Blood Stocks Management Scheme

Blood Stocks Management Scheme Information Governance Arrangements

Blood Stocks Management Scheme

Blood Stocks Management Scheme
Information Governance Arrangements

Date Created 28/05/2021 *Date ratified by Steering group 15/06/2021* *Date Published 07/07/2021*

TABLE OF CONTENTS

1. PURPOSE OF THE DOCUMENT

The purpose of this document is to outline the Information Governance arrangements adopted by the Blood Stocks Management Scheme (BSMS) to ensure the ongoing, appropriate access to, and use of, the data acquired through and held within the BSMS data management system. The BSMS system currently collects data on stock and wastage from hospitals via VANESA, the BSMS data management system. Blood Services extract and transfer stock and wastage data via an automated process. Data is also gathered via surveys and filed in a secure storage area. Outputs are produced from any part of the system.

UK Blood Services in England, Wales and Northern Ireland together with the hospitals they serve participate in the Blood Stocks Management Scheme.

Some of the relevant legislation, policies and standards pertinent to these arrangements are listed in Annex A.

2. CONTEXT

The origin of the BSMS development lies in the English 1984 Health Circular asking hospitals to establish accurate record keeping in relation to blood stock and wastage management. In 1997 the DoH/ NHSBT launched an initiative to promote greater compliance with HC (84)7. The National Blood Stocks project was established in 1997 as a collaborative venture between NHSBT and the hospital sector to understand and achieve

improvements in blood stock management. The results of this project were taken forward as the BSMS which was implemented in 2001 and administered by NHSBT.

Participation in the BSMS was a recommendation in HSC 2002/09. Better Blood Transfusion II. Participation in the BSMS was extended to the UK Blood Services and the Republic of Ireland. Currently Blood Services in England, Wales and Northern Ireland participate in the BSMS.

The BSMS system is designed to meet ongoing information needs in relation to the demand for blood components and the stock available to meet that demand and can provide information in support of hospital and Blood Service objectives, namely: The optimisation of blood component stock management.

3. DATA FLOWS

All data is processed and stored in accordance with NHSBT information security policies and confidentiality guidelines and is subject to NHSBT corporate management.

The relevant data flows are illustrated in Figure 1.

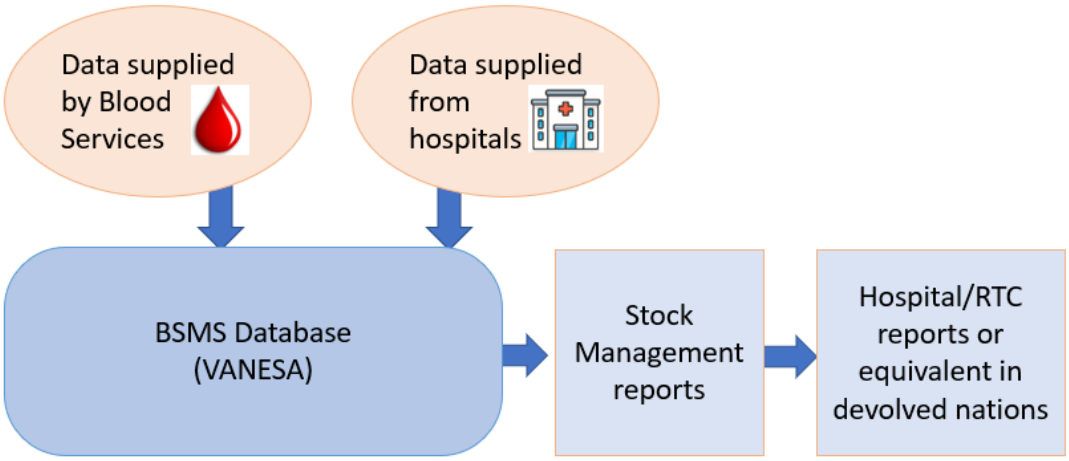

Fig 1. BSMS Data Flow

4. BSMS INFORMATION GOVERNANCE

The role of BSMS is to ensure appropriate guardianship of the data held within the BSMS system by applying appropriate access controls and maintaining a rigorous approach to release of data and /or reports. The following sections describe the BSMS approach to ensuring that the benefits of the BSMS system development are maximised while compliance with the relevant legislation, policy and standards of all stakeholders (Appendix A) is maintained. The policy makes reference to the following considerations:

- System Security.
- The process for approval and review of BSMS system access arrangements.
- The NHSBT personnel working with the BSMS system.
- A practical framework on data disclosure for potential customers and BSMS/NHSBT analysts to work to.

- The governance structure within BSMS that ensures corporate responsibility for compliance with these arrangements.

5. SYSTEM SECURITY

Maintenance of the BSMS system's functionality and security is the responsibility of NHSBT Digital, Data & Technology Services (DDTS). The BSMS system relies on existing, established NHSBT processes for importing, linking and providing access to data and/or reports.

A hierarchy also exists within the system to limit the access of users and administrators, where applicable. Hospital users have personal logins linked to their account, which is only accessible externally by the individual's username and password. BSMS administrators will have access to any data supplied by the user.

6. BSMS USER ACCESS

External users wishing to gain access to VANESA, the BSMS data management system, can register for an account on the VANESA home page, using their work email address or via the e-mail address bsms@nhsbt.nhs.uk.

Participants must complete an access application form. This request will be considered and approved by one of the BSMS administrators, who will set up a user account.

Once activated, VANESA may be accessed directly by registered participants via the web, or indirectly by requesting a data output or report (see section 7).

Registered participants can input data, view, refresh or create reports from VANESA depending on the level of user access granted. In general, user access and level will be determined by designation, role and location.

7. REQUESTS FOR REPORTS

For persons who do not wish to have or for whom it would not be appropriate to grant VANESA access, data can be made available by requesting a bespoke report from the BSMS team.

Requests for data **must** contribute the optimisation of blood component stock management in hospitals and must not be used to name and shame an organisation or to harass a participant about their performance. Blood Services and hospitals will work together to ensure that both parties have a complete understanding of the issues affecting stock and wastage levels. Any request not meeting this requirement will be rejected and the requestor informed.

Whilst acknowledging that data is paramount for benchmarking and monitoring performance, sensitive dialogue may be necessary to understand a hospital's individual circumstances. It is therefore important to build relationships with all users and treat all parties with respect.

All requests for information, data or reports derived from the data held in the BSMS system will be logged, reviewed, approved, and actioned by appropriately trained BSMS/NHSBT staff. All requests for information must be documented using the BSMS request form. The BSMS office will review the process.

Requests for information, data or reports will be processed according to the inferred need and the resource available. Each request will be logged and tracked in a database. Requests will be acknowledged, approved and planned according to available resource. An appropriate delivery time will be agreed at the outset.

The BSMS data is viewed as confidential under the common law duty of confidence (Annex A). If a request from an external organisation is viewed as supporting the optimisation of blood component stock management data will usually be provided in an anonymous format. Requests for de-anonymised data i.e. data in a hospital identifiable format will only be provided if approval has been gained from the BSMS Steering Group. A level of de anonymised data is available through the Transparency Reports within VANESA.

As a condition of fulfilling the request, the person or organisation in receipt of the output must acknowledge BSMS as the source of the information in any publication, presentation or report arising from that output.

8. BSMS SYSTEM GOVERNANCE STRUCTURE

Day to day oversight will be undertaken by the BSMS Lead Specialist and BSMS Manager.

Where it is deemed by the BSMS Manager that a request for data needs further discussion prior to approval; the request will be reviewed by the BSMS Steering Group together with the identified data asset owner. The decision from these sources will be final.

9. BSMS/NHSBT PERSONNEL

The BSMS Lead Specialist and Data Analysts directly managed by the BSMS Manager will have administrative access to VANESA whilst any other users will have basic access.

Access to the BSMS system either directly or indirectly by NHSBT staff other than the BSMS team will be determined by role and granted on a need only basis. Any NHSBT staff deemed appropriate by the BSMS Manager to access the data for purposes of analysis will be expected to complete the appropriate authorisations. The BSMS generic e-mail (bsms@nhsbt.nhs.uk) will be the single point of receipt for access requests. If access is granted the members of staff will be expected to provide a written request (as in section 7) of what data is being accessed and if requested and appropriate provide copies of the final information, data and report to the BSMS Lead Specialist or Manager. No reports, data or information will be sent outside of the organisation without prior approval of the BSMS Manager. Relevant training will be provided by BSMS and supporting materials made available.

As a condition of fulfilling the request, the person or organisation in receipt of the output must acknowledge BSMS as the source of the information in any publication, presentation or report arising from that output.

10. SUMMARY OF CHANGES

This section records the history of significant changes to this document. Only the most significant changes are described here.

Version	Date	Author/Reviewer	Description of change
1.3	28/05/21	Jill Caulfield Lead Specialist BSMS	Reviewed Matthew Bend as BSMS Manager New template
1.2	01/09/19	BSMS Manager	Document signed off by BSMS Steering Group members

Where significant changes are made to this document, the version number will be incremented by 1.0.

Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number will be increased by 0.1.

11.APPENDIX – LEGAL AND POLICY BACKGROUND

In its 2006 'Working Paper 1: Confidentiality Protection – Legal and Policy Considerations' the Office for National Statistics states:
'For health statistics, it is essential that any published statistic respects the privacy of the information shared by individuals with health and statistics professionals. Failure to respect this privacy might result in harm or distress to a specific individual. Such a breach may have a wider effect. A breach of privacy in Official Statistics could damage the relationship of trust between private individuals and health and statistics professionals. Thus the public interest is served when statistical records are kept strictly confidential.'

The Code of Practice for Official Statistics, which were issued by the UK Statistics Authority in 2009, requires that arrangements for confidentiality protection are sufficient to protect the privacy of individual information, but are not so restrictive as to limit unduly the practical utility of official statistics.

The Data Protection Act
This Act is the UK enactment of the European Union Data Protection directive and it sets standards for, and safeguards individuals' rights in relation to, how identifiable personal information is used and disclosed. The definition of 'personal data' broadly means data that relate to a living individual who can be identified-

(a) from those data, or
(b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'

With some limited exemptions, personal data must be used and disclosed in a way that meets the standards known as the 'Data Protection Principles' set by the Act. These include the requirements of fairness and lawfulness, appropriate data quality and security and the right of access.

Common law duty of confidence
For information to be confidential in law, it must have been imparted in circumstances importing an obligation of confidence and it must have the "necessary quality of confidence", this means:

The information is in fact confidential i.e. not in the public domain, not common knowledge or not easily available by other means. That is not to say it must be a secret but is not widely available e.g. the fact that you have told your friend does not necessarily undermine the information's legal confidentiality. The information must be worthy of protection i.e. is neither useless nor trivial. The public interest that confidences should be preserved outweighs some other public interest that favours disclosure.

Confidentiality in NHSBT

NHSBT staff, in common with those of the rest of the NHS more widely, are contractually obliged to protect confidentiality. NHSBT staff are required to read, understand, and adhere to the NHSBT Confidentiality Guidelines.

General Data Protection Regulations

The General Data Protections Regulation (GDPR) is intended to protect the data of citizens within the European Union. The GDPR is a move by The Council of the European Union, European Parliament, and European Commission to provide citizens with a greater level of control over their personal data.