

	T	M	E	0	7	4	3	B	Dispatch: 2.4.07	Journal: TME	CE: Jincy
	Journal Name			Manuscript No.					Author Received:	No. of pages: 21	ME: Nagalakshmi

GUIDELINES

# The specification and use of information technology systems in blood transfusion practice

British Committee for Standards in Haematology Blood Transfusion Task Force

Received 21 August 2006; accepted for publication 14 December 2006

## METHODS

The guideline has been drafted by a working party of the Blood Transfusion Task Force of the BCSH. Information was gathered from several sources. These include references known to the working party members, supported by a search of MEDLINE and the UK Departments of Health websites using the terms blood transfusion and computers, information technology, electronic crossmatch, bedside tracking, bar codes, validation and information governance.

Unless otherwise stated, the recommendations within this guideline are based on professional experience and expert advice; therefore, the levels of evidence for this document are mainly level IV evidence, grade C recommendations (see Appendix 1).

## 1. PURPOSE AND SCOPE OF GUIDELINES

- 1.1. The publication of the BCSH (2000) 'Guidelines for blood bank computing' marked a significant step forward in defining best practice for this area.
- 1.2. Blood transfusion practice is an evolving field, and this revision updates previous work by addressing issues related to developing practice and also aims to highlight the importance of auditing systems against best practice guidance and acting to address non-conformances.
- 1.3. EU Directives 2002/98/EC and 2004/23/EC have been accepted into UK Law as the *Blood*

*Safety and Quality Regulations 2005: Statutory Instrument 2005/50*, and place legal requirements upon hospital blood transfusion laboratories and transfusion centres.

- 1.4. These guidelines will help organizations to implement this legislation that places statutory obligations on transfusion centres and hospital blood transfusion laboratories.
- 1.5. The Better Blood Transfusion documents (see references) outline the clinical governance arrangements for blood transfusion in the UK and where relevant these have been addressed.
- 1.6. With the rapid development of IT systems across the NHS, and in particular the introduction of national electronic patient record systems, these guidelines highlight the specialist nature of blood transfusion computing. This specialism needs to be taken into account in the development of integrated system design in order to maintain and further enhance the safety of transfusion medicine.
- 1.7. These guidelines provide comprehensive advice for the safe management of IT systems in hospital blood transfusion laboratories. They cover not only the blood transfusion laboratory operational procedures but also the underlying IT infrastructure and its support. It is essential that trusts recognize the importance of providing compliant IT systems to hospital blood transfusion laboratories and ensure that the management responsibility for achieving and maintaining compliance with these guidelines is clearly defined. Where appropriate, internal service level agreements between IT departments and blood transfusion laboratories may be helpful to clarify the arrangement.
- 1.8. This document gives an outline of minimum functionality as well as developments required to meet good practice, regulatory requirements and other elements to support audit and the production of management information.

Correspondence: BCSH Secretary, British Society for Haematology, 100 White Lion Street, London N1 9PF, UK.

E-mail: daphne.harvey@b-s-h.org.uk

Writing group members: J. Revill (Convenor, Task Force nominee), P. Ashford (Task Force nominee and former Chairman of UKBTS/NIBSC Standing Advisory Committee on Information Technology), J. Jones (BBTS nominee), F. Regan (BSH nominee), M. Rowley [UKNEQAS (BTL) and Task Force member].

Task Force Chairman: F. Boulton.

- 1.9. The scope of this guideline has broadened to include
  - all blood components and products;
  - tissues (bone, skin, tendons, etc.);
  - stem cell transplants;
  - interaction with automated systems for blood grouping, antibody screening/identification and compatibility testing;
  - bedside patient identification systems;
  - systems outside the laboratory used to order tests remotely, control the release of blood from blood fridges and control the administration of blood and blood components/products at the patient's bedside.
- 1.10. Because of the rapidly changing IT environment in which systems operate, it is recommended that hospital blood transfusion computing systems be audited against §13–15 of these guidelines on an annual basis to ensure ongoing compliance and to identify an action plan to address areas of non-compliance.
  - 1.10.1. An audit tool has been provided to assist with this process (Appendix 3).
- 1.11. Modern blood transfusion practice demands effective and appropriate computer software to control blood transfusion activities. The benefits are significant, including fast and accurate data retrieval, maintenance of quality/safety controls at critical points throughout processing of requests and the production of management information details.
- 1.12. Computerization of blood transfusion processes improves availability of statistical information necessary to support clinically effective practice.

## 2. TRANSFUSION INFORMATION MANAGEMENT

- 2.1. In common with other pathology systems, data processing in the hospital blood transfusion laboratory is concerned with patient records and laboratory activities. However, it is imperative for the system to provide for the strict accountability of blood components/products, to include safety prompts for standard procedures, to inhibit the issue of incompatible or unsuitable components/products and to alert the user to special transfusion requirements.
- 2.2. Patient demographic details held in blood transfusion computers fulfil a special role that cannot be replaced by simple reference to PAS demographic data. The information held is a snapshot of the patient demographics obtained at the

point of request/sample collection, is unique to the request/sampling event and is essential to the safety of subsequent transfusions. It is therefore essential that this information is held independently of the PAS and is not automatically updated by PAS or other system update transactions, including pathology, administration or clinical areas.

- 2.3. The evolution from data processing to information production and the business/audit requirement for statistical information have necessitated systems being able to produce a wide variety of management information as well as maintaining records able to be interrogated for medicolegal and other reasons.
- 2.4. The *Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50*, require that all records pertaining to blood and blood components that are collected, tested, processed, stored, released and/or distributed can be traced from donor to recipient and vice versa for at least 30 years after clinical usage. Suppliers must support data transfer from systems as they become obsolete in order to satisfy this requirement.
  - 2.5. Increasingly, hospital transfusion laboratories take a role in handling tissue products such as stem cells, bone, skin, tendons, cornea and heart valves.
    - 2.5.1. EU Directive 2004/23/EC places legal responsibilities on departments undertaking processing, testing, storage, preservation or distribution of human tissues and cells. Therefore, departments will need to ensure strict compliance with the Directive.
    - 2.5.2. The controls required for release of tissues and cells will be different from that of blood components, and local policies will need to be established.
    - 2.5.3. Traceability from donor to patient and vice versa is mandatory for 30 years from the date of clinical use of the tissue.
- 2.6. To ensure maintenance of safe blood transfusion practice all blood transfusion computer systems should have the potential to be operational 24 h a day (see §15).
- 2.7. There is a need to hold specific information regarding additional local processing activities carried out to standard issue blood components.
- 2.8. Adequate training of staff is essential. Blood transfusion computer systems should only be used by appropriately trained staff.
- 2.9. There must be a documented programme for training staff which covers all standard operating

procedures in use and which fulfils the documented requirements of the laboratory.

2.9.1. All training records must be retained as per current guidelines.

- 2.10. Access levels should be set to limit access to functions such as editing and user-definable parameters, to those with appropriate authority and training.

### 3. INFORMATION GOVERNANCE

- 3.1. The security and confidentiality of patient identifiable computer records is covered by the eight principles of the Data Protection Act 1998 and the Caldicott Principles.
- 3.2. The DoH has produced an NHS Code of Practice (Department of Health, 2003), which outlines the responsibilities of staff.
- 3.3. All NHS staff must comply with relevant information governance regulations under the terms and conditions of their employment.

### 4. EXTERNAL COMMUNICATIONS

- 4.1. All electronic data interchange should conform to the criteria detailed in the *Guidelines for the Blood Transfusion Services in the United Kingdom* (2004) or to other standards as approved by the NHS Information Authority.
- 4.2. The system should be able to generate a request for stock that can be transmitted to the Blood Centre by electronic data transfer.
- 4.2.1. The request for stock should be in a form electronically compatible with the Blood Centre computer system, or manual transcription to the Blood Centre computer is to be used, as closely similar as possible, to avoid errors in interpretation.
- 4.2.2. The request should have a unique reference number and should include date, time and identity of person making the order.
- 4.3. The system should be able to accept from the Blood Centre electronic transfer of issue details and test results using the Dispatch File format specified in the *Guidelines for the Blood Transfusion Services in the United Kingdom*.
- 4.3.1. Privacy-enhancing technologies should be used where appropriate – this includes techniques such as encryption and password protection. Pseudonyms and anonymization should be used as necessary.

All new developments should contain these features.

- 4.4. The system should be able to support the provision of information for the Blood Stocks Management Scheme.

### 5. PERIPHERAL ENQUIRY

- 5.1. It is desirable that users in theatres or wards can enquire via remote terminals for the availability of allocated blood components for patients, availability of suitable samples in the blood transfusion laboratory and test results.
- 5.1.1. For correct blood availability to be displayed, mechanisms for real-time update of blood withdrawal must be in place.
- 5.1.2. Other information, such as if the patient has atypical red cell antibodies or special transfusion requirements, should be included.
- 5.2. Clear and logical data display is essential for non-specialist users.

### 6. INPUT TECHNIQUES

- 6.1. Methods of inputting data include the use of bar codes, optical mark readers, electronic transfer from other systems and manual entry.
- 6.1.1. Staff performing these tasks should be trained to a level of competence commensurate with the importance of this task.
- 6.1.2. Wherever possible, electronic input devices should be used to reduce the risk of human transcription errors.
- 6.2. Bar coding is carried out to ensure the accuracy of transmitted information. To gain the maximum benefit from such coding, systems reading and interpreting the bar codes need to ensure that valid codes have been scanned. The following minimum checks should be carried out by the receiving application software:
- 6.2.1. Bar code identifiers (data identifiers in ISBT 128, start/stop sequences in Codabar) are those of the expected code;
- 6.2.2. Format (length and character types) of the received data string matches the defined format for the expected code;
- 6.2.3. Checksums are used to validate correct data transmission (with ISBT 128 ensure that the scanner is performing the internal Code 128 checksum validation);

- 6.2.4. Data values are within acceptable ranges.

## 7. PATIENT RECORD MANAGEMENT

### 7.1. Unique patient identifiers

- 7.1.1. The use of unique patient identifiers (UPN) is essential for positive patient identification prior to transfusion in order to prevent transfusion of the wrong blood to patients. All systems should support the use of the NHS number (or equivalent).

- 7.1.2. Other numbering systems are available, and it should be possible to incorporate various forms and configurations of such identifiers, including hospital unit number, accident and emergency numbers or major incident numbers for those individuals involved in a major incident (these may differ from the standard A/E numbers).

- 7.1.2.1. A unique number for neonates, which should be available immediately after birth, must be utilized.

- 7.1.2.1.1. This should be the NHS patient record identifier.

- 7.1.3. An alert is necessary at sample registration when a possible duplicate patient record attached to a different unique identifier is created, to enable record linking or merging to be actioned if considered appropriate after review (see §7.3).

### 7.2. Data sets (see Appendix 4)

- 7.2.1. Further items of patient demographic and other associated information are also necessary in order to

- 7.2.1.1. Fully identify the patient concerned;

- 7.2.1.2. Ensure that all previous records relating to a patient can be identified to allow checking of current blood group with historical records, ensure provision of special requirements and support the resolution of red cell antibody problems;

- 7.2.1.3. Enable prompt contact with appropriate clinical staff if further samples are required or any difficulty in providing blood is envisaged;

- 7.2.1.4. Support the production of data for retrospective audit and management information.

- 7.2.2. As a minimum requirement in terms of fields supported, the system should include items listed in Appendix 4.

- 7.2.2.1. Further information and advice are provided in the BCSH (2004b) guidelines.

- 7.2.3. There is an increasing need to determine the appropriateness of the use of blood components/products. For this reason, it should be possible to search for keywords or coded comments in respect of the indications for use of components/products.

- 7.2.4. Suggested appropriate indication codes for transfusion have been prepared as part of the Better Blood Transfusion initiatives and are available in the SHOT annual report covering years 2001–2002.

- 7.2.5. SNOMED-CT is the preferred standard in the national Integrated Care Record Strategy project, and appropriate codes are being developed.

- 7.2.6. The ability to use free text should be part of the system where codes do not apply.

### 7.3. Managing duplicate patient records

If duplicate patient records exist within a blood transfusion database, there is serious risk of incorrect or inappropriate actions from a lack of recognition of previous results, including missing the opportunity to recognize a current incorrect ABO/D type, the presence of patient atypical red cell antibodies or special transfusion requirements. Therefore, active management of the database is essential to avoid errors and omissions.

- 7.3.1. Systems will need to provide a facility for handling duplicate patient records, either by merging or record linking.

- 7.3.2. Appropriate password-controlled user authorities must be in place.

- 7.3.2.1. Users should define who is authorized to merge patient transfusion records to ensure that staff who are unaware of the risks of erroneous transfusion records do not perform these tasks.

- 7.3.3. Criteria for merging/linking should be locally defined but must include matching of ABO and D blood groups.

- 7.3.4. Merging should only be permitted if relevant patient identifiers, which should be defined by users, are identical.

- 7.3.4.1. Exceptionally, this may need to be overridden when updated or amended patient information becomes available.

- 7.3.4.2. Change of name should be allowable, but strict validation criteria must be defined prior to merging/linking of records.
  - 7.3.4.2.1. These actions should be strictly controlled to high-level system users.
- 7.3.5. Whatever mechanism is used, a comprehensive audit trail must be retained holding the full patient details of both records prior to the merge/link, the date/time of the merge/link and the name of the individual authorizing the merge/link.
- 7.3.6. A system for searching the database for potential duplicate records should be available.
  - 7.3.6.1. This may be activated manually or run automatically at pre-determined time periods.
  - 7.3.6.2. Search criteria should be user definable.
    - 7.3.6.2.1. These should include all mandatory patient demographic data and date of sample registration.
    - 7.3.6.2.2. Use of a limited data set search should be possible to allow for misspellings of patient names or amended DOB entries.
      - 7.3.6.2.2.1. 'Soundex' or similar intelligent style searches would be advantageous.
  - 7.3.6.3. Merging/linking of patient records, as defined above, should be able to be performed directly from the search result display programme.
- 7.4. Record association
  - 7.4.1. For foetal or neonatal samples, the name, DOB and hospital number of the mother should also be given, on paper or on electronic requests, in order to link their transfusion records.
  - 7.4.2. It should be possible to link or identify the patient and partner records for antenatal testing.
- 7.5. Record amendment
  - 7.5.1. If patient details need to be amended as new information becomes available, users should define who is authorized to do this.
  - 7.5.2. When the master patient demographic details are amended, the original patient data should be retained against that specific sample.
  - 7.5.3. Details of patient record amendments, including user identification, should be logged and retained as part of an audit trail.

## 8. ELECTRONIC REQUESTING FROM WARD-BASED TERMINALS

- 8.1. Electronic requesting is only suitable where a full hospital-wide information system is available. In all other situations manual requesting is required, compliant with BCSH guidelines (BCSH, 2004b).
- 8.2. A benefit of such systems is the ability to pass an electronic request across an interface into the blood transfusion computing system. This has two immediate benefits:
  - 8.2.1. Elimination of transcription error.
  - 8.2.2. Speed of entry of the request into the blood transfusion system.
- 8.3. The patient information is retrieved from the PAS and associated with a unique order number identifying the request. Because this process can occur in the absence of the clinical notes, it is imperative that correct patient identification occurs. The items of information that should be transferred to the blood transfusion computer system are given in Appendix 4.
- 8.4. Electronic requesting does not eliminate the necessity for request information to be available during phlebotomy to ensure correct patient identification.
- 8.5. The request may be linked to an existing record where the hospital unit number, surname, forename and DOB of the two records are identical.
  - 8.5.1. Where an identical record is not found, the blood transfusion system should search for closely matching records, and alert the user to their existence.
  - 8.5.2. Local policies must exist to define under what conditions the linking of an imperfect match is permitted (see §7.3).

## 9. LABORATORY SAMPLE HANDLING/PROCESSING

- 9.1. General
  - 9.1.1. Samples need to be uniquely identified in the laboratory by a bar coded sample number which must be associated with the patient record (BCSH, 2004b).
  - 9.1.2. All information generated from sample processing must be stored against the sample number.
  - 9.1.3. Blood transfusion laboratories must conform to requirements for ensuring continuity between test results and reagent batch information; therefore, appropriate

- systems should be designed and implemented.
- 9.1.4. It is recommended that EQA samples be labelled as per routine patient samples, including assigning laboratory numbers with test results attached, for long-term retention.
    - 9.1.4.1. Internal quality control samples may usefully be recorded in the same way.
- 9.2. Automation
- The majority of automated and semi-automated equipment in use in blood transfusion laboratories have some degree of integral computer control, and instruments are often interfaced directly into the main laboratory computer system. All such equipment should be validated as defined in the ISBT (2003) document 'Guidelines for validation and maintaining the validation state of automated systems in blood banking'.
- 9.2.1. All sample identification, test result display, amendment, storage and subsequent electronic downloading should be performed using the bar coded sample number as the unique identifier.
  - 9.2.2. Pre-transfer manipulation and interpretation of data is often performed within the automated equipment, dependent on the equipment used, with subsequent electronic transfer on the interpreted result.
    - 9.2.2.1. Interpreted results should be automatically inserted into the appropriate patient record.
    - 9.2.2.2. The original reaction pattern must still be retained according to current legislation.
      - 9.2.2.2.1. This may be either in the laboratory computer system, in the automation equipment database or in secure off-line storage.
      - 9.2.2.2.2. EQA sample results should be retained as per patient test results.
  - 9.2.3. Test result amendments, whether performed using the primary equipment software or main computer functions, must be fully logged, including original and amended results, date and time of action and operator identification.
  - 9.2.4. Strictly defined user criteria for allowable test result amendments must be defined and implemented, with appropriate accessibility controls.
    - 9.2.4.1. Patient red cell blood group test results obtained from automated equipment should not be amended, but repeated or investigated as per recommendations in BCSH (2004b) guidelines.
  - 9.2.5. Any test result amendment details must be retained according to current legislation.
    - 9.2.5.1. Reason for amendment should be logged.
  - 9.2.6. Date and time of result input, and source of result, must be recorded and stored attached to the patient sample record in the laboratory computer system.
  - 9.2.7. Electronically transferred results should clearly indicate if any manual editing of information has occurred prior to transfer, and ideally should be stored with the patient record.
  - 9.2.8. The equipment and technique used to perform each test must be recorded.
  - 9.2.9. Users should be aware that such automated systems are not foolproof and be alert for erroneous results.
    - 9.2.9.1. Strict adherence to protocols is essential.
    - 9.2.9.2. Regular quality checks should be performed to ensure sensitivity of the testing system and reagent stability by the use of serological controls.
    - 9.2.9.3. Electronic controls, such as liquid-level sensors, are particularly important to prevent false-negative results where plasma has not been aspirated or reagents have not been added (see §11.5.6.3.1).
    - 9.2.9.4. Only competent experienced users should operate the equipment and amend/validate results for electronic download.
- 9.3. ABO and D grouping
- 9.3.1. The following information should be stored:
    - 9.3.1.1. The sample number;
    - 9.3.1.2. The test results, including reaction grades and interpretation;
    - 9.3.1.3. Date and time test is performed;
    - 9.3.1.4. Identity of person(s) entering/validating results;
    - 9.3.1.5. Technique used for performance of test;
      - 9.3.1.5.1. Including where automated or semi-automated equipment is used (see §9.2.8).
  - 9.3.2. Manual entry may be by means of reaction patterns, or interpreted blood group, using keyboard or bar code menu.

- Manual results should be verified by a second blind entry, which wherever possible should be carried out by a second operator.
- 9.3.3. If there is any anomaly between current ABO and D group results with those stored in the system, these discrepancies must be immediately flagged and investigated following BCSH (2004b) guidelines.
  - 9.3.4. There should be a facility for supervisory editing and correction with appropriate audit trail.
    - 9.3.4.1. Trend analysis should be possible.
  - 9.3.5. Where necessary, e.g. following stem cell transplant, there should be a password-controlled override option to allow the entry of a different patient blood group to the historical record. This should be accompanied by appropriate warning messages.
- 9.4. Antibody screening and identification
    - 9.4.1. The methodology used should be stored with the result.
    - 9.4.2. There should be the facility to enter multiple antibody specificities, and the date of identification for each separate antibody should be stored.
    - 9.4.3. There should be a facility to allow for comments, e.g.
      - 9.4.3.1. Clinical significance of antibody;
      - 9.4.3.2. Additional time required for selection of appropriate blood for transfusion.
  - 9.5. Direct antiglobulin test
    - 9.5.1. When entering results of the DAT, the type of sample tested, e.g. ethylenediamine tetraacetic acid or clotted blood sample, should be recorded.
      - 9.5.1.1. There should be available space for comments to be added.
    - 9.5.2. It should be possible to enter results obtained with monospecific AHG reagents.
  - 9.6. Pregnancy-related testing
    - 9.6.1. It should be possible to associate the following with the patient record, including:
      - 9.6.1.1. Number of weeks' gestation at the time of testing;
      - 9.6.1.2. Foetomaternal haemorrhage bleed volume in millilitres;
      - 9.6.1.3. Dose and batch number of anti-D immunoglobulin issued (facility for multiple entries).
    - 9.6.2. A recall system linked to gestation would be useful. If there is a system in operation to recall antenatal patients, this should be in accordance with BCSH (1996) guidelines and addendum (BCSH, 1999a).
      - 9.6.2.1. A mechanism for the notification of need for prophylactic antenatal administration of anti-D immunoglobulin may be advantageous.
    - 9.6.3. There should be facilities to record the results of antibody titration and/or antibody quantitation.
    - 9.6.4. There should be facilities to request and enter results of partners' phenotypes and link records (see §7.4).
    - 9.6.5. It should be possible to enter coded and free-text comments against patients' results.
  - 9.7. Other miscellaneous tests
    - 9.7.1. It should be possible to request and record a wide variety of other tests as required.
    - 9.7.2. Where possible, all inputs should be coded to enable easy retrospective analysis.
  - 9.8. Investigation of transfusion reactions
    - 9.8.1. It should be possible to store the results of serological testing performed in the case of a suspected transfusion reaction.
    - 9.8.2. It would be advantageous to flag the record of a patient or component/product to indicate that they have been involved in a transfusion incident that has been reported within the hospital or to Medicines and Healthcare products Regulatory Agency and/or SHOT.
  - 9.9. Reporting issues
    - 9.9.1. Report formats should guard against possible misinterpretation, e.g. 'antibody screen negative' reported next to ABO group could be misread as 'D negative' through expectation that the D group would follow the ABO group.

## 10. COMPONENT AND BATCH PRODUCT STOCK MANAGEMENT

Stock management is an integral function of the hospital blood transfusion IT system. It is imperative that the system is able to store and recall details of blood component transactions from receipt to eventual transfusion or disposal in order to satisfy the statutory traceability requirements.

Manufacturers of computer software should be mindful of the current and potential future changes in national and international legislation and flexibility to adapt systems should be maintained.

#### 10.1. Components

The term component is used in this document for all red cell, platelet, FFP/cryoprecipitate and white cell preparations produced by the UK Blood Services and supplied to hospitals labelled with unique donation numbers. Information on the fate of all components must be held for a minimum of 30 years (*Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50*).

10.1.1. Bar codes and the text display of bar coded information will comply with the UKBTS/NIBSC standards for uniform labelling of blood and blood components (UKBTS, 1998).

10.1.2. The date and time of receipt of all components into the receiving establishment must be recorded.

10.1.3. Entry of stock into the system for all components should be by means of electronic transfer (see §4.3) or a bar code reader. The following information must be captured for each individual unit:

10.1.3.1. Unique donation identifier;

10.1.3.2. ABO and D groups;

10.1.3.3. Component code;

10.1.3.4. Expiry date (and time where appropriate).

10.1.4. Where check characters are included, systems must use these to validate the data inputs.

10.1.5. Allocated units received from external sources must be entered into the local computer system prior to transfusion.

10.1.5.1. The supplying organization should be recorded.

10.1.6. In addition to the above, the system should allow for component characteristics to be retained against the component, either as an integral part of the component information or as coded entries, e.g.

10.1.6.1. Additional typing;

10.1.6.2. CMV antibody negative;

10.1.6.3. Irradiated;

10.1.6.4. Transfer from/to.

10.1.7. Other comments, either coded or free text, should be able to be recorded and retained.

10.1.7.1. Such comments may need to be entered post-issue or after transfusion of the component.

10.1.8. The system must be able to store and recall the crossmatch and in-house manipulation history of all units received in the blood transfusion laboratory.

10.1.8.1. Dates and times of movements of components in order to support temperature-monitoring requirements.

10.1.8.2. Patient(s) to whom unit was previously allocated.

10.1.8.3. Details of patient to whom unit was transfused, date of transfusion and, where direct links are in place, the time.

10.1.8.3.1. This should ideally be recorded as a result of data capture at the point of transfusion.

10.1.8.4. Stock recall or 'reason for discard' if not transfused, e.g. damaged upon receipt, outdated, inappropriate storage and wastage, and, where possible, coded comments/reason codes should be used to permit audit.

10.1.8.5. All manipulations of components subsequent to receipt must be recorded, e.g. when frozen units are thawed with subsequent reduction of component expiry date/time.

10.1.8.5.1. On no account should extension of expiration time/date be permitted.

10.1.9. Stock movements.

10.1.9.1. The system should be able to record and store details of unit movements including transfer between unreserved and reserved stock, transfer to and from satellite refrigerators, issues to wards and departments and transfers to other hospitals.

10.1.9.2. Units returned unused should be booked in using a similar procedure and the time out of the regulated blood bank storage facilities should be logged against that unit. If the time out of storage exceeds that defined by local policy, a warning should be generated and action taken in line with standard procedures.

10.1.10. The system should allow for a comment on adverse reactions following transfusion of a component (see §9.8).

#### 10.2. Autologous red cell units

Blood collected for autologous purposes must meet the selection, labelling, processing, quality

assurance and testing criteria as appropriate (see *Guidelines for the Blood Transfusion Services in the United Kingdom* and *Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50*).

10.2.1. It is necessary to ensure full traceability and audit trails as for allogeneic units, and therefore, all computer systems must have complete handling functionality for autologous units.

10.2.2. It should be possible to identify autologous units as a distinct entity from allogeneic units.

10.2.3. Autologous units should be treated as per allogeneic units and issued through the computer using identical procedures.

10.2.4. Controls need be in place to prevent allocation of autologous units other than to the intended recipient and to record wastage if not transfused.

### 10.3. Batch product management

The term batch product is used in this document for those plasma derivatives that are prepared using a large pool process or recombinant technology, and usually supplied with multiple units having the same batch number and no individual unique identifier on the units. These will include human albumin solutions, immunoglobulin preparations (including anti-D and intravenous immunoglobulin), pooled viral inactivated FFP and individual factor concentrates.

10.3.1. It is a requirement of the EU Directive 2001/83/EC that records are retained allowing tracing of all products from source to patient.

10.3.2. The system must allow entry on receipt of multiple quantities from a single batch.

10.3.3. Full details of products must be entered and retained. These include:

10.3.3.1. Date and time of receipt;

10.3.3.2. Product name;

10.3.3.3. Supplier;

10.3.3.4. Batch number;

10.3.3.5. Expiry date;

10.3.3.6. Quantity of units received;

10.3.3.7. Batch comments, including volume and amount of product/bottle (e.g. IU mL<sup>-1</sup> or bottle), where appropriate;

10.3.3.8. Location of stock;

10.3.3.9. Stock movements;

10.3.3.10. Stock recall.

10.3.4. Issues for single or multiple units to individual patients should be possible and the details recorded and stored must include:

10.3.4.1. Patient identifiers;

10.3.4.2. Date of administration or other fate;

10.3.4.3. Batch number;

10.3.4.4. Number of units;

10.3.4.5. Product name;

10.3.4.6. Expiry date;

10.3.4.7. Batch or issue comments.

## 11. COMPONENT/BATCH PRODUCT ISSUES

### 11.1. Patient compatibility labels

11.1.1. All such labels when attached to components or products should not cover or obscure donation or manufacturer information on the unit base labels.

11.1.2. Labels should comply with recommendations in BCSH (2004b) guidelines.

### 11.2. Patient special requirements

11.2.1. Records of atypical antibodies and special transfusion requirements must be displayed at entry into unit allocation programme.

11.2.1.1. The system should ensure that these details are always displayed clearly on the current record and are not lost in the patients' historical records.

11.2.2. The system should have the facility to flag individual patients' records to indicate that mandatory special transfusion requirements apply, e.g. CMV antibody-negative or irradiated cellular components, and these should be clearly displayed at allocation.

11.2.2.1. Mandatory requirements should be automatically validated against the component characteristics being issued.

11.2.3. Other special needs may also be required, e.g. platelets in platelet suspension medium or washed red cells, and these should be displayed and authenticated at issue of component or product to the patient.

11.2.4. Some patients have special transfusion requirements due to age, clinical diagnosis or local preferences, and alert mechanisms requiring action or

- acknowledgement should be available during allocation. Examples are:
- 11.2.4.1. CMV antibody-negative cellular components for infants <1 year of age;
  - 11.2.4.2. Viral inactivated FFP for specific patients based on age or DOB;
  - 11.2.4.3. D-negative cellular components for women of childbearing potential who are D negative;
  - 11.2.4.4. Special requirements for blood components during pregnancy;
  - 11.2.4.5. Haemoglobin S-negative red cells for sickle cell disease patients;
  - 11.2.4.6. A warning of recent administration of anti-D immunoglobulin.
- 11.3. Compatibility testing
- All procedures must also conform to the recommendations made in 'Guidelines for compatibility procedures in blood transfusion laboratories' (BCSH, 2004b), with particular reference to appropriate timing between any previous transfusion(s) and the current sample.
- 11.3.1. The system must not allow selection of ABO-incompatible red cell units and should demand authorization of D mismatch. The issue of suitable, but non-identical, ABO group red cells should also demand authorization from the user.
  - 11.3.2. For components other than red cells, it should be possible to define criteria for each component locally with regard to ABO and D group acceptability.
  - 11.3.3. The system should allow a definable reservation period for allocated units and produce a return to stock list.
    - 11.3.3.1. The reservation period should be user definable where necessary, considering date of component requirement, not just date of component issue.
    - 11.3.3.2. The reservation period must not extend beyond the expiry date of the component or product.
  - 11.3.4. The system should allow results to be entered against each unit crossmatched. Whatever the method of entry, the following information should be stored:
    - 11.3.4.1. Date and time test performed;
    - 11.3.4.2. Type of compatibility testing performed, e.g. AHG crossmatch, rapid spin technique or electronic selection/issue;
    - 11.3.4.3. Compatibility result;
    - 11.3.4.4. Issue status (uncrossmatched, group compatible, crossmatch compatible, electronic issue, suitable for, incompatible, etc.);
    - 11.3.4.5. Reservation period where appropriate;
    - 11.3.4.6. Identity of person(s) entering/validating results.
  - 11.3.5. After verification of results, a compatibility report and labels should be produced as required (BCSH, 2004b).
  - 11.3.6. The crossmatch record should retain information on both compatible and incompatible units.
  - 11.3.7. The facility should exist in exceptional circumstances to allow the issue under password control of ABO-compatible but serologically incompatible units, e.g. in cases of autoimmune haemolytic anaemia.
- 11.4. Red cell units released for emergency issue
- 11.4.1. The system should allow for the issue of 'emergency' units, either O D-negative or O D-positive, without a known patient blood group.
  - 11.4.2. It should be possible to issue group compatible units, based on an emergency blood group only, prior to entry of antibody screen or compatibility results.
  - 11.4.3. Retrospective entry of further tests, e.g. compatibility results, should be allowed with recording of the timing of such entries.
- 11.5. Electronic selection and issue of units without serological testing between patient and donor red cells
- 11.5.1. The use of electronic issue procedures without serological testing will very much depend on the level of automation in use within that laboratory. A completely automated system for ABO/D testing will ensure that there is no manual step or clerical input into the process from the entry of the sample for testing into the laboratory system until the final result is obtained and downloaded into the laboratory computer record.
    - 11.5.1.1. The lack of electronic result transfer, especially for ABO/D blood group results, inherently increases the risk within the system.

- 11.5.2. The absolute necessity for correct determination of the ABO (and D) group of the patient is paramount when the check for errors afforded by the serological crossmatch is no longer present.
- 11.5.3. Robust procedures and strict adherence to protocols is essential to ensure safe working practices.
- 11.5.4. All electronic issue procedures should be controlled by computer algorithms to validate appropriateness of actions (level III evidence, grade B recommendation).
- 11.5.5. Extensive 'on-site' validation prior to introduction of electronic issue, and checking after computer maintenance or updates, is essential (see §16).
  - 11.5.5.1. Computer software should have been validated to ensure complete compliance with the requirements for ABO and D group compatibility.
  - 11.5.5.2. The system should be challenged with a variety of clinical scenarios to ensure compliance with the recommended criteria.
- 11.5.6. The following criteria must be satisfied before electronic selection and issue is permitted:
  - 11.5.6.1. Provided that sample handling and identification are fully automated and results are transferred electronically with no manual editing, the ABO/D group of the patient may be determined by testing twice using two aliquots from the same sample;
  - 11.5.6.2. If a manual step, including amendment of results from automation, is required at any stage in the procedure, it is recommended that either two samples, collected on different occasions, or a current sample with a historical record, should have been tested;
  - 11.5.6.3. Antibody screening, in addition to ABO and D typing, must be performed on the sample that is currently being used;
    - 11.5.6.3.1. Electronic controls to prevent false-negative antibody screen results in automated systems must be used (see §9.2.9.2.1);
  - 11.5.6.4. Blood group results on the current sample(s) and any historical record must be identical;
  - 11.5.6.5. If manual entry of current blood group result is necessary, the previous blood group result must not be displayed on the same screen;
  - 11.5.6.6. For previously transfused patients, the timing of the sample must comply with BCSH (2004b) guidelines;
  - 11.5.6.7. The patient's serum/plasma does not contain, and has not been known to contain, clinically significant red cell alloantibodies reactive at 37 °C;
    - 11.5.6.7.1. Further guidance regarding the potential significance of red cell antibodies is provided in the BCSH (2004b) guidelines;
  - 11.5.6.8. Antibody screening procedures must conform to the minimum recommendations as detailed in BCSH (2004b) guidelines;
  - 11.5.6.9. Entry of unique donation number, blood group, component code and expiry date from the unit(s) must be done using bar code reader or other electronic means.
- 11.5.7. When the above criteria are not met a serological test of compatibility between patient and donor(s) must be performed.
- 11.5.8. Electronic issue must not be used in the event of computer downtime or when interfacing to automated blood grouping systems is down.
  - 11.5.8.1. The lack of electronic validation procedures is a significant risk.
- 11.5.9. Results from 'send away samples', including antenatal samples, if entered manually into the system should not be considered as the first group entry.
  - 11.5.9.1. If these results are electronically transferred onto the system by the testing laboratory, and the same local requirements for pre-transfusion testing, labelling and identification of the sample are guaranteed by the testing laboratory, these results may be acceptable as the first group entry for electronic issue, following a risk assessment.
- 11.5.10. A facility to flag individual patients as being unsuitable for electronic issue

must be available. Such examples may include:

- 11.5.10.1. Permanent exclusion of patients with significant red cell antibodies;
- 11.5.10.2. Limited period exclusion for 3 months post-transplant of solid organs, including kidney (BCSH, 2004b).
- 11.5.11. The use of electronic issue for neonates is not recommended (BCSH, 2004a) when issuing group-specific red cells because of possible maternal ABO antibody transfer to the neonate.
  - 11.5.11.1. Providing all other criteria for maternal/neonatal testing are met, the use of electronic issue may be acceptable if the standard practice locally is to transfuse specially selected group O D-negative red cells to all neonates.
- 11.5.12. The previous administration of anti-D immunoglobulin to D-negative females does not exclude the use of electronic issue once the anti-D immunoglobulin is no longer detectable.
- 11.5.13. When circulating anti-D is still detectable after the administration of anti-D immunoglobulin to D-negative females an AHG crossmatch should be performed unless:
  - 11.5.13.1. Following a local risk assessment the use of electronic issue is identified as being acceptable providing:
    - 11.5.13.1.1. The presence of all significant red cell antibodies (other than the anti-D) have been excluded by the use of appropriate antibody identification panels;
    - 11.5.13.1.2. In the absence of recent transfusions the sample had been obtained in the previous 7 days (BCSH, 2004b);
    - 11.5.13.1.3. All other criteria are met.
- 11.5.14. The use of a different protocol for group O patients is not recommended.
  - 11.5.14.1. In the event of incorrect phlebotomy or technical errors where this is not the correct blood group for that patient, it must be realized that the transfusion of group O components containing plasma to non-group O patients may cause acute transfusion reactions [SHOT (2003) annual report for 2001–2002].

## 12. WARD PHLEBOTOMY/COMPONENT AND PRODUCT COLLECTIONS/TRANSFUSION EVENTS

Comprehensive audit trails for all blood component/product storage, movement and fate are legal requirements (*Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50*). Furthermore, BCSH (1999b, 2004b) guidelines provide best practice approach to laboratory and ward protocols for blood component/product handling, documentation and patient verification. Because of the strict requirements, both for detailed documentation and validation of patient identity at various stages of the process, the increased utilization of computer technologies has been recommended at phlebotomy, component collection and pre-transfusion patient validation stages, to reduce the possibility of manual error [SHOT annual reports for 2001–2002 (2003) and 2002–2003 (2004)].

### 12.1. Bedside blood sample ‘tracking’

- 12.1.1. Bar coding systems can offer improved security and safety in the identification of samples and patients. Introduction of such systems is encouraged, but they must be designed and implemented in such a way as to meet the specific safety requirements of transfusion medicine.
- 12.1.2. It is recommended that computer-generated addressograph labels should not be used on samples for pre-transfusion compatibility procedures (BCSH, 2004b) except where associated with a bar code scanner which scans a unique bar code from the patient’s wristband and the labels are printed and attached to the samples at the patients bedside at the time of phlebotomy.
  - 12.1.2.1. Systems must be capable of rejecting a request for labels to be printed after a specified time between identifying the patient and printing the labels.
    - 12.1.2.1.1. This will minimize the chances of labels being printed at the bedside of a wrong patient.

### 12.2. Fridge tracking activities

- 12.2.1. When components/products are collected for patient use or moved between storage facilities or hospitals, a full audit trail is mandatory.
- 12.2.2. It is preferable that a computer program should be available to electronically track the blood and blood

components. This is to provide a full audit trail record for units leaving the laboratory storage facilities. It is desirable that such an issue program should be interfaced to the main blood transfusion computer system to provide the facility for issue control and correct patient verification.

12.2.2.1. It is desirable that the fridge only unlocks when the correct patient verification has been confirmed.

12.2.2.1.1. An alarmed emergency override feature is necessary for use in extreme circumstances to obtain unmatched red cells.

12.2.2.1.1.1. Such events should be logged and retrospectively auditable.

12.2.2.2. The current location of all blood and blood components should be displayed to both laboratory and ward enquirers.

12.2.3. The details below should be recorded and retained:

12.2.3.1. Identity of the individual undertaking collection;

12.2.3.2. Hospital number or other appropriate patient identifier;

12.2.3.3. Donation number(s) of unit(s) being removed;

12.2.3.4. Component/product type(s);

12.2.3.5. Destination of unit(s);

12.2.3.6. With each issue the date and time must be recorded.

12.2.4. These details are required for all transfers between approved storage and ward locations, or for movement between hospital sites.

12.2.5. For any returned units the date and time must be recorded and an alert should be provided for those units which have been 'out of controlled storage' for longer than a pre-defined period of time (see §10.1.9.2).

### 12.3. Bedside tracking functions

12.3.1. Electronic bedside tracking systems may be used to provide comprehensive bedside verification of patient and component/product suitability, full documentation of administration events and recording of nursing observations.

12.3.1.1. Details recorded should include:

12.3.1.1.1. Receipt of component/product into clinical area;

12.3.1.1.2. Identification of caregiver;

12.3.1.1.3. Time of actions including:

12.3.1.1.3.1. Start of each unit;

12.3.1.1.3.2. Nursing observations;

12.3.1.1.3.3. End of transfusion;

12.3.1.1.3.4. Any adverse events;

12.3.1.2. Interfacing to the laboratory computer system will allow bedside control of transfusion processes and provide real-time updates of usage for effective stock management.

## 13. INFORMATION SECURITY

Blood transfusion IT systems and the more general information systems they support (including manual records) will need to comply with best practice guidance on information security to ensure confidentiality, integrity and availability of information. The following sections address the key essential requirements, but departments should aim to achieve compliance with BS 7799 Information Security Standard (also see §3 – Information Governance).

Blood transfusion computer systems hold confidential personal information, and system design and use should take into account the requirements of the relevant legislation and best practice guidance. The Department of Health (2003) publication *Confidentiality: NHS Code of Practice* provides a comprehensive summary of these requirements.

### 13.1. Access security

13.1.1. As a minimum, access security design should:

13.1.1.1. Require password entry to gain initial access to the system;

13.1.1.2. Require password entry immediately before non-standard high-level activity;

13.1.1.3. Not display passwords on the screen during entry;

13.1.1.4. Allow individual user access rights to be tailored to specific tasks or task groups;

13.1.1.5. Validate passwords to prevent use of trivial or insecure passwords;

13.1.1.6. Enforce password expiry after a specified time span and should prevent re-use of passwords;

13.1.1.7. Store passwords in an encrypted form, separately from the main database;

13.1.1.8. Disable or disconnect terminals that have been inactive for a specified period of time.

- 13.1.2. Operational procedures should make full use of the security features provided and should not compromise access security. In particular, procedures should ensure that:
  - 13.1.2.1. Each user has a unique password;
  - 13.1.2.2. Passwords meet minimum security standards (e.g. at least six characters long, containing a combination of numeric and alpha characters, no common or user specific words, names or dates);
  - 13.1.2.3. Passwords are not written down or released to any other individual;
  - 13.1.2.4. Suspected security breaches are notified, documented and acted upon quickly;
  - 13.1.2.5. Staff are aware of their security responsibilities.
- 13.1.3. There is one possible exception to these requirements. Where critical access, such as system administrator access, is limited to one person, details of the account name and password should be recorded and stored in a sealed container in a secure location for use in emergency only.
- 13.2. Documentation
  - 13.2.1. There must be a comprehensive, up-to-date and controlled set of system documentation that describes the physical and logical configuration of the system. This documentation must be sufficiently comprehensive to:
    - 13.2.1.1. Provide a fallback in the event of catastrophic system loss from which a replacement system can be configured;
    - 13.2.1.2. Provide a historic record for audit and litigation purposes so that the configuration in place at a specified time in the past can be reconstructed;
    - 13.2.1.3. Assist in the transfer of information when changes of personnel take place.
  - 13.2.2. The system documentation must be maintained under version control and should comprise the following elements:
    - 13.2.2.1. The physical and logical design including details of hardware, software (with version numbers), communication and networking protocols, backup and recovery procedures;
    - 13.2.2.2. Full system configuration details;
    - 13.2.2.3. Site acceptance tests and validation records;
    - 13.2.2.4. Backup logs;
    - 13.2.2.5. Record retention reviews (see §14);
    - 13.2.2.6. Details of all changes to the system with date and authorization including hardware changes, software upgrades and configuration changes;
    - 13.2.2.7. Reports of audit against statutory requirements and best practice guidance;
    - 13.2.2.8. Adverse incident reports where incident or cause relates to IT systems.
- 13.3. Data backup and recovery
  - 13.3.1. Data backup and recovery procedures must be available to allow retrieval of the system and database in the event of serious loss or corruption. In the blood transfusion laboratory environment, with the continual movement of samples and blood packs, it would be very difficult to securely reconstruct input activity over any significant length of time.
  - 13.3.2. It is strongly recommended that systems are designed to incorporate disk mirroring, or transaction journaling to a separate storage unit, in order to allow full recovery in the event of disk failure.
  - 13.3.3. If temporary manual procedures are necessary then robust documented manual systems should be in place, with secure retrospective entry of transactions.
  - 13.3.4. System design should allow full testing of backup and recovery procedures without adversely affecting routine operation.
  - 13.3.5. Data backups should include site configuration information in addition to the user databases to allow full recovery from the supplier's default configuration system.
  - 13.3.6. Operational procedures for data backup should address the following requirements:
    - 13.3.6.1. Backups must be performed on a regular basis, and documented;
    - 13.3.6.2. Backup media must identify the database, backup type (full or incremental) and the date;

- 13.3.6.3. Backup data should be removed from the system and stored in a secure manner in a separate fire zone;
- 13.3.6.4. As a minimum, backup media should be retained long enough to recover from either of the two most recent full backups;
- 13.3.6.5. A backup log should be retained recording date, time and operator name for each backup event.
- 13.3.7. Testing of backup and recovery should be undertaken at regular intervals and documented

#### 14. ELECTRONIC RECORD RETENTION

- 14.1. Record retention requirements are detailed in the Guidance from the Royal College of Pathologists and the Institute of Biomedical Science (2005). Where records are stored electronically, the retention strategy must ensure that not only are records retained for the relevant period, but that they can be accessed. *Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50* require that the information necessary to ensure traceability of the path between donor and patient be retained for at least 30 years.
- 14.2. There needs to be a regular review to ensure that hardware, operating systems and database systems are still being supported. Sufficient documentation should be retained to ensure that the system can be started and the database accessed. It is almost inevitable that systems will need to be replaced at least once during the data retention period. This may simply be to an upgraded version of the database system or transfer to a completely new system. The review will need to ensure that existing data transfer media, such as disks or tape drives, will not become obsolete before such a transfer can be achieved and that the necessary technical knowledge and skills are shared across a sufficient number of people.
- 14.3. With the rapid development of computer systems, it is recommended that such a review should be carried out at least once every 2 years.
- 14.4. A formal record of the review and outcome should be retained as part of the system documentation.
- 14.5. Loss of traceability information due to obsolescence of hardware or software would be a breach of the statutory requirements of the *Blood Safety and Quality Regulations 2005*.

#### 15. SYSTEM AVAILABILITY

- 15.1. Systems will normally need to be available 24 h a day, 7 days a week, but this may vary according to local situations. In all cases, appropriate fallback and support arrangements need to be in place that can deliver the required availability.
  - 15.1.1. Availability requirements must be reflected in network design to ensure adequate network resilience and recovery plans.
  - 15.1.2. For multisite organizations the wide area network configuration must ensure the necessary degree of resilience and recovery.
- 15.2. Procedural backup plans must be in place to maintain continuity of critical transfusion provision.
- 15.3. The limitations of alternative manual systems must be recognized.
- 15.4. The risks associated with system failure must be addressed and an appropriate risk analysis performed [see Internet references (a), (b), (c) and (d) for examples].
- 15.5. A critical failure disaster recovery plan should be in place.
- 15.6. The disaster recovery plan should be periodically tested and reviewed.

#### 16. VALIDATION OF COMPUTER SYSTEMS

- 16.1. All software must be appropriately validated before use. The validation approach required should be determined in accordance with the guidance (GAMP 4) produced by the International Society of Pharmaceutical Engineering (2001).
- 16.2. Validation of any system requires a structured approach (see Appendix 5 for example) and should include the following:
  - 16.2.1. Suitability for intended purpose;
  - 16.2.2. User requirement definition;
  - 16.2.3. Test plans;
  - 16.2.4. Validation of raw data;
  - 16.2.5. Validation report;
  - 16.2.6. Validation of use of check digit;
  - 16.2.7. A functional risk assessment taking into account:
    - 16.2.7.1. The likelihood of the event;
    - 16.2.7.2. Severity of potential consequences.
- 16.3. Test plans should be based on:
  - 16.3.1. User requirement definition;

- 16.3.2. 'High-risk' functions must be challenged thoroughly;
- 16.3.3. Does not allow the issue of ABO-incompatible units;
- 16.3.4. Does not allow the issue of expired blood components/products;
- 16.3.5. Warning flags for special transfusion requirements and local rules where applied;
- 16.3.6. All areas of the user requirement should be tested and demonstrate that all functions needed are available;
- 16.3.7. Interfaces deliver as expected;
- 16.3.8. All logic rules are fully tested under all situations.
- 16.4. Expected results and acceptance criteria should be recorded and all results obtained should be documented, as well as deviations from expected results.
- 16.5. Validation failures
  - 16.5.1. Document all failures;
  - 16.5.2. Investigate to determine if failure was because of the following:
    - 16.5.2.1. Test case was properly written;
    - 16.5.2.2. User error in executing the test;
    - 16.5.2.3. System limitation.

## 17. SYSTEM CHANGES

- 17.1. It is important that further validation of the system is performed when the following occur:
  - 17.1.1. When a system is changed (version updates), there must be a completely new validation, or if the changes are small, a partial validation should be performed;
  - 17.1.2. Following preventative maintenance or other engineer attention to hardware or software, or after automation interfacing to the system;
    - 17.1.2.1. Even minor system changes may have unexpected effects upon functionality, and the user must be vigilant to ensure correct functioning of all aspects of the system;
  - 17.1.3. If a new process is being undertaken, such as electronic issue, additional validation is required relating to the specific functionality of the software;
  - 17.1.4. Changes to user-defined settings may need revalidation of all areas covered by these changes.

## 18. DATA TRANSFER BETWEEN SYSTEMS

- 18.1. Data transfer between legacy and new systems often requires the development of bespoke software elements by the suppliers of both systems.
- 18.2. The database structure of the legacy system will need to be thoroughly reviewed to ensure all data fields and linkages are accounted for and that a positive decision is made and recorded about which fields are and are not to be migrated.
- 18.3. It is critical that the input and output protocols are compatible. In particular, care must be taken to completely and unambiguously map the information between systems giving particular attention to possible differences in definitions of terms used by different suppliers.
- 18.4. Trial transfers of a subset of the database should be performed and carefully checked to ensure correct assignment of information in all scenarios. It is important that this step covers the full range of test outcomes and full patient details and transactions (see Appendix 6).
- 18.5. Details of all records reviewed should be retained.
- 18.6. Transfer software should be designed to identify and report on any unexpected or spurious data found on the legacy system.
- 18.7. Merging/linking of patient records should not be performed while data transfer is being undertaken, unless specifically approved by the system suppliers.
- 18.8. Validation procedures must be performed to allow the accuracy of the data transferred to be verified.
  - 18.8.1. The level of validation required will depend on several factors and should be determined through a risk assessment process.
- 18.9. Where information is not being migrated from the legacy system, consideration needs to be given to the record-keeping requirements for the non-migrated information and, if necessary, steps put in place to ensure ongoing access to this information is retained.
- 18.10. The operational processes to be followed at the time of migration need to be carefully planned. Questions that need to be considered include:
  - 18.10.1. Will there be a period of parallel running?
  - 18.10.2. Will stock be migrated or logged in to the new system?

- 18.10.3. How will cover be provided during the migration process?
- 18.10.4. What is the fallback strategy in the event of migration failure?
- 18.11. Roles and responsibilities of suppliers, laboratory staff and IT departments need to be clearly defined.
- 18.12. Training requirements of the staff who will use the new system need to be met prior to migration. Even minor changes in presentation (such as menu titles or order) can cause serious disruption if not properly prepared for.

## 19. INFORMATION AUDIT TRAILS

- 19.1. Database navigation
  - 19.1.1. To facilitate best practice in transfusion, easy extraction of data is required to enable audit, review of appropriateness of blood component usage and participation in the Blood Stocks Management Scheme.
  - 19.1.2. Systems must provide sufficient indexing to ensure that critical data paths can be readily followed. Examples of such data paths include:
    - 19.1.2.1. From patient record to donation and component details of all transfused units;
    - 19.1.2.2. From donation number to patient name for all transfused components;
    - 19.1.2.3. From patient record to batch number of all products;
    - 19.1.2.4. From product batch number to all patients receiving the product.
- 19.2. The system should be capable of maintaining a permanent audit trail of critical actions associated both with patient records and blood components/products.
  - 19.2.1. Logs will need to be retained for 30 years.
  - 19.2.2. Due to the size of such records, these details may require eventual offline storage.
- 19.3. All details, including initial entry and subsequent amendments/changes and actions, should be logged and recorded associated with a date/time of action, and identification of the individual performing the action.
  - 19.3.1. Recording of any system warning overrides are desirable.
- 19.4. All records should be able to be reviewed and retrospectively searched as necessary.

## 20. MANAGEMENT INFORMATION/ CLINICAL AUDIT DATA

Mention of the following data fields has already been included in the relevant sections but is repeated here as examples of the audits or database searches that may be required as part of the operation of an effective and efficient hospital transfusion department. Where possible, the systems should be configured to enable the production and analysis of this information electronically, which is quicker, less prone to error and more easily verifiable than manually extracted data.

- 20.1. There is a demand for *ad hoc* management information, and the system should be able to support enquiry either by inbuilt query support or by making the database available for external access. It is important that such *ad hoc* enquiry has access to all data items.
  - 20.1.1. Where external query systems are used, access security requirements detailed in §13.1 must continue to be enforced.
  - 20.1.2. Where sophisticated query systems are not available, the blood transfusion system must be able to provide a minimum set of management information as indicated below.
- 20.2. Component/batch product usage statistics
  - 20.2.1. The system should be able to provide flexible, user-defined, usage statistics categorized by one or more of the following:
    - 20.2.1.1. Consultant;
    - 20.2.1.2. Location, e.g. ward/clinical directorate/hospital;
    - 20.2.1.3. By reason for request/clinical diagnosis;
    - 20.2.1.4. Maximum surgical blood ordering schedule (if used);
    - 20.2.1.5. Status of units when issued (uncross-matched, group compatible, cross-match compatible, electronic issue, suitable for, incompatible, etc.);
    - 20.2.1.6. Destination of unit when issued;
    - 20.2.1.7. Type of component/product used;
    - 20.2.1.8. Fate of units, including stock recall;
    - 20.2.1.9. Whether an adverse reaction to a component/batch product has been reported.
- 20.3. Stock information
  - 20.3.1. The system should be able to assess at any time details of both reserved and unreserved stock held by type of unit, group and special characteristics.

- 20.3.2. This should include details of shelf-life of all units (i.e. time to expiry) and be able to give a list of units in order of remaining shelf-life for any unit type and ABO and D groups.
- 20.3.3. The system should be able to give details of stock received, stock used and stock discarded at monthly or other intervals to support the input requirements of the Blood Stocks Management Scheme or equivalent.

## DISCLAIMER

While the advice and information in these guidelines is believed to be true and accurate at the time of going to press, neither the authors, the British Society for Haematology, nor the publishers can accept any legal responsibility or liability for any omissions or errors that may be made.

Where this document refers to English DoH publications, there may be alternative documents in Northern Ireland, Scotland and Wales that need to be considered. Where possible, these have been included in the references.

## REFERENCES

- BCSH (1996) Guidelines for blood grouping and red cell antibody testing in pregnancy. *Transfusion Medicine*, **6**, 71–74.
- BCSH (1999a) Addendum for guidelines for blood grouping and red cell antibody testing during pregnancy. *Transfusion Medicine*, **9**, 99.
- BCSH (1999b) Guidelines for the administration of blood and blood components and the management of transfused patients. *Transfusion Medicine*, **9**, 227–239.
- BCSH (2000) Guidelines for blood bank computing. *Transfusion Medicine*, **10**, 307–314.
- BCSH (2004a) Transfusion guidelines for neonates and older children. *British Journal of Haematology*, **124**, 433–453.
- BCSH (2004b) Guidelines for compatibility procedures in blood transfusion laboratories. *Transfusion Medicine*, **14**, 59–73.
- Better Blood Transfusion documents: England, HSC 2002/009; Northern Ireland, HSS(MD)6/03; Scotland, NHSHDL (2003)19; Wales, WHC2002/137.
- Blood Safety and Quality Regulations 2005: Statutory Instrument 2005/50* (ISBN 0110990412) [WWW document]. URL <http://www.hmso.gov.uk/si/si2005/20050050.htm>.
- BS 7799 Information Security Standard: ISO/IEC 17799 Code of practice for information security management. BS 7799–2:2002 Information security management. Specification with guidance for use. British Standards Institution. URL <http://www.bsi-global.com/TQ3.pdf>.
- Department of Health (2003) *Confidentiality: NHS Code of Practice*.
- Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use.
- Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003 Setting standards of safety and quality for the collection, processing, testing, storage and distribution of human blood and blood components.
- Directive 2004/23/EC of the European Parliament and of the Council on Setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage, and distribution of human tissues and cells.
- Guidance from the Royal College of Pathologists and the Institute of Biomedical Science. (2005) *The Retention and Storage of Pathological Records and Archives* (3rd edn).
- Guidelines for the Blood Transfusion Services in the United Kingdom* (7th edn) (2004) [WWW document]. The Stationery Office. URL <http://www.transfusionguidelines.org.uk>.
- International Society of Blood Transfusion (2003) Guidelines for validation and maintaining the validation state of automated systems in blood banking. *Vox Sanguinis*, **85**(Suppl. 1), S1–S14.
- International Society of Pharmaceutical Engineering (2001) *The Good Automated Manufacturing Practice (GAMP 4) Guide for Validation of Automated Systems in Pharmaceutical Manufacture*.
- Internet (a) URL <http://www.npsa.nhs.uk>
- Internet (b) URL <http://www.apsf.net.au>
- Internet (c) URL <http://www.patientsafety.com.au>
- Internet (d) URL <http://www.consequence.org.uk>
- Mollison, P.L., Engelfriet, C.O. & Contreras, M. (1997) *Blood Transfusion in Clinical Medicine* (10th edn). Blackwell Science Ltd., Oxford.
- Serious Hazards of Transfusion (2003) *Annual Report 2001–2002* (Stainsby, D., Cohen, H., Jones, H., Todd, A., Knowles, S., Taylor, C., Beattie, C., Davison, K., Revill, J., Norfolk, D) (ISBN 0-9532-789-5-6).
- Serious Hazards of Transfusion (2004) *Annual Report 2002–2003* (Stainsby, D., Cohen, H., Jones, H., Knowles, S., Milkins, C., Chapman, C., Gibson, B., Davison, K., Norfolk, D., Taylor, C., Revill, J., Asher, D., Atterbury, C., Gray, A) (ISBN 0-9532-789-6-4).
- UKBTS Standing Advisory Committee on Information Technology, Barcode Committee (1998) *Specification for the Uniform Labelling of Blood and Blood Components (Version 4.1)*.

## APPENDIX 1

### *Levels of evidence*

The definitions of the types of evidence and the grading recommendations used in this guideline originate from the US Agency for Health Care Policy and Research and are listed below.

### *Statements of evidence*

- Ia Evidence obtained from meta-analysis of randomized controlled trials.
- Ib Evidence obtained from at least one randomized controlled trial.
- IIa Evidence obtained from at least one well-designed controlled study without randomization.
- IIb Evidence obtained from at least one other type of well-designed quasi-experimental study.
- III Evidence obtained from well-designed non-experimental descriptive studies, such as comparative studies, correlation studies and case studies.
- IV Evidence obtained from expert committee reports or opinions and/or clinical experiences of respected authorities.

### *Grades of recommendations*

- A Requires at least one randomized controlled trial as part of a body of literature of overall good quality and consistency addressing the specific recommendation (evidence levels Ia and Ib).
- B Requires the availability of well-conducted clinical studies but no randomized clinical trials on the topic of recommendation (evidence levels IIa, IIb and III).
- C Requires evidence obtained from expert committee reports or opinions and/or clinical experiences of respected authorities. Indicates an absence of directly applicable clinical studies of good quality (evidence level IV)

## APPENDIX 2

### *Glossary*

A/E: Accident and Emergency Department  
 AHG: Anti-human globulin  
 BBTS: British Blood Transfusion Society  
 BCSH: British Committee for Standards in Haematology  
 BTLP: Blood Transfusion Laboratory Practice  
 CMV: Cytomegalovirus  
 Codabar: An early bar code system that only allows the bar coding of digits and a small number of other

non-alphabetic characters. Widely used in blood labelling but being replaced by the ISBT 128 standard

Code 128: A linear bar code system that encodes all numeric, and upper- and lower-case alphabetic characters, plus other symbols. Allows higher density packing of data, particularly numeric data allowing much more information to be stored in less space than Codabar

DAT: Direct antiglobulin test

DOB: Date of birth

DoH: Department of Health

EC: Commission of the European Communities

EQA: External quality assessment

EU: European Union

FFP: Fresh frozen plasma

GAMP: Good Automated Manufacturing Practice

HDN: Haemolytic disease of the newborn

HSC: Health Service Circular

ISBT: International Society for Blood Transfusion

ISBT 128: International information standard for transfusion and transplantation. Where ISBT 128 information is transmitted using linear bar codes, the Code 128 bar code standard is used

IT: Information technology

UKNEQAS: UK National External Quality Assessment Scheme

NHS: National Health Service

NIBSC: National Institute of Biological Standards and Controls

PAS: Patient administration system

SHOT: Serious Hazards of Transfusion

SNOMED-CT: Systematized nomenclature of medicine – clinical terms

UKBTS: UK Blood Transfusion Services

UPN: Unique patient number

## APPENDIX 3

### *Audit checklist*

- 1 Review procedure for allocation and control of database administrator access rights. Ensure a list of authorized persons is available and appropriate.
- 2 Confirm that the system requires Database Administrator passwords to be changed at regular intervals.
- 3 Review the system documentation set. Check the last recorded update, and gain confirmation that no further configuration changes have occurred since this date.
- 4 Verify that hardware configurations and operating system and application versions and configurations are accurately reflected in the system documentation.

- 5 Review backup logs to ensure regular documented backups are occurring.
- 6 Examine storage conditions for backup media to ensure that they are stored remotely from the live database, are secure and are protected from fire and flooding risks.
- 7 Check for last backup recovery exercise. Ensure the exercise demonstrated full recovery and normal operation of the recovered system.
- 8 Ensure that there is evidence of a record retention review to ensure that all information required to meet mandatory requirements is available, secure and protected from obsolescence.
- 9 Confirm that system support contracts reflect the availability requirements of the system in terms of response windows and response times.
- 10 Ensure that fallback procedures exist and have been tested for continuity of service provision in the event of system downtime.
- 11 Confirm that a disaster recovery plan is in place, works and has been successfully tested.

**17 APPENDIX 4. Minimum data set requirements**

Criteria to be included	Minimum data set supported by IT system	Minimum data for manual requesting of tests within laboratory	Minimum data required for ward-based electronic requesting
Surname	X	X	X
Forename	X	X	X
DOB	X	X	X
Sex	X	X	X
Hospital number (or A/E or major incident number)	X	X	X
NHS number	X	Optional	Optional
Date/time request made	X	X	X
Unique request reference number	X	X	X
Consultant responsible for this admission episode	X	X	X
Ward or clinic	X	X	X
Patient address	X	Optional	Optional
Request type (e.g. group/screen, crossmatch)	X	X	X
Reason for request	X	X (Coded)	X
Requesting doctor/contact details or designated nurse	X	X	X
Type of component	X	X	X
Special transfusion requirements	X	With local logic rules	X
Number of units required	X	X	X
Date/time component(s) required	X	X	X
Blood group	X	Optional	Optional
Previous transfusion (y/n)	X	Optional	Optional
Pregnancy history (antibodies, HDN)	X	Optional	Optional
Gestation at time of sample collection	X	Optional	Optional
Known antibodies	X	Optional	Optional
High-risk indicator	X	Optional	Optional
Diagnosis	X	X	X
Electronic signature with adequate security features	X		X
Urgency of request	X	X	X
Electronic crossmatch suitability	X		
If merged/linked patient information	X		
If major incident admission	X		
If amendment of PID made	X		

**APPENDIX 5.** Example of possible validation sheet

Reference software version	Computer validation sheet	Page 1 of 1
Issue date	Title: ABO and D Grouping	Test date

Script written by: ..... Approved by: .....

Modules used: Request Entry/Result Entry/Validation/Printing

Acceptance testing performed by: .....

No.	Description	Expected results	Comment	Pass/Fail
1	Data entry	Patient information recorded		
2	Test requested	Test profiles requested		
3	Transfer of results from automated equipment	Results transmitted as +/-/?		
4	Assigns ABO and D results	Correct result assigned		
5	Validation	Searches for historical result validated vs. historical/current data		
6	Print	All validated forms are printed		

RESULT: PASS/FAIL

TESTER: Signature: ..... Date: .....

ACCEPTED BY: Signature: ..... Date: .....

**APPENDIX 6***Trial transfer data checking*

Prior to data migration between systems, a trial migration should be carried out and the migrated data checked to ensure correct transfer and interpretation. The following list provides some pointers to the scope of checking required but is not exhaustive:

- Patients of each ABO and D group;
- Patients with irregular antibodies;
- Patients linked to every component/product that was held in the 'old system';
- Merged/linked patient records, especially with component/product issues on each record;
- Patients with critical notes/special transfusion requirements;
- Multitransfused patients;
- Patients with DAT and other miscellaneous test results;
- Patients with foetomaternal haemorrhage results and anti-D issued:
  - During pregnancy;
  - Post-delivery;
  - To ward, general practitioners, midwives, etc.;
- Patients who have received a massive transfusion;
- Multiple components/products in a single transfusion episode;
- Where possible, patients with multiple events (as above) attached to a single sample or patient record.

# Author Query Form

**Journal: Transfusion Medicine**

**Article: tme\_743**

Dear Author,

During the copy-editing of your paper, the following queries arose. Please respond to these by marking up your proofs with the necessary changes/additions. Please write your answers on the query sheet if there is insufficient space on the page proofs. Please write clearly and follow the conventions shown on the attached corrections sheet. If returning the proof by fax do not write too close to the paper's edge. Please remember that illegible mark-ups may delay publication.

Many thanks for your assistance.

Query No.	Query	Remark
1	Please check if the short title provided is appropriate.	
2	Please note that the year '2004' has been introduced from the reference list.	
3	Please provide the accessed date for Blood Safety and Quality Regulations 2005, Statutory Instrument 2005/50.	
4	Please provide the accessed date for BS 7799 Information Security Standard.	
5	Please provide the name and location of the publisher (if any) for Department of Health (2003).	
6	Please provide the name and location of the publisher for Guidance from the Royal College of Pathologists and the Institute of Biomedical Science (2005).	
7	Please provide the accessed date for <i>Guidelines for the Blood Transfusion Services in the United Kingdom</i> (2004).	
8	Please provide the name and location of the publisher for International Society of Pharmaceutical Engineering (2001).	
9	Please provide the complete details (e.g., accessed date) for Internet (a).	
10	Please provide the complete details (e.g., accessed date) for Internet (b).	
11	Please provide the complete details (e.g., accessed date) for Internet (c).	
12	Please provide the complete details (e.g., accessed date) for Internet (d).	
13	Please note that Mollison <i>et al.</i> (1997) is not cited. Please include in-text citation or delete from the list.	
14	Please check if the names given in brackets should be given as authors. Also, please provide the location of the publisher and check whether Serious Hazards of Transfusion should be given as the publisher for Serious Hazards of Transfusion (2003).	

---

15 Please check if the names given in brackets should be given as authors. Also, please provide the location of the publisher and check whether Serious Hazards of Transfusion should be given as the publisher for Serious Hazards of Transfusion (2004).

---

16 Please provide the name and location of the publisher for UKBTS (1998).

---

17 Please spell out PID in the table of Appendix 4.

---

UNCORRECTED PROOF

# MARKED PROOF

## Please correct and return this set

Please use the proof correction marks shown below for all alterations and corrections. If you wish to return your proof by fax you should ensure that all amendments are written clearly in dark ink and are made well within the page margins.

<i>Instruction to printer</i>	<i>Textual mark</i>	<i>Marginal mark</i>
Leave unchanged	... under matter to remain	Ⓟ
Insert in text the matter indicated in the margin	∧	New matter followed by ∧ or ∧ <sup>Ⓢ</sup>
Delete	/ through single character, rule or underline or ┌───┐ through all characters to be deleted	Ⓞ or Ⓞ <sup>Ⓢ</sup>
Substitute character or substitute part of one or more word(s)	/ through letter or ┌───┐ through characters	new character / or new characters /
Change to italics	— under matter to be changed	↙
Change to capitals	≡ under matter to be changed	≡
Change to small capitals	≡ under matter to be changed	≡
Change to bold type	~ under matter to be changed	~
Change to bold italic	≈ under matter to be changed	≈
Change to lower case	Encircle matter to be changed	≡
Change italic to upright type	(As above)	⊕
Change bold to non-bold type	(As above)	⊖
Insert 'superior' character	/ through character or ∧ where required	Υ or Υ under character e.g. Υ or Υ
Insert 'inferior' character	(As above)	∧ over character e.g. ∧
Insert full stop	(As above)	⊙
Insert comma	(As above)	,
Insert single quotation marks	(As above)	ʹ or ʸ and/or ʹ or ʸ
Insert double quotation marks	(As above)	“ or ” and/or ” or ”
Insert hyphen	(As above)	⊥
Start new paragraph	┌	┌
No new paragraph	┐	┐
Transpose	└┘	└┘
Close up	linking ○ characters	○
Insert or substitute space between characters or words	/ through character or ∧ where required	Υ
Reduce space between characters or words		↑