NHS Blood and Transplant

NHSBT Board
July 28, 2016

Data Security and Consent for Data Sharing

1. Status – Public

2. Executive Summary

On July 6, two new reports on data security and sharing were published, namely the National Data Guardian's (Dame Fiona Caldicott) *Review of Data Security, Consent and Opt-Outs* and the Care Quality Commission *Safe Data, Safe Care: Data Security Review*. The former recommends ten new 'Data Security Standards' for health and social care information. The latter report overlaps the former considerably with the addition of proposals to strengthen audit and validation and to make data security a part of the CQC assessment framework. The NDG report also recommends a new consent/opt-out model for the sharing of health and social care information where 'people should be able to opt out from personal confidential data being used beyond their own direct care'.

This report provides an initial assessment of NHS Blood and Transplant's position in respect of the proposed new data security standards and a very early indication of the implications of the opt-out proposal on NHSBT's operations.

3. Action Requested

The Board is asked to:

- **Note the anticipated NHSBT position in relation to the National Data Guardian and Care Quality Commission data security and sharing reports;**
- **Identify any particular concerns for inclusion in the consultation response in early September 2016.**

4. Purpose of the paper

On July 6, two new reports on data security and sharing were published, namely the National Data Guardian's (Dame Fiona Caldicott) *Review of Data Security, Consent and Opt-Outs* and the Care Quality Commission *Safe Data, Safe Care: Data Security Review*. The former recommends ten new 'Data Security Standards' for health and social care information designed 'to be simple for people to understand and follow', 'support rather than inhibit data sharing' and 'to be fit for the future, where personal confidential data will be stored digitally rather than in filing cabinets, and health and social care will be integrated'. The latter report overlaps the former considerably with the

addition of proposals to strengthen audit and validation and to make data security a part of the CQC assessment framework.

The NDG report also recommends a new consent/opt-out model for the sharing of health and social care information where 'people should be able to opt out from personal confidential data being used beyond their own direct care' although the format of the opt-out question is not specified.
This report provides an initial assessment of NHS Blood and Transplant's position in respect of the proposed new data security standards and a very early indication of the implications of the opt-out proposal on NHSBT's operations. A formal NHSBT response to the Department of Health consultation questionnaire on these reports will be drafted during August for review and sign-off by both the Caldicott Guardian (the Medical and Research Director) and Senior Information Risk Owner (the Chief Digital Officer) by 7th September 2016.

5. Data Security Standards

5.1. The proposed 10 new data security standards are grouped under three leadership principles which are:

- Leadership Obligation 1: *People:* Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.
- Leadership Obligation 2: *Process:* Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
- Leadership Obligation 3: *Technology*: Ensure technology is secure and up-to-date.

The report notes the importance of having an effective Senior Information Risk Owner (SIRO) and Caldicott Guardian but emphasises that data security is a whole Board responsibility. It is in this context that Non-Executive Directors of both the Department of Health and NHS Digital wrote to NHSBT's own NEDs on 6th July on the publication of these reports.

5.2. Leadership obligation 1, relating to people, proposes three data security standards primarily concerning the understanding of these obligations and standards and training. They are:

- *Data Security Standard 1.* All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
- *Data Security Standard 2.* All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

- *Data Security Standard 3.* All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

5.3. All NHSBT staff are informed of their obligations in relation to information security both in the NHSBT IT Acceptable Use Policy and in the Comprehensive Information Security Policy (POL10). Online training on information governance is part of the mandatory training requirement of all staff and is required to be completed annually. It includes a short test. It is likely that NHSBT's own training and policies will need review in light of the new data security standards. It is unclear when or how the HSCIC IG toolkit will be upgraded to meet the new training and test requirements.

5.4. Leadership obligation 2 relates to the organisation's processes to prevent and respond to information security breaches. Each of the four recommendations under this obligation are addressed below.

5.5. *Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.*

5.6. NHSBT provides role-based access to most of its core systems, especially those containing patient sensitive data. Access to these systems is provided on confirmation from the relevant line manager that such access is required. Removal of access to these systems when an individual changes role is dependent upon notification from the person's line manager and regular review by the Information Asset Owners for each system. It has been noted that these processes could be improved and they are subject to review. While NHSBT's core applications support logging of access to confidential data at the application level, some of our legacy systems do not currently support logging of access at the individual record level. New systems are being designed to ensure that this level of logging is supported.

5.7. Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

5.8. All of NHSBT's processes are reviewed according to their review cycle which is recorded in the Q-Pulse system, at least annually. In addition, security breaches are reviewed quarterly by the Information Governance Committee and are presented annually to the Governance and Audit Committee in the Information Governance Annual Report.

5.9. Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is

taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

5.10. NHSBT uses firewalls to protect against cyber attacks. A business case to replace these firewalls with new firewalls which include intrusion detection and prevention systems was approved by the Board in May 2016 and these will be implemented by the end of 2016. CareCERT security notifications are provided to the SIRO and Head of Information Security and action confirmed to the Department of Health on receipt. NHSBT classifies information security incidents according to the current HSCIC (now NHS Digital) Information Governance toolkit guidance with the most serious incidents requiring notification to the DH, via the SIRO, within 24 hours.

5.11. Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

5.12. NHSBT's information systems business continuity plans have recently been updated following the move of the data centres and these are tested annually. These tests do not, however, include specific tests relating data breaches or near misses. Business continuity plans and tests will need to be reviewed in light of this proposed standard.

5.13. The fundamental principle behind the third leadership obligation which relates specifically to technology is that systems are up-to-date and therefore less vulnerable to attack. The three recommendations under this obligation are as follows.

5.14. Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

5.15. NHSBT has embarked on a major technology transformation programme to address its use of unsupported systems and software. To date, a number of systems rely on out-of-date components or are accessible only using internet browsers which are no longer supported. This is being addressed by the Core Systems Modernisation, ODT Hub and Desktop Modernisation programmes. A new strategic objective has been added to the strategic plan to reduce the number of unsupported systems in use. It is likely, however, that this will take at least three years to achieve. It is not clear that any additional funding will be available to support NHS organisations to meet this standard more quickly.

5.16. Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

5.17. NHSBT has a comprehensive Information Security policy (POL10). This was comprehensively reviewed in 2015 and launched in March 2016. It will be reviewed annually.

5.18. Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

5.19. NHSBT's contracts with IT suppliers all include clauses designed to ensure accountability for the use of personal confidential data. Key suppliers are audited by Quality Assurance to ensure that they meet their obligations and have adequate protections and processes in place. The text of the NDG report suggests that model clauses should be inserted into all standard NHS contract terms which are already used by NHSBT.

6. Consent for data sharing and opt-outs

6.1. The National Data Guardian's report addresses four types of use of patient data – data that is used for 'direct care' purposes; use of personalised data for purposes beyond direct care; use of anonymised data and use of data for specified research projects.

6.2. As regards the use of data for direct care purposes the report notes that there is a public expectation that data will be shared for these purposes and that data sharing is important to avoid errors. The report therefore recommends that data should be shared for direct care purposes between health and social care organisations, but that this relates only to *relevant information*, with sharing of the whole record requiring explicit consent, and that fair processing information should be available so that there are no surprises for patients as to who has access to their data. This recommendation may be more relaxed than NHSBT's current operational practice in some areas where, for example, explicit consent is sought for sharing of transplant patient information even when such sharing is necessary to support waiting list registration.

6.3. The NDG reports notes that its review had heard that 'high quality, linked data was required for running the health and social care system and improving the safety and quality of care, but that for the majority of purposes personal confidential data was not required.' In these cases, it is noted that the NHS Constitution provides a right for patients to request that their personal confidential data is not shared but that there is no easy mechanism for them to do so currently. The report therefore proposes that every organisation implements an opt-out model of consent for the sharing of personal confidential data.

6.4. For NHSBT, the principle impact of this is that existing consent provisions will need to be reviewed as many have been developed on the principle of opting-in, rather than opting-out. The opt-out principle will need to be designed in to all future systems. In practice, NHSBT's current data sharing consent measures are likely to be more restrictive

than the guidance requires and are designed to reflect our legal obligations under the Data Protection Act and common law.

6.5. In relation to anonymised data the report is clear that the majority of uses beyond direct patient care do not require confidential personal data. On that basis, the report proposes more widespread use of anonymised data and a process in which personal confidential data is provided to HSCIC (NHS Digital) to de-identify and anonymise it ready for sharing. It is recommended that the Information Commissioner's Office Anonymisation Code is adopted for this process and that stronger penalties should be introduced for the misuse of anonymised data, including criminal sanctions for the deliberate or negligent re-identification of individuals from anonymised data. With these safeguards in place the report suggests that the data sharing opt-out need not apply to anonymised data.

6.6. From an NHSBT perspective, more widespread availability of anonymised data via NHS Digital may present a significant opportunity if, for example, it is at a level that allows us to identify use of blood in hospitals. It is not yet clear whether there will be any requirement for NHSBT to share its own extensive data sets with NHS Digital for anonymisation.

6.7. The NDG report also proposes that people should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. This is consistent with NHSBT's existing approach to research participation where explicit consent is requested of participants where person specific data is to be shared or where genomic results could result in de-anonymisation.

7. Next Steps

7.1. An action plan is in place to collate responses to the DH consultation document (available on request) by 17th August. This will ensure appropriate time for reviews before formal submission on 7th September.

7.2. A Task and Finish group will also be put together to identify those actions that can be taken now to address any risks of non-compliance, pending longer term technology upgrades and to work through the recommendations around consent, data sharing and opt-outs in more detail. This Task and Finish group will be led by Dr Gail Miflin.

Author
Aaron Powell, Chief Digital Officer

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

NED Scrutiny
None