Responsible	Accountable	Consulted	Informed
Establish Strategy KPI's and Governance Reporting	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead	Executive Directors Project / Programme Management CFO Caldicott Guardian
Allocate funding to deliver the strategy, establishing governance to review and align plans, across the ICS	SIRO CISO InfoSec Team	CFO	IG Team Risk & Assurance Manager IT Lead Project / Programme Manager	Executive Directors Caldicott Guardian
Establish defined security Roles and Responsibilities, across the ICS	SIRO CISO DPO	Executive Directors CFO	InfoSec Team IG Team Risk & Assurance Manager IT Lead Caldicott Guardian	Wider Organisation
Establish a common language and understanding of risks, across the ICS – Develop and publish an ICS Risk Management Framework	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Identify and record risks within the Trust, including supplier cyber risks, that would affect the local system's ability to function	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian Procurement	Executive Directors Project / Programme Management CFO

Task	Responsible	Accountable	Consulted	Informed
Monitor risks at ICS level to manage risks / investments, in a collaborative and efficient manner	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Ensure cyber risk is reviewed as part of broader corporate risk management – Board Assurance Framework	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Ensure Trusts maintain an understanding of their suppliers' cyber security controls and risks	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian Procurement	Executive Directors Project / Programme Management CFO
Increase visibility of the attack surface, primarily using NHSE centrally provided tools	InfoSec Team IT Lead	SIRO CISO		IG Team Risk & Assurance Manager Caldicott Guardian Executive Director Project / Programme Management CFO
Establish a Threat Management Framework (Threat Intelligence, Threat Modelling and Threat Hunting), across the ICS	InfoSec Team IT Lead	SIRO CISO	Security Operations Centre / Managed Detection and Response provider (if any)	IG Team Risk & Assurance Manager Caldicott Guardian Executive Director Project / Programme Management CFO
Create and publish an ICS Cyber Incident Management Standard and Cyber Incident Response Plan (adopt a common language for reporting and managing Cyber Incidents)	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager	Executive Directors Project / Programme Management CFO Caldicott Guardian
Review current Policies and Standards, to ensure they support the adoption of the	InfoSec Team IG Team	SIRO CISO	Risk & Assurance Manager IT Lead	Executive Directors Project / Programme Management

Task	Responsible	Accountable	Consulted	Informed
CAF-aligned DSPT and Regulatory requirements		DPO	Caldicott Guardian	CFO
Develop an appropriately resourced and accountable cyber security function, to manage cyber risk	SIRO CISO DPO	Executive Directors CFO	InfoSec Team IG Team Risk & Assurance Manager IT Lead Caldicott Guardian Human Resources / Recruitment Team	Wider Organisation
Develop a recruitment strategy, to maintain an adequate cyber security support function, across the ICS	SIRO CISO DPO	CFO	InfoSec Team IG Team Risk & Assurance Manager IT Lead Human Resources Team	Executive Directors Caldicott Guardian
Embed Cyber Security resources, into multi-disciplinary forums (such as Digital, Physical, Project and Programme Management), to ensure holistic cyber security culture, across the ICS	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Document and publish guidance and training on Secure by Design	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Document an ICS level Secure by Design Assurance / Certification Process (3LOD model)	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Practice Secure by Design, on new projects and programmes, across the ICS	InfoSec Team IG Team Project / Programme Management	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors CFO
Establish an ICS Third Party Supplier Assurance Framework	InfoSec Team IG Team Procurement	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO

Task	Responsible	Accountable	Consulted	Informed
Trusts and ICS to have defined the definition of their Key Third Party Suppliers	InfoSec Team IG Team Procurement	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Trusts and ICS to initiate Third Party Assurance, on Key Third Party Suppliers, in accordance with the Framework	InfoSec Team IG Team Procurement	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
Document an ICS / Trust – Cyber Incident Simulation Exercise Plan	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager Caldicott Guardian Communications Team Executive Directors Project / Programme Management	CFO
Conduct Simulation Exercises, in accordance with the published plan – conducting at least one ICS wide simulation	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager Caldicott Guardian Communications Team Executive Directors Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	CFO
Conduct lessons learned activity, and enhance Cyber Incident Response Plan	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager Caldicott Guardian Communications Team Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors Project / Programme Management CFO

## Appendix G – Outcome 2 – Organisational RACI for the NHSE Cyber Risk Investment

For each task to be completed associated with the NHSE Cyber Risk Investment, the indicative RACI table below sets out the people responsible and accountable for the completion, as well as anyone who may be consulted during the task, and who should be informed when the task is being undertaken, and when it has been completed:

Table 23

Task	Responsible	Accountable	Consulted	Informed
'NW London ICS Cyber Risk Investment – Assessment Tool' issued to Security Leads	InfoSec Team	CISO	IT Team	CFO
Returns received for 'NW London ICS Cyber Risk Investment – Assessment Tool'	InfoSec Team	CISO	IT Team	CFO
Cyber Security Risk Reduction Funding Submission Form for ICSs FY24-25 - Submitted	CISO	CFO	InfoSec Team	Executive Directors NHSE – Regional Security Lead
Malware Detection: Anti-virus(AV)/Anti-malware(AM) is installed on all systems that are connected/able to connect to the internet The Trust is leveraging Microsoft Defender AV from NHSE	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Perimeter Protection: Utilise a well-managed Web Application Firewall to monitor inbound traffic and filter outbound web connections	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Vulnerability Management (VM): A dedicated VM tool has been deployed A dedicated VM resource is in post	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO	Executive Directors

Task	Responsible	Accountable	Consulted	Informed
			Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	
Backups: Regular backups are conducted with >2 copies available Backups are immutable Backups are offline / off-site Backups are tested, to assess validity, security and practical recover times, against business requirements	InfoSec Team IT Lead Information Asset Owners	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Security Event Logs - MVP Phase 1 - Log Retention / Minimum Viable Logs (Critical Logs): A Security Information Event Management (SIEM) solution is in place Critical system logs are being received by the SIEM Logs are retained in the SIEM for >6 months	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Identity and Access Management (Including Privileged Access Management): Separate internal access controls are clearly defined and documented External access controls are defined and documented for remote access users	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Multi-Factor Authentication (MFA): MFA is enforced on all remote access and privileged user accounts External users are forced to re-authenticate after a period of inactivity	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors

Task	Responsible	Accountable	Consulted	Informed
<p>Security Event Logging - Phase 2 - Fully operational SIEM solution:</p> <p>A Security Information Event Management (SIEM) solution is fully operational and receiving logs from key security tooling</p>	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
<p>Cyber Strategy &amp; Governance:</p> <p>A cyber strategy is published at the Trust level The Board has endorsed your cyber security strategy</p>	CISO	SIRO Executive Directors	InfoSec Team IT Lead Risk & Assurance Manager IG Team CFO Communications Team Project / Programme Management	Wider Organisation
<p>Cyber Risk Management:</p> <p>A standardised Risk Management process, is published You operate and maintain a data security and protection risk register, effectively</p>	Risk & Assurance Manager	SIRO CISO DPO	InfoSec Team IG Team IT Lead Caldicott Guardian	Executive Directors Project / Programme Management CFO
<p>Domain Name System (DNS) traffic filtering - Phase 1 - PDNS Deployment:</p> <p>NHSE PDNS solution is deployed</p>	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
<p>Cyber Incident Management:</p> <p>A cyber incident response plan has been published, with clear roles and responsibilities defined A cyber incident test plan, has been published Cyber incident simulations / tests, are conducted against the plan</p>	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager	Executive Directors Project / Programme Management CFO Caldicott Guardian

Task	Responsible	Accountable	Consulted	Informed
You leverage the Cyber Incident Response Exercise (CIRE) service				
Business continuity & disaster recovery: A BCP has been defined and published You perform tests, in accordance with a defined BCP test plan	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager Caldicott Guardian Communications Team Executive Directors Project / Programme Management	CFO
Scenario based technical exercising: Scenario based exercising is regularly completed Cyber Incident Response plans are updated, to reflect lessons learned Red, Blue and Purple team exercises are conducted	InfoSec Team IG Team IT Lead	SIRO CISO DPO	Risk & Assurance Manager Caldicott Guardian Communications Team Executive Directors Project / Programme Management	CFO
Third party secure remote access: Third party access is routed through a centralised gateway, to facilitate monitoring and oversight Role Based Access Control (RBAC) is defined and enforced on third party accounts Remote desktop software / virtual private network (VPN) solutions are utilised, for third party remote access	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Domain Name System (DNS) traffic filtering - Phase 2 - Secure Boundary: You utilise DNS traffic filtering to block malicious websites/inappropriate content	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Asset management: You have an up to date asset register, which captures: Sensitive information / data / personal data Hardware Software Connected medical devices				

Task	Responsible	Accountable	Consulted	Informed
Automated tools are used, such as a central management database (CMDB) A formal change management process exists				
Vulnerability scanning - External (Bit Sight): An external VM tool is deployed Vulnerabilities are managed by defined processes / resources	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Vulnerability scanning – Internal An internal VM tool is deployed Vulnerabilities are managed by defined processes / resources	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors
Network Segmentation: Critical systems are protected via appropriate and documented segmented networks A Network Detection and Response (NDR) solution is deployed Logs from the NDR are feeding into a Security Information and Event (SIEM) solution	InfoSec Team IT Lead	SIRO CISO	Risk & Assurance Manager IG Team CFO Project / Programme Management Security Operations Centre / Managed Detection and Response provider (if any)	Executive Directors

## Appendix H – Outcome 3 – Organisational RACI for Staff Awareness and Culture

For each task to be completed to deliver the Staff Awareness and Culture, the indicative RACI table below sets out the people responsible and accountable for the completion, as well as anyone who may be consulted during the task, and who should be informed when the task is being undertaken, and when it has been completed:

Table 24

Task	Responsible	Accountable	Consulted	Informed
Issue the NHSE Staff Awareness and Culture Questionnaire (17 questions), across the ICS and Trusts	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian Communications Team Human Resources Team	Executive Directors Project / Programme Management CFO
Receive responses to NHSE Staff Awareness and Culture Questionnaire	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian Communications Team Human Resources Team	Executive Directors Project / Programme Management CFO
Review feedback at ICS level, and develop a future Staff Awareness and Culture Improvement Plan	InfoSec Team IG Team	SIRO CISO DPO	Risk & Assurance Manager IT Lead Caldicott Guardian Communications Team Human Resources Team CFO Project / Programme Management	Executive Directors

## Appendix I – Outcome 4 - Organisational RACI for CAF Aligned DSPT

For each task to be completed during a CAF-aligned DSPT, the indicative RACI table below sets out the people responsible and accountable for the completion, as well as anyone who may be consulted during the task, and who should be informed when the task is being undertaken, and when it has been completed:

Table 25

Task	Responsible	Accountable	Consulted	Informed
Collect documentation for each principle to be assessed	InfoSec Team IG Team	SIRO DPO	Procurement	Wider Organisation
Discuss and agree current position of each outcome (Achieved, Partially Achieved, Not Achieved)	InfoSec Team IG Team	SIRO DPO	Procurement	Caldicott Guardians Executive Directors
Agree Terms of Reference and timelines for the assessment	IG/IT Manager	SIRO DPO	InfoSec Team IG Team	Caldicott Guardians Executive Directors
Communicate assessment timelines with departments	IG/IT Manager	SIRO DPO		Wider Organisation
Kick off call	IG/IT Manager	SIRO DPO		Caldicott Guardians Executive Directors
Arrange fieldwork meetings	IG/IT Manager	SIRO DPO	Caldicott Guardian	
Send documents to assessors	InfoSec Team IG Team	SIRO DPO		
Take part in fieldwork meetings and collate additional documents	IG/IT Manager DPO Caldicott Guardian	SIRO	InfoSec Team IG Team	
Close out call	IG/IT Manager	SIRO DPO		Caldicott Guardians Executive Directors
Read and discuss draft report	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO		Executive Directors
Agree action owners and timelines	IG/IT Manager	SIRO	Executive Directors	

Task	Responsible	Accountable	Consulted	Informed
	SIRO DPO			
Provide management responses	IG/IT Manager	SIRO		DPO Caldicott Guardian Executive Directors
Read and agree final report	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO		Executive Directors
Create action plan for remediation of findings	IG/IT Manager SIRO DPO Caldicott Guardian	SIRO	Executive Directors	
Add assessors to the toolkit	IG Manager	SIRO		DPO Executive Directors
Submit final report to NHSE	SIRO	SIRO		DPO Caldicott Guardian Executive Directors IT/IG Manager
Present final report to audit committee	SIRO			DPO Caldicott Guardian Executive Directors IT/IG Manager
Ongoing reporting of progress to audit committee	SIRO	SIRO		DPO Caldicott Guardian Executive Directors

# Appendix J – Outcome 1 – Adopting the Cyber Security Strategy Pillars Gantt Chart

The Gantt chart provides an indicative timeline for the adoption for the Cyber Security Strategy Pillars.

<b>Key</b>	<b>Outcome 1 - Actions</b>
------------	----------------------------

## Activities to be Undertaken (2025)

2025 Q1	2025 Q2	2025 Q3	2025 Q4
Practice Secure by Design, on new projects and programmes, across the ICS	Establish Strategy KPI's and Governance Reporting	Identify and record risks within the Trust, including supplier cyber risks, that would affect the local system's ability to function	Create and publish an ICS Cyber Incident Management Standard and Cyber Incident Response Plan (adopt a common language for reporting and managing Cyber Incidents)
Document an ICS level Secure by Design Assurance / Certification Process (3LOD model)	Review current Policies and Standards, to ensure they support the adoption of the CAF-aligned DSPT and Regulatory requirements	Monitor risks at ICS level to manage risks / investments, in a collaborative and efficient manner	Conduct lessons learned activity, and enhance Cyber Incident Response Plan
Document and publish guidance and training on Secure by Design	Allocate funding to deliver the strategy, establishing governance to review and align plans, across the ICS	Ensure Trusts maintain an understanding of their suppliers' cyber security controls and risks	Document an ICS / Trust – Cyber Incident Simulation Exercises Plan
Trusts and ICS to initiate Third Party Assurance, on Key Third Party Suppliers, in accordance with the Framework	Ensure cyber risk is reviewed as part of broader corporate risk management – Board Assurance Framework	Establish a common language and understanding of risks, across the ICS – Develop and publish an ICS Risk Management Framework	Conduct Simulation Exercises, in accordance with the published plan – conducting at least one ICS wide simulation
Trusts and ICS to have defined the definition of their Key Third Party Suppliers		Develop an appropriately resourced and accountable cyber security function, to manage cyber risk	
Establish an ICS Third Party Supplier Assurance Framework		Establish defined security Roles and Responsibilities, across the ICS	
		Embed Cyber Security resources, into multi-disciplinary forums (such as Digital, Physical, Project and Programme Management), to ensure holistic cyber security culture, across the ICS	

### Activities to be Undertaken (2026)

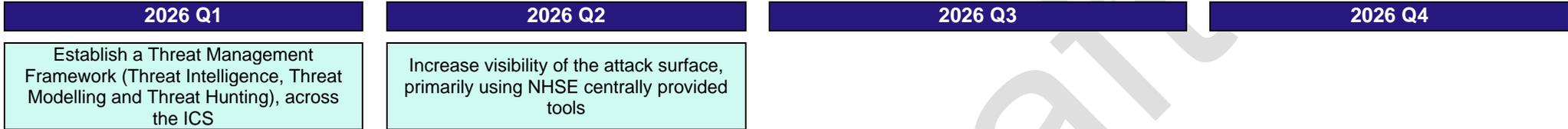


Figure 10

# Appendix K – Outcome 2 – NHSE Cyber Risk Investment Gantt Chart

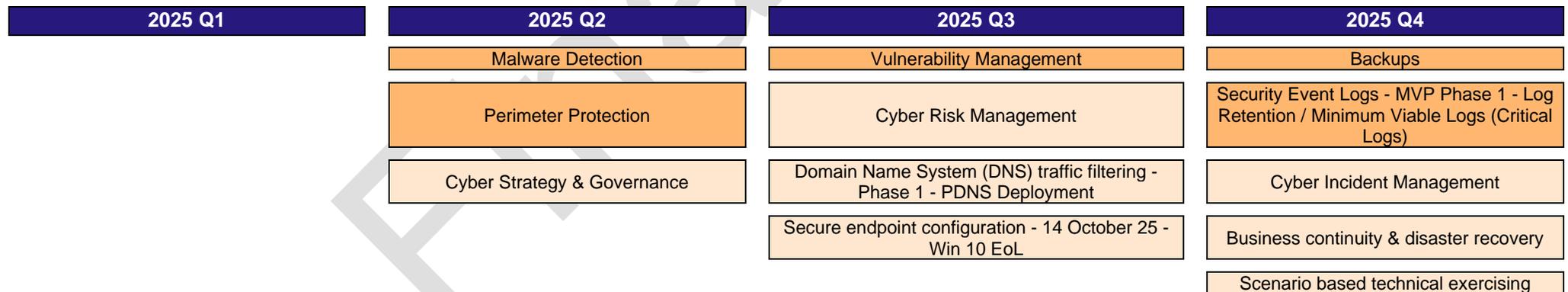
The Gantt chart provides an indicative timeline for the NHSE Cyber Risk Investment actions, as defined in Outcome 2.

<b>Key</b>	<b>Outcome 2 – Cyber Risk Investment Tool</b>	<b>Outcome 2 – Foundational Priorities</b>	<b>Outcome 2 – Other Priorities</b>
------------	---	--	-------------------------------------

## Activities to be Undertaken (2024)



## Activities to be Undertaken (2025)



### Activities to be Undertaken (2026)

2026 Q1	2026 Q2	2026 Q3	2026 Q4
Identity and Access Management (Including Privileged Access Management)	Asset management	Vulnerability scanning - Internal	
Multi-Factor Authentication (MFA)	Security Event Logging - Phase 2 - Fully operational SIEM solution		
Third party secure remote access	Vulnerability scanning - External (Bit Sight)		
Domain Name System (DNS) traffic filtering - Phase 2 - Secure Boundary			

### Activities to be Undertaken (2027)

2027 Q1	2027 Q2	2027 Q3	2027 Q4
Network Segmentation			

Figure 11

## Appendix L – Outcome 3 – Staff Awareness and Culture

The Gantt chart provides an indicative timeline for the Staff Awareness and Culture Outcome.

**Key** Outcome 3 – Activities

### Activities to be Undertaken (2025)

2025 Q1		
[January]	[February]	[March]
Issue the NHSE Staff Awareness and Culture Questionnaire (17 questions), across the ICS and Trusts	Receive responses to NHSE Staff Awareness and Culture Questionnaire	Review feedback at ICS level, and develop a future Staff Awareness and Culture Improvement Plan feedback.

Figure 12

## Appendix M – Outcome 4 – CAF-Aligned DSPT Gantt Chart

The Gantt chart provides an indicative timeline for the completion of the CAF-aligned DSPT, starting with the preparation of the assessment, and ending with post-assessment activities. Collation of the documents and discussions around the organisation’s position for each outcome should take place year-round and are therefore listed as “Prior to week 1” in the chart. Submitting the final report to NHSE must be done before the **30 June 2025** deadline, but this may be farther away than week 9 if the organisation has undertaken their CAF-aligned DSPT early in the year.

<b>Key</b>	<b>Outcome 4 – CAF Align DSPT</b>
------------	-----------------------------------

### Activities to be Undertaken (2024)

2024 Q1	2024 Q2	2024 Q3	2024 Q4
-	-	-	Interim Baseline Assessment - 31 Dec 24

### Activities to be Undertaken (2025)

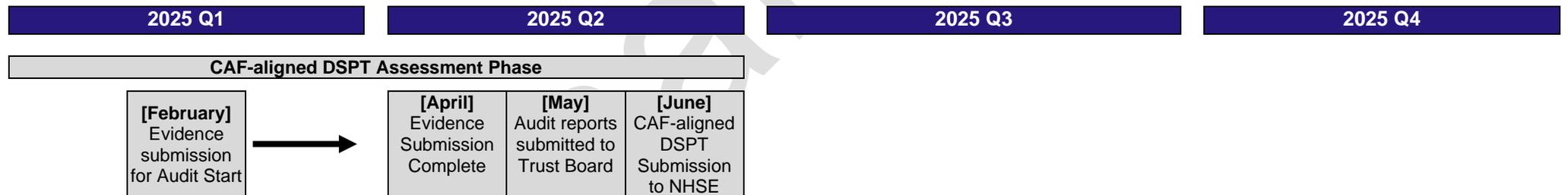


Figure 13

## Activities to be Undertaken Ahead of the Assessment (Assessment Preparation Phase)

Table 26

Task	Assigned To	Prior to Week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post Week 9
Interim Baseline Assessment Submission via DSPT Portal		31 December 2024										
Collate documents for each Outcome in scope	IG Team IT Team											
Discuss and agree current position of each outcome (Achieved, Partially Achieved, Not Achieved)	IG Manager IT Manager SIRO											
Document Terms of Reference and document request list	Assessors											
Agree Terms of Reference with Assessors	IG Manager IT Manager SIRO											
Communicate assessment timelines with departments	IG Manager IT Manager											

## Activities to be Undertaken During the Assessment

Table 27

Task	Assigned To	Prior to Week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post Week 9
Kick off call	IG Manager IT Manager Assessors											
Arrange fieldwork meetings	IG Manager IT Manager Assessors											
Send documents to assessor	IG Manager IT Manager											
Carry out evidence review	Assessors											
Take part in fieldwork meetings and collate additional documents	IG Manager IT Manager											
Close Out call	IG Manager IT Manager Assessors											

## Activities to be Undertaken on Conclusion of the Assessment

Table 28

Task	Assigned To	Prior to Week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post Week 9
Draft report with findings, risks and recommended actions	Assessors											
Read and discuss draft report	IG/IT Manager SIRO DPO Caldicott Guardian											
Agree action owners and timelines	IG/IT Manager SIRO DPO Caldicott Guardian Assessors											
Provide management response	IG/IT Manager											
Draft final report	Assessors											
Read and agree final report	IG/IT Manager SIRO DPO Caldicott Guardian											
Create action plan for remediation of findings	IG/IT Manager SIRO											

Task	Assigned To	Prior to Week 1	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Post Week 9
	DPO											
Add assessors to the Toolkit	IG Manager											
Submit final report to the Toolkit	Assessors											
Submit final report to NHSE	SIRO											
Present final report to Audit Committee	SIRO Assessors											
Ongoing reporting of progress to Audit Committee	SIRO											

Final

## Appendix N – Outcome 2 – NW London ICS Cyber Risk Investment – Assessment Tool

The ‘NW London ICS Cyber Risk Investment – Assessment Tool’ was shared with the organisations of the NW London ICS to assess their current cyber maturity and cyber defence capabilities against the cyber capabilities outlined in ‘Cyber Risk Investment Decision Making – Annex A’.

### Assessment Tool sent out to ICS organisations

Table 29

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care	
Foundational Priorities	Identity and Access Management (Including Privileged Access Management)	Do you have separate Internal Access controls are clearly defined	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
		Do you have separate External Access controls clearly defined for remote access users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Multi-Factor Authentication (MFA)	Is MFA enforced on all remote access and privileged user accounts	No	No	No	No	Yes	Yes	Yes	Yes	Yes
		Are external users forced to re-authenticate following a period of inactivity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Malware Detection	Is Anti-virus(AV)/Anti-malware(AM) installed on all systems that are connected/able to connect to the internet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care	
	Do you leverage Microsoft Defender AV from NHSE	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	
	Perimeter Protection	Do you utilise a well-managed Web Application Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
		Do you monitor inbound traffic	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
		Do you filter outbound web connections	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		Do you have a Security Information Event Management (SIEM)	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
	Security Event Logging	Do you monitor events 24/7 x365	Yes	Yes	Yes	Yes	No	No	Yes	No	No
		Do you store logs off your network	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
		Do you have credentials you can access with that aren't Active Directory (AD) credentials	Yes	No	No	No	Yes	No	No	No	No

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	Do you retain logs for >6months	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
	Are the following recorded:									
	a. failures for input validation	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	b. authentication and authorisation failures	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	c. session management	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
	d. errors in applications, as well as their initialisation/shutdown/pausing	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Vulnerability Management	Is there a dedicated tool deployed	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	Is there a dedicated post occupied	No	Yes	Yes	Yes	No	Yes	No	No	No

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care	
Backups	Regular backups are conducted with >2 copies available	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
	Do you have immutable backups	No	Yes	No	No	No	No	Yes	Yes	No	
	Do you have an offline/off-site backup	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	
	Do you test backups to assess validity, security and practical recovery times	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	
	Generic accounts are not used (best practice is dedicated named accounts)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	
Other Cyber Capabilities	Third party secure remote access	Do you route traffic is through a centralised gateway to facilitate monitoring and oversight	No	Yes	Yes	Yes	Yes	Yes	Yes	No	
		Do you utilise an access control mechanism such as PAM to permit access only to authorised users	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes
		Do you utilise an access control mechanism such as Role-Based Access Management (RBAC) to permit access only to authorised users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	Do you enforce the use of remote desktop software/Virtual Private Network (VPN) which controls access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network segmentation	Do you only permit access to critical systems from certain network segments	No	Yes	No	No	No	No	Yes	Yes	Yes
	Do you limit access between networks to prevent lateral movement	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
	Do you have a Network Detection and Response (NDR) solution deployed	No	No	Yes	Yes	No	Yes	No	No	No
Domain Name System (DNS) traffic filtering	Do you utilise DNS traffic filtering to block malicious websites/inappropriate content	Yes	No	No	No	Yes	No	Yes	Yes	Yes
	Do you leverage the NHS DNS (Protective DNS (PDNS))	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Secure endpoint configuration	Do you configure devices, systems, and applications based on 'gold build,' which are hardened against common vulnerabilities	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Do you use Microsoft Defender for Endpoint (MDE), Intune or an alternative technology to support configuration management	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
Cyber Incident Management	Do you have policies that clearly define who and when a crisis is declared, as well as immediate actions	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Do you test and rehearse Crisis management regularly, with real life simulations used to embed behaviours and required actions	No	Yes	Yes	Yes	Yes	No	Yes	No	No
	Do you have Roles and responsibilities clearly defined and communicated	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Do you leverage the Cyber incident Response Exercise (CIRE) service	No	No	No	No	No	Yes	No	No	No
Cyber Strategy & Governance	Does your board endorsed your cyber security strategy that articulates current and targets state	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
	Does your information security strategy and structure align to the organisation's cyber risk strategy and structure.	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
	Do you have clear documented lines of responsibility and accountability to named individuals for data security and data protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cyber Risk Management	Do you operate and maintain a data security and protection risk register which is linked to the corporate risk framework	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	Do you use benchmarking to understand your current maturity state	Yes	No	No	No	No	No	Yes	Yes	Yes
Scenario based technical exercising	Do you regularly run scenario based exercising and document findings to refine IR plans and protective security	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes
	Do you conduct Red, Blue, and Purple team exercises	No	No	No	No	No	No	No	No	No
Asset management	Do you have an up-to-date asset register for the following:									
	a. Information	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	b. Hardware	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	c. Software	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	d. Connected medical devices,	No	Yes	Yes	Yes	Yes	No	Yes	No	No

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care	
	e. Systems storing personal data,	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
	f. Systems storing business and commercial data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
	Do you use automated tools to support asset management processes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	
	Do you have a formal change management function that governs decentralised or highly distributed change requests	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	
	Business continuity & disaster recovery	Do you have a cyber specific incident recovery plan	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
		Do you have a cyber specific incident Business Continuity Plan (BCP)	No	Yes	No	No	No	No	Yes	No	No
	Vulnerability scanning	Do you have a tool for vulnerability scanning	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
		Do you use any of the following services:									

Organisation / Capability		Imperial College Healthcare NHS Trust	Chelsea and Westminster Hospital NHS Foundation Trust	London North West University Healthcare NHS Trust	The Hillingdon Hospitals NHS Foundation Trust	Central and North West London NHS Foundation Trust	West London NHS Trust	Central London Community Healthcare NHS Trust	North West London ICB	Primary Care
	a. NHSE Vulnerability Monitoring Service (VMS)	Yes	No	No	Yes	No	Yes	No	No	No
	b. BitSight	Yes	Yes	Yes	Yes	Yes	No	No	No	No
	c. MDE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Final

## Abbreviations

Table 30

Abbreviation	Meaning
3LOD	Three Lines of Defence
AI	Artificial Intelligence
ALARP	As little as Reasonably Possible
ALB	Arm's length bodies
AM	Anti-Malware
AV	Anti-Virus
BAF	Board Assurance Framework
BAU	Business as Usual
BCP	Business Continuity Plan
CAF	Cyber Assessment Framework
CAN	Cyber Associates Network
CCA	Civil Contingencies Act
CCG	Clinical commissioning groups
CCS	Care Co-ordination Solution
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, and Availability
CIP	Cyber Improvement Programme
CIRE	Cyber Incident Response Exercise
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISP	Cyber Security Information Sharing Partnership
CLHC	Central London Community Healthcare NHS Trust
CMDB	Central Management Database
CNWL	Central and North West London NHS Foundation Trust
CQC	Care Quality Commission
CSOC	Cyber Security Operations Centre
CSU	Commissioning Support Units
CVSS	Common Vulnerability Scoring System
DHSC	Department of Health and Social Care
DNS	Domain Name System
DPA18	Data Protection Act 2018
DPO	Data Protection Officer
DSIT	Department for Science, Innovation and Technology
DSPT	Data Security Protection Toolkit
EoL	End of Life
EoVS	End of Vendor Support
EPR	Electronic Patient Records
GDPR	General Data Protection Regulation
GP	General Practitioner

Abbreviation	Meaning
HSE	Health Service Executive
IAM	Identity and Access Management
ICB	Integrated Care Board
ICH	Imperial College Healthcare
ICP	Integrated Care Partnership
ICS	Integrated Care System
IG	Information Governance
IGP	Indicator of Good Practise
InfoSec	Information Security
IoC	Indicators of Compromise
IT	Information Technology
KPI	Key Performance Indicators
MDE	Microsoft Defender for Endpoint
MDR	Managed Detection and Response
MFA	Multi-Factor Authentication
MTTA	Mean Time to Assignment
MTTD	Mean Time to Detect
MTTF	Mean Time to Fulfilment
MTTT	Mean Time to Triage
MVP	Minimum Viable Product
NCSC	National Cyber Security Centre
NDR	Network Detection and Response
NHS	National Health Service
NHSE	National Health Service - England
NIS	Network and Information Systems Regulations
NW	North West
OES	Operators of Essential Service
PAM	Privileged Access Management
PDNS	Protective Domain Name Service
PESTILE	Political, Economic, Social, Technological, Legal and Environmental
RACI	Responsible, Accountable, Consulted, and Informed
RAG	Red, Amber, and Green
RBAC	Role-Based Access Control
RPA	Robotic Process Automation
RSL	Regional Security Lead
SBD	Secure by Design
SIEM	Security information and event management
SIRO	Senior Information Risk Officer
SLA	Service Level Agreement
SOC	Security Operations Centre
TPRM	Third-Party Risk Management
UEBA	User and Entity Behaviour Analytics
VfM	Value for Money

Abbreviation	Meaning
VM	Vulnerability Management
VMS	Vulnerability Management Service
VPN	Virtual Private Network
WAF	Web Application Firewall
WLNT	West London NHS Trust
WSIC	Whole Systems Integrated Care

Final draft

## Document control

This document will be reviewed on a yearly basis, or when a change is identified due to regulation or business activities. All changes will be communicated.

Version	Date of Creation	Approver	Role
0.1 – Initial Creation	27 September 2024	Kathy Lanceley	ICH CISO and Deputy SIRO
0.2 – Update following initial review	3 October 2024	Kathy Lanceley	ICH CISO and Deputy SIRO
0.3 – Update following Trust Cyber Security Strategy Workshop	8 November 2024	Kathy Lanceley	ICH CISO and Deputy SIRO
0.4 – Update following review	11 December 2024	Kathy Lanceley	ICH CISO and Deputy SIRO