10 Information Technology (IT) Incidents

Authors: Megan Rowley and Paula Bolton-Maggs

Since 2007, the Annual SHOT Report has included a detailed analysis of transfusion adverse events related to laboratory information management systems (LIMS) as well as other information technology (IT) systems used in hospital transfusion service delivery. This year we have not undertaken an in-depth analysis but have taken the opportunity to reflect on the recurrent IT-related themes identified year-on-year and to review key messages and recommendations made in previous annual reports. The aim was to see if SHOT messages about IT remain valid, to summarise whether any progress has been made to prevent IT-related errors and to apply 'human factors' thinking and methodology to the 'human-computer' interface!

Each year an increasing number of cases have been identified where IT systems may have **caused** (or contributed) to the errors reported, have been **used incorrectly** resulting in an error or where IT systems **could have prevented** errors but were not used. A recent patient safety report also noted that with increasingly complex care 'the increasing reliance on IT in healthcare can threaten patient safety' (Yu et al. 2016). The SHOT IT system messages fall into 4 broad categories:

1. **Promoting** the benefits of existing IT systems, and **developing** new IT systems, to aid transfusion safety recognising that national standardised specifications are essential to ensure systems support compliance with regulations, guidelines and emerging clinical requirements.

   The benefits of IT systems to support safe transfusion practice are many including: LIMS configuration to prevent issue of ABO-incompatible blood; algorithms for electronic issue of blood; alerts, warnings and logic rules to ensure specific requirements are met; widely accessible databases of patients with complex transfusion requirements; vein-to-vein electronic blood management systems to support giving the 'right blood' to the 'right patient'.

   There are now national and international specifications for IT systems to support safe blood transfusion practice and to structure the important dialogue between manufacturers and hospital transfusion services. The recent National Institute for Health and Care Excellence (NICE) transfusion guidelines recommend electronic patient blood management systems (NICE 2015) and a business case with evidence has been published based on data from Oxford (OUH 2016).

2. **Validating** IT systems to ensure they are configured correctly by using a broad range of scenarios covering the whole spectrum of transfusion practice. This applies to new systems but is equally important when existing systems are upgraded.

   Validation is costly and time consuming but essential to ensure that IT systems are working as intended. SHOT has repeatedly shown that incompletely validated systems can put patients at risk.

   We rely on IT systems in transfusion as a fail-safe mechanism to protect patients from receiving the wrong blood. It is important to still have an understanding of correct practice so that, when IT systems fail, the people operating the systems are in a position to detect and correct the errors.

3. **Training** all clinical and laboratory staff to use IT systems correctly and as intended. This includes communicating the very real risk to patient safety that exists where flags, alerts and warnings are bypassed in an IT system designed to protect patients from wrong blood incidents. Training should cover both routine and emergency situations so that IT systems support both safe and timely blood supply.

The importance of training and assessment of competence to use IT systems in the laboratory and clinical setting cannot be overemphasised. SHOT errors, and audits of transfusion practice, show how people are able to circumvent the barriers and prompts put in place.

Examples where training has not been adequate include: overriding or ignoring error messages for ABO-incompatible blood or specific requirements; using other people's identification (ID) badges (or logon details) to gain unauthorised access to remote issue refrigerators; being unable to issue blood resulting in delay because of unfamiliarity with standard operating procedures (SOP) for the LIMS.

4. **Ensuring accuracy** and security of data transfer across electronic interfaces to minimise error-prone manual transcription of data to and from IT systems.

   Despite the national guidance to healthcare providers to use transferrable unique patient numbers (National Health Service (NHS) number, community health index (CHI) number) the uptake of this has been incomplete. Transfusion errors arise when patients move from hospital to hospital, or where hospitals and/or transfusion departments merge, and computer records are not accessible, visible or robustly linked or merged.

   Inevitably there are some manual steps in the transfusion process but these can be minimised. The Medicines and Healthcare Products Regulatory Agency (MHRA) have issued guidance that electronic issue of blood components should not be possible if there is a manual step in the process but not all laboratories can comply with this because of their LIMS systems.

   In some situations, and SHOT has shown maternity records as an example, there is no computer interface between laboratory and clinical systems so data has to be transcribed manually. This has led to both incorrect administration of anti-D immunoglobulin (Ig) to women with immune anti-D and omission of anti-D Ig in D-negative women because the wrong blood group or antibody screen result has been copied over.

COMMENTARY

IT systems are increasingly used to make blood transfusion safer but, in 2015, SHOT reports show the same pattern of IT system errors. This means that the full benefit of the protection for patients afforded by IT systems has not been realised and there is room for improvement. It is both an individual and organisational responsibility to ensure that IT systems that have been shown to improve transfusion safety are specified correctly and validated thoroughly. Training to use IT systems needs careful planning and to be adequately resourced because healthcare staff who use them need to understand their limitations and understand the consequences of using them incorrectly.

Case examples:

Case 10.1 (Case 6.1 in Chapter 6, Incorrect Blood Components Transfused): ABO-incompatible transfusion permitted by electronic issue (EI)

Case 10.2: Failure of correct bedside check

In 2014 one hospital noted after audit that 273 units were transfused by 105 different staff bypassing the final bedside check because the BloodTrack system had been set up to suit local preferences rather than as the manufacturer intended (staff using the emergency mode intended only for emergency O D-negative units on the personal digital assistant (PDA) to administer blood components that had been grouped and issued for a named patient). This was reported in the Annual SHOT Report 2014, Chapter 12, Summary of Errors Related to Information Technology.

Surprisingly, in 2015 SHOT received a further report from the same hospital concerning 162 units transfused by 58 further members of staff in the same way over 11 months, indicating that their corrective action had not been effective. Each of these had the potential for ABO-incompatibility if a wrong unit was selected. A poster was issued to all clinical areas and was on all the crash trolleys; the staff involved received further training but clearly this was not sufficient. The company introduced new software in

November 2015, but this has taken time to implement because the company has to build 125 secure digital (SD) cards, one for each PDA. This shows how very difficult it can be to catch the horse after it has bolted, to change wrong practice in a very large hospital, leaving patients at risk for a further 12 months.

Case 10.3: Electronic prescribing system in paediatric intensive care defaults to adult units

A 2 month-old child was prescribed 65mL of red cells over 2 hours in a paediatric intensive care unit, but the electronic prescribing system (for intensive care) automatically defaulted to one adult unit over 2 hours so the child received 141mL before the error was recognised but suffered no ill effects.

Case 10.4: (Case 8.4 in Chapter 8, Near Miss Reporting) WBIT shows a secure electronic labelling system was being used incorrectly

References

BCSH Jones J et al. (2014) **Guidelines for the specification, implementation and management of information technology (IT) systems in hospital transfusion laboratories**. Transfus Med 24, 341-71

BCSH Allard S, Burgess G et al. (2012) **Guidelines for validation and qualification, including change control, for hospital transfusion laboratories**. Transfus Med 22, 5-43

Karsh BT, Weinger MB et al. (2010) **Health information technology: fallacies and sober realities**. J Am Med Inform Assoc 17, 617-23

MHRA (2010) **Guidance on Electronic Issue**. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/449059/MHRA_Guidance_on_Electronic_Issue_new_logo.pdf [accessed 27 April 2016]

NICE (2015) **Guidance: Blood Transfusion** (NG24). https://www.nice.org.uk/guidance/ng24 [accessed 27 April 2016]

Oxford University Hospitals (OUH) (2011 updated 2016) **Electronic blood transfusion: improving safety and efficiency of transfusion systems**. https://www.nice.org.uk/localPractice/collection [accessed 25 March 2016]

Yu A, Flott K et al. (2016) **Patient safety 2030**. London, UK: NIHR Imperial Patient Safety Translational Research Centre http://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/centre-for-health-policy/Patient-Safety-2030-Report-VFinal.pdf [accessed 13 April 2016]