Medicines & Healthcare products
Regulatory Agency

MHRA
Regulating Medicines and Medical Devices

Guidance on Transfusion IT Systems

This guidance has been produced in conjunction with the MHRA Blood Consultative Committee following concerns expressed by both transfusion laboratory staff and the MHRA Inspectorate division. The concerns included:

1. That Laboratory Information Management Systems (LIMS) for Blood Transfusion may not be compliant, particularly in hospitals, because of the disparate nature of IT management in hospitals.
2. That IT system developers and providers are not fully appreciative of the legal requirements relating to transfusion (which represents a comparatively small section of the Pathology IT market).
3. That regulatory compliance is not consistently being met with regard to IT systems, and that the issues are being found to be reasonably widespread by MHRA GMP inspectors during recent inspection cycles.

This guidance is relevant to both software suppliers and users of LIMS and those who support and manage IT systems within transfusion laboratories, establishments and any healthcare organisations where blood transfusion activities are undertaken.

The task and finish group included representation from the MHRA, hospital transfusion laboratories and the UK blood transfusion services.

Clarification of regulatory aspects with regards to the IVDD/Medical Device Directive

Laboratory Information Management Systems (LIMS) such as those IT systems used within transfusion and LIMS used elsewhere in pathology are not qualified as medical devices or In-vitro diagnostic medical devices. However modules which are intended to be used with LIMS may be regulated as medical devices if they are intended to directly influence the medical treatment a patient receives by providing some sort of automated reasoning (e.g. dosage calculation, clinical decision support or clinical decision making functionality). However LIMS themselves are essentially information management systems whose purpose is primarily the storage and transmission of data. The MHRA are currently working with relevant stakeholders including NHSBT to clarify which modules are IVDs and how the legislation may be applied.

Data Quality, Merging and Governance

Poor quality data creates unacceptable risk with respect to patient safety .and organisations have a responsibility to ensure the quality of data is not compromised. Where the quality of data with respect to patient ID is poor those data sets should be discarded rather than accepted in cases of partial patient identity.

The implementation of a new LIMS, especially where this involves a change in system, represents significant risk of perpetuating poor historical data as any data taken on from a legacy systems requires substantial control and validation of the quality of the data from transfusion departments and this is not often fully understood by management groups from other areas.

When merging patients the following should be followed:

1. Ensure there is a full and complete patient identification record
2. If there is a transfusion history that is discrepant ensure a root cause can be identified and documented (e.g. Transplant) before proceeding
3. Identify requirements for the system involved in merging
    a. Manual – knowledge, training and a strict protocol to follow
    b. Electronic:
        i. Rule based when there is a discrepant transfusion history
        ii. Discrepancy in patient identification = no merge
4. Ensure there is a robust and validated interface between the LIMS and any other system involved and that any such interfaced system is not able to overwrite patient demographic or transfusion data on the transfusion module of a LIMS without being subject to the same merge controls as the LIMS.

Further guidance is provided in the BCSH Guidelines for the specification, implementation and management of IT systems in hospital transfusion laboratories (2013) and in GAMP5 which has guidance on data migration and in particular its validation.

Particular concern has been raised about control of data transferred from outside of transfusion IT systems, these interfaced systems are subject to the same regulatory requirements as the transfusion specific IT. Implementation of new interfaced systems represent a similar risk to transfusion data as a new LIMS and must be subject to the same considerations of control and validation as when implementing a new LIMS.

Therefore Pathology, and in particular transfusion departments, need to be party to organisational decision making in regard to relevant IT systems (PAS, Order Comms etc.). Organisational decisions taken regarding these systems should be taken and agreed at the Pathology Executive Board meetings and any planned changes to systems signed off by this Board. The departments responsible for these systems external to transfusion IT should work with transfusion departments to ensure their processes and documentation meet GMP requirements e.g. validation and change control.

Supplier Leverage

It is critical when procuring a new IT system that the user requirements are fully specified for every aspect of the system. A supplier audit may be essential depending on the output of the system and GAMP category e.g. non configurable, off the shelf systems in common use may not require a supplier audit but the more complex GAMP category 4 and 5 systems will require a supplier audit to demonstrate the existence of a robust quality management system and practical application of the principles of GAMP.

All new systems and updates to current systems must be managed under change control and qualification procedures that meet GMP requirements with the full involvement of transfusion laboratory management. These procedures should ensure not only that the user requirements as specified have been met but that the operational pathways developed for use with the system are robust and meet GMP, regulatory guidance and professional guidance.

Recommendations made by professional organisations (e.g. BCSH, SHOT) should be supported especially where it is identified as a patient safety issue.

Technical support and maintenance

There must be an SLA between the transfusion department and the IT support team (unless this is an "in house" team) but where this is outsourced this must comply with the requirements of Chapter 7 Outsourced Activities in Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use (Vol. 4)

This document must identify:

- Clears lines of responsibility and accountability between IT support provider and Blood Transfusion department.
- The mechanism by which hardware and software updates are controlled.
- Provision of a robust mechanism(s) for the security of data held
- How disaster recovery of data will be achieved.
- The approved mechanism by which data may be archived.
- How data retention and the traceability strategy will be managed
- Responsibility and mechanisms for maintaining data quality, particularly around merging of records. Staff having access to merge records must have undergone specific training, including GMP/GxP requirements, and have protected access rights.

Contingency

Systems will normally need to be available 24 hours a day, seven days a week, but this may vary according to local situations. Contingency plans that detail appropriate fallback and support arrangements need to be in place to ensure continued service delivery in the absence of the IT system, including scheduled downtime for maintenance and upgrades as well as unscheduled downtime. Availability requirements must be reflected in system and network design and maintenance/ support arrangements. These must cover all appropriate software, hardware and network systems.

All transfusion IT systems must have a back up plan to ensure full data recovery in the event of catastrophic system failure. The backup process must be documented and validated and regularly tested to demonstrate its ongoing effectiveness.

Learning from failure

Information identified from investigating any IT failures that have or could affect transfusion can, if suitably reported and disseminated heighten awareness of the pitfalls in specifying, validating and operating such systems and help prevent similar occurrences.

Any incident arising from the use of transfusion IT systems, peripheral equipment or interfaces to *in vitro* diagnostic (IVD) medical devices/accessories that might impact on patient safety or the efficient running of the transfusion department, either directly or indirectly, must be logged on the laboratory's adverse incident system and, where appropriate, be reported to the MHRA either to SABRE or the Devices division. Failure to do so may put other patients at risk where laboratories are using the same equipment and may not have experienced or recognised a similar problem.

Prepared on behalf of the MHRA BCC IT Task & Finish Group

October 2014