NHS Blood and Transplant Board Meeting
30 November 2017

General Data Protection Regulation (GDPR) Gap Analysis

1. Status – Public

2. Executive Summary

New data protection rules, known as the General Data Protection Regulations (GDPR) will become law in May 2018. Following a high-level gap analysis, this paper outlines the key gaps currently within NHS Blood and Transplant (NHSBT) and the proposed actions to address the identified gaps. The headline gaps/areas for action for NHSBT relate to:

- The Information Asset Owner (IAO) Register
- Privacy notices
- Consent
- Sharing data outside NHSBT
- Information Governance (IG) policies and procedures

In addition, some work is needed to raise awareness of the new regulations with NHSBT. At November Executive Team (ET) Meeting it was agreed this would be managed as a TPB project, further detail of the gaps and required actions to ensure compliance will be obtained through delivery of the project.

3. Action Requested

The GAC are requested to note the outcome of the gap analysis prior to submission to the November Board.

4. Purpose of the paper

New data protection rules, known as GDPR will become law in May 2018. They will come into force across EU member states and will complement the 1995 EU Directive on which the current 1998 Data Protection Act (DPA) is based. The GAC has previously received a paper outlining the key requirements of GDPR and the key potential impacts for NHSBT. This paper includes the summary outcome of the high-level gap analysis, the full high-level gap analysis and proposed actions are available on request. At November ET it was agreed this would be managed as a TPB project, further detail of the gaps and required actions to ensure compliance will be obtained through delivery of the project. This paper will be submitted to the November Board for approval.

5. Gap Analysis

The gap analysis was led by the Assistant Director, Governance and Clinical Effectiveness, and supported by the Head of Information Security and representatives from each of the operational business units and group service directorates. Current NHSBT practice was assessed against the identified GDPR requirements to identify the gaps. The full gap analysis outcomes and the associated actions are available on request. This paper will provide an overview of the key headline gaps to address and priority actions for NHSBT. It is worth noting that the Information Commissioner's Office (ICO) continue to release guidance as to how the new regulations relate to organisations like NHSBT and how best to ensure compliance. This guidance will be released up to, and beyond, 25 May 2018 when

GDPR comes into force, and will mean NHSBT may be required to continue to make further changes to current practice after that date.

6. Key headlines gaps and associated priority actions

6.1 Information Asset Register and Owner:
A key requirement of GDPR is to understand what data NHSBT holds. NHSBT is required to document what personal data it holds, where it came from, and who it is shared with. An effective Information Asset (IA) register should document this and each IA should have a designated owner (IAO). Currently NHSBT's IA register is not up to date, and does not meet the full requirements of GDPR. Within NHSBT the role of IAO is not clearly defined and understood. A priority action is to address this issue. The IA register will be re-designed to ensure it fully meets the requirements of GDPR and will be linked, via IT, to the information held on employees. The role of the IAO will also be fully defined and training delivered to all IAOs.

6.2 Privacy notices:
GDPR increases the amount of information that must be provided to data subjects when collecting their personal data, to ensure processing activities are fair and transparent. Privacy notices in NHSBT do not currently meet the full requirements of GDPR, some of the gaps identified are due to these being new requirements under GDPR. NHSBT has a generic privacy notice on the website and privacy notices for blood donation, Tissue Eye Services (TES) and the Organ Donation Register (ODR). The gaps in the current privacy notices include:

- Doesn't state right to withdraw consent.
- It states there will be a charge for provision of personal data.
- The references to categories of personal data will be out of date due to the updated categories.
- Doesn't make specific references to children, people with special needs, or the services NHSBT provides or any other privacy notices in NHSBT.

Privacy notices will be key to ensuring donors, staff, and patients understand why NHSBT collects data, how it is stored and who it is shared with, so where appropriate they can provide consent to processing of data. New privacy notices, fully compliant with GDPR, will be developed and in use by the end of February 2018. NHSBT is not required to retrospectively contact people to inform them there has been a change in the privacy notices, however, we will inform them there has been a change to the privacy notices when they for example, next donate blood.

6.3 Consent:

6.3.1 GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms. NHSBT will need active and more granular opt-in methods (with "soft opt-in" such as not ticking an opt-out box, no longer sufficing), good records of consent, and simple easy-to-access ways for people to withdraw consent, currently this can't be supported by NHSBT's systems, however, it will be built into system changes and/or re-design such as the Core Systems Modernisation (CSM). The changes reflect a more dynamic idea of consent: consent as an organic, ongoing and actively managed choice, and not simply a one-off compliance box to tick and file

away. Consent is a priority area for NHSBT and will be a complex area to fully address the challenges of GDPR. A more comprehensive list of the gaps regarding consent is contained in appendix one, however, some examples include:

- Use of assumed consent for data sharing
- Information not provided on how to withdraw consent
- Consent statements used which include a list of consent statements and only one consent signature for all
- Consent taken as part of Terms and Conditions (T&Cs)

6.3.2 Currently on NHSBT's IA register we document the lawful basis for which we share data; one of which could be on the lawful basis of consent. The ICO has issued guidance outlining that sharing data, using the lawful basis of consent, will be one of the most challenging for public organisations such as the NHS. This is due to two main reasons; firstly, consent to share data cannot be a condition of service (consent must be freely given). Secondly, there should be a balance of power when consent is given, therefore, public authorities, employers and other organisations in a position of power over individuals, should avoid over-relying on consent when other exemptions are available. What this means in practice for NHSBT is we will review the internally documented lawful basis for sharing data, with a view to potentially sharing data on the lawful basis of one of the following reasons as opposed to its historical basis of consent:

- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller

There are far greater restrictions and requirements when sharing data based on the lawful basis of consent.

6.3.3 A group will be established to review consent across NHSBT, and will consider and agree action to meet the requirements of GDPR, Caldicott 3 and outstanding actions as a result of the new Human Tissue Authority (HTA) Code of Practice. The group will be led by the Assistant Director (AD) Governance & clinical effectiveness and will include; the Data Protection Officer, AD of Quality Assurance (QA) and Regulatory compliance, Programme Manager (Big-Data), Head of information Security, Head of IG, Consultant in Transfusion Medicine, Clinical Support Team Consultant, DTS Professional Nursing Lead, AD, Education and Governance (ODT). All relevant processing of data will be reviewed to establish if consent is the most appropriate lawful basis to process the data, as described above. If consent is not the most appropriate that will be clearly articulated and documented on the IAO register, if it is the most appropriate, the gaps identified will be addressed to ensure compliance with GDPR.

6.3.4 Due to the complexity of NHSBT and the use of many different IT and paper systems it will not be possible to build into all current systems the ability to withdraw consent. As outlined above this will be built into new systems, but will remain a gap when the regulation takes effect in May 2018. The ICO

have indicated an understanding of the challenges for organisations to ensure full compliance by May 2018, and that regulatory action is unlikely to be taken against organisations in the short-term if gaps remain, but rather the key is that the organisation understands its gaps and has actions in place to address them.

6.4 Sharing of data outside NHSBT:

6.4.1 There are greater requirements placed on sharing data outside of NHSBT if it is not anonymised. All instances of sharing data outside NHSBT will be reviewed to establish whether or not identifiable data could in fact be shared in anonymised form. GDPR requires that where data is shared internationally, it is agreed who is the lead data protection authority; currently in NHSBT we haven't agreed this with other organisations. It is also required that when sharing information with other organisations NHSBT is assured, via its data sharing agreements, that the data is being managed in-line with GDPR requirements.

6.4.2 Currently in NHSBT we have data sharing agreements/contracts in place which don't currently meet the requirements of GDPR, due to additional expectations as part of GDPR. For example, in Therapeutic Apheresis Services (TAS), diagnostic results sharing with Hospitals via Sp-ICE (Specialist Services Electronic Reporting System). We also have instances where identifiable data is being shared outside NHSBT with other organisations in the UK, in Europe, and in the US, for which there are no specific data sharing agreements, rather T&Cs that organisations sign up to. An example of this includes data shared with Public Health England. Where data sharing agreements/contract are in place for sharing data, they do not meet the full requirements of GDPR, therefore, an action is to update all to meet the requirements. It is also worth noting NHS Organisations will also be expected to meet this requirement and therefore there is the potential for there to be a significant pull on NHSBT time to provide statements to NHS Trusts for inclusion in data sharing agreements where they share identifiable data with NHSBT.

6.4.3 Where data is shared internationally the lead data protection authority will be established and agreed. All instances where data sharing agreements need to be in place will be identified; and developed, and where they are covered by other arrangements this will be clearly articulated and assessed to ensure compliance with GDPR. The contracts for review will be prioritised and all will be reviewed and updated to ensure full compliance with GDPR.

6.5 Information Governance (IG) policies and procedures:
Up to date IG policies and procedures will be vital in ensuring compliance with GDPR. All will be reviewed and updated introduction of GDPR in May 2018.

6.6 Awareness raising:
Awareness of GDPR is key to ensuring all staff across NHSBT are compliant at all times. An awareness campaign has already commenced and includes/will include

articles in team talk, awareness training via Shine for all users, screensavers, and FAQs regarding general IG.

7. Operational impacts

7.1 The changes to Subject Access Requests (SARs) has the potential to have a significant operational impact on NHSBT. In the last 12 months NHSBT has processed 15 requests across customer services and HR, it is likely the number of these requests will increase (as NHSBT no longer has a right to charge for responding to requests), leading to an increased call on resources to access and provide this information. The changes to the type of information that could be requested will provide some challenges to NHSBT. We could be asked to provide information outlining who has accessed their record. Currently we don't have the ability to provide that information comprehensively, due to not regularly auditing our systems for this information, not having the ability to audit electronic systems due to the way they are set up, and/or having paper records. The ability to audit electronic systems in this way in the future is being built into our new electronic systems and will enable us to provide this information more easily.

7.2 Currently we are not set up to be able to meet the requirement of the right to be forgotten. Whilst this is predominantly aimed at non-NHS organisations, such as social media companies, and search engines, there will be some expectations on NHSBT, the detail of which is yet to be fully clarified. This right is being considered as part of the development of new IT systems, however, we will need to clear what information we need to hold on to due to a safety/legal requirement. This requirement would override the right to be forgotten, however, it would need to be clearly articulated to the data subject.

7.3 Due to GDPR NHS organisations across the UK will be seeking to have data sharing agreements in place with NHSBT, and/or update current agreements, where they share identifiable data with ourselves. This action has the potentially to cause a significant amount of work for NHSBT to meet these requirements, both from an operational perspective in liaising with the Hospital, and from an Information Governance/Caldicott perspective in reviewing them and signing them off. Within NHSBT we will look to develop some standard responses for requests regarding how we manage and safeguard the data, and will continue to explore with NHS Digital the development of a NHS wide template data sharing agreement.

7.4 The changes identified as part of the work to ensure compliance with consent have the potential to have an operational impact on services in practice. Currently this impact is unknown, however, we need to mindful during the work regarding consent of any operational impacts and where possible minimise them.

Authors
Louise Cheung,
AD, Governance & Clinical Effectiveness
Barry Richardson,
Head of Information Security
November 2017

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