NHS Blood and Transplant

NHS Blood and Transplant Board Meeting
24 May 2018

General Data Protection Regulation (GDPR) Compliance Position

1. Status – Official

2. Executive Summary

New EU data protection rules, known as the General Data Protection Regulations (GDPR), come into force on 25 May 2018. These rules place significant new obligations on all organisations that process personal data either a data controller or under contract as a data processor. In particular, organisations are required to identify what personal data is held and to document the lawful basis on which that data is held and processed. The regulations also give individuals (data subjects) about whom organisations hold personal data, rights to greater control over the use of that data, particularly where their consent is relied upon as the lawful basis for processing.

NHSBT staff completed a high-level gap analysis against GDPR compliance in the autumn of 2017 and this was submitted to the November 2017 NHSBT Board meeting. The January Transformation Programme Board (TPB) approved the request to manage the action plan resulting from the gap analysis as a project. These actions were mapped into nine project workstreams.

It was also agreed that a RAG (Red, Amber, Green) rating would be used to assess whether each of the workstreams had achieved baseline compliance with the regulations as at the 25 May 2018. Baseline compliance is defined as meeting the core GDPR requirement based upon the guidance currently available and our understanding of it. At this time, of the nine workstreams; seven are rating as green and two are rated as amber. Significant activity will remain post 25 May to ensure NHSBT maintains GDPR compliance. NHSBT's Information Governance (IG) team has also completed the Information Commissioner's Office (ICO) online self-assessment tool which has provided a Green rating.

3. Action Requested

The Board are requested to note the compliance position outlined in this paper.

4. Purpose of the paper

The paper outlines the baseline compliance position against each of the GDPR workstreams as at the 25 May 2018, and seeks the Board's acknowledgement of this position. The paper also briefly outlines the key next steps to ensure and maintain compliance.

5. Background

New data protection rules, known as GDPR will become law 25 May 2018. In November 2017 the Board received a paper outlining a high level NHSBT gap analysis. In January 2018 the TPB approved the management of the GDPR action plan as a project. The initial high-level gap analysis was written against each of the GDPR requirements. Once the project was established those key actions were converted into the nine workstreams outlined in this paper. The GDPR project board

has reviewed and signed off the RAG rating for each of the workstreams, prior to submission to NHSBT Board, based upon the evidence submitted by the various workstreams and confirmation of the actions taken. The project team completed the ICO on-line GDPR self-assessment tool and was rated as Green.

6. Baseline compliance RAG rating

The following criteria were agreed by the project board and used to establish the RAG rating for each workstream:

	Deliverable meets core GDPR requirement, with accepted activity and risk post 25 May
	Deliverable meets core GDPR requirement as far as current guidance allows and/or carries a level of risk with critical activity identified post 25 May
	Deliverable behind schedule to be GDPR compliant by 25 May, carries a level of risk with critical activity identified post 25 May

7. Overview of RAG ratings for the workstreams

The table below provides an overview of the baseline compliance RAG ratings, as at the 25 May, for each of the nine workstreams, along with the agreed pre and post 25 May actions, which have been signed off by the GDPR Project Board.

Workstream	Key Deliverable & Approach (Pre / Post 25 May)	Compliance RAG
Information We Hold	**Pre**: Information Asset (IA) Register re-drafted in-line with GDPR, lawful basis identified and documented for all assets, register fully populated for all critical assets **Post**: Minor assets populated, embed role of IA Owners	
Privacy Notices	**Pre**: Single Organisational Notice updated and published in-line with GDPR, referencing directorate sub notices	
Subject Access Requests	**Pre:** MPD11 Subject Access Requests updated in-line with GDPR **Post:** Monitoring established	
Lawful basis	**Pre:** All instances of processing data reviewed and alternative/appropriate lawful basis identified, actions completed to make required identified changes **Post:** System changes (Organ Donor Register, Information Services) scheduled, complete leaflet and welcome pack amendments	
Breaches	**Pre:** Review of current processes; issue of Quick Reference Guide (QRG) regarding breaches	
Data Protection by Design	**Pre:** Interim utilisation of existing governance until ICO/IGA guidance is released **Post:** Core Information Governance policies updated, Information Governance Assessment forms updated and new approach embedded	
Data Protection Officer	**Pre:** Appoint a Data Protection Officer within the organisation **Post:** Update Job Description, attend any necessary training, and review allocation of Data Protection Officer role	
Contracts	**Pre:** Following Crown Commercial Service (CCS) Policy Procurement Note; Notify suppliers of potential GDPR changes, categorise contracts and waivers, send compliance questionnaires out for high risk contracts. Issue new GDPR compliant CCS T&Cs for all new supplier contracts. **Post:** Assess GDPR compliance of contracts (based on returns) & amend in priority order**.** Implement Department of Health policy note once issued. For data sharing agreements and third-party agreements when due for update amend to reflect GDPR.	
Comms & Training	**Pre:** Delivery of GDPR Awareness campaign and specific GDPR role training **Post:** Further development of training and awareness packages	

8. Detailed workstream overviews

Outlined below are details of each of the workstreams, with an overview of the baseline compliance work agreed by the project board as at the 25 May, and the identified post 25 May actions.

*8.1 Information we hold:*Baseline compliance agreed as: re-drafted IA register in-line with GDPR; re-defined and communicated role of the IA Owner (IAO); identified and documented lawful basis for processing information against all of the IAs (254), and fully populated register for all the critical assets (53). All these actions have been completed with the exception of the full population of the critical assets as at the meeting of the project board on 14 May. This workstream has been provisionally signed off as Green until the outstanding action is complete, which will be before the NHSBT Board 24 May. Post 25 May the focus of work will be on: the full population of the remainder of the register; further guidance/training to IAOs, and the development/implementation of an on-going maintenance process for the register.

8.2 Privacy notices:
Baseline compliance agreed as updated organisational privacy notice in-line with the new GDPR requirements, published on the NHSBT Website, and linked to updated directorate sub-notices. All actions have been completed and the project board have signed off this workstream as Green. There is no current post 25 May activity identified. An update or review of the privacy notices would be triggered if new services are introduced or existing services are changed.

8.3 Subject Access Requests (SARs):
The project team established that NHSBT was already compliant with most of the GDPR requirements regarding SARs as existing data protection legislation in England includes this. Baseline compliance agreed as an updated MPD11 to reflect the GDPR changes. This action has been completed and the project board has signed off the workstream as Green. Post 25 May activity includes continued adherence to the MPD and GDPR requirements and on-going monitoring of compliance.

8.4 Lawful Basis:
The project team worked with representatives from each of the operational directorates to establish all instances where consent, both explicit and implicit, was being taken to process data. This was then assessed and an alternative/appropriate lawful basis to process the data was then identified. This is important as, under GDPR, consent is seen as the weakest basis for processing data and affords data subjects additional rights. If there is an alternative lawful basis for processing data, such as an overriding public duty, some rights such as the 'right to be forgotten' do not apply. In NHSBT only one instance of using consent as the lawful basis for processing data remains; for the Organ Donor Register (ODR). Detailed action plans were developed for each of the operational directorates to implement the changes required, which included updating leaflets, websites, T&Cs, and system changes to remove unnecessary or inappropriate references to consent to process data.

The agreed post 25 May actions relate to update of some low risk leaflets, such as those which refer to the DPA rather than GDPR, and the identified system changes

for the ODR and ODT information services. An interim solution, an insert, has been agreed for the welcome packs. The welcome packs and low risk leaflets will be updated in-line with their normal update schedule in order to reduce the financial and business impact. All actions have been planned, agreed, and scheduled. The project board took the view that the approach is low risk and we are further along regarding the system changes than originally anticipated. The consent working group, which is broader than just GDPR, had detailed oversight of this workstream and signed off the action plans and suggested RAG rating prior to submission to the project board. The project board approved these actions as achieving baseline compliance for GDPR as at the 25 May and signed the workstream off as Green. Post 25 May activity to complete the outstanding actions has all been agreed and scheduled and therefore has been identified as low risk to GDPR compliance.

8.5 Breaches:
The project team assessed the breach requirements of GDPR, alongside the breach requirements of the new Directive on security of network and information systems (the NIS Directive), to establish what changes were required in NHSBT, and to ensure there would be no duplicate action. NHSBT's processes already meet the GDPR requirement to report breaches within 72 hours. The project board agreed the additional activity of producing a Quick Reference Guide for staff pre- 25 May and fully embedding into the Quality Management System (QMS) post 25 May. The pre- 25 May activity has been completed and the project board signed off this workstream as Green.

8.6 Data Protection by Design:
The ability to fully comply with this workstream is dependent on the release of final guidance from the ICO and from the Information Governance Alliance neither of which have yet been released. Post 25 May, and upon the release of this guidance and templates, there will be significant activity to update all the relevant NHSBT MPDs and assessment forms, link with business processes in Quality Assurance (QA), Business Transformation Service (BTS) and Procurement, and to fully embed the new processes across NHSBT. The project board has agreed an interim position to mitigate the delay in guidance using existing Data Protection based assessment mechanisms to assess requirements against GDPR until business processes can be updated, and to enforce that current Information Governance Assessments (IGAs) are mandatory in relevant business areas (QA, BTS, Procurement) to ensure IG have visibility of any data related requirements. The project board signed this workstream off as Amber as a result of the relative lack of guidance in this area.

8.7 Data Protection Officer (DPO):
The Chief Digital Officer, who is the Senior Information Risk Owner for NHSBT, has been identified as the DPO for NHSBT. The current ICO guidance states appointing the Head of IT to the role of DPO as a conflict of interest, however, the ICO criteria for the DPO role also highly restricts potential candidates. Engagement with other European Blood Services and NHS Trusts, has shown a range of approaches being adopted, highlighting the challenge to meet this requirement. The DPO has therefore been appointed with the accepted risk that the appointment is potentially in conflict with published guidance. The Executive Team were supportive of the appointment subject to ongoing review. The project board signed off this workstream

as Green. Post 25 May activity will include updating the Chief Digital Officer's Job Description, and reviewing the appointment to consider any alternatives.

8.8 Contracts:
The Crown Commercial Service (CCS) issued a Policy Procurement Note (PPN) directing relevant organisations to write to all suppliers informing them of GDPR and the potential change to contracts in-line with GDPR. They also issued updated T&Cs for new contracts, and did direct that an indemnity clause, to match the maximum fines available from the ICO be added to all contracts. Baseline compliance was agreed as: write to all suppliers using the issued standard letter; categorise all contracts and waivers to identify the high-risk contracts/waivers based on the volume of personal data processed; send the high-risk contract suppliers an audit form to assess readiness for GDPR. The basis for the audit form was provided by Louise Fullwood. All these actions have been completed. With regards to the indemnity clause, the Department of Health and Social Care have informed us that they will be issuing an updated PPN clarifying their different position regarding the indemnity clauses. As a result of this the project board signed this workstream off as Amber. Post 25 May there will be significant work to interpret and respond to the supplier returns, initiate and implement contract changes, issue the standard T&Cs for all new contracts, review and update any third-party agreements and data sharing agreements in-line with GDPR as and when they are due for renewal.

8.9 Communications and Training:
The project team has produced and released a GDPR awareness campaign which included: a GDPR Awareness Module on the SHINE Academy; GDPR Frequently Asked Questions; 10 things to know about GDPR; and a breaches Quick Reference Guide. Post 25 May activity will focus on a 'GDPR is now live' message and further training for Information Asset Owners, project board members and other identified individuals, and updating relevant mandatory training for all staff. The project board signed off this workstream as Green.

9. Approval

The Board is asked to note the baseline compliance position outlined in this paper.

10. Next Steps

The May TPB approved a change request to extend the scope of the current project beyond the 25 May to facilitate the development of a business case focusing on outlining the detailed work plan, deliverables, and required resources for the predicted 6 months remaining intensive GDPR work.

Author
Louise Cheung,
AD, Governance & Clinical Effectiveness
May 2018

Responsible Directors
Aaron Powell, Chief Digital Officer
Gail Miflin, Medical & Research Director