Information Technology (IT) Incidents 13

Author: Megan Rowley

Definition:

This chapter covers transfusion adverse events that relate to laboratory information management systems (LIMS) as well as other IT systems and related equipment used in the delivery of hospital transfusion services.

Cases selected include events where IT systems may have caused or contributed to the errors reported, where IT systems have been used incorrectly and also includes cases where IT systems could have prevented errors but were not used. Where the corrective and preventive action suggested by hospitals in response to errors included IT solutions, these have been included.

Key SHOT messages

- **Knowledge and training** – IT systems can make transfusion safer by supporting and controlling clinical and laboratory tasks but they do not replace knowledge about the supported task and are only safe if timely and accurate training to undertake the role is provided. You can not rely on IT to replace knowledge – you need both
- **Leadership, supervision and personal responsibility** – Although procurement and implementation of new IT systems, or system upgrades, require the leadership of subject matter experts (SME) it should be the responsibility of managers and supervisory staff to ensure appropriate role-based training and for individuals to ensure that they are trained and confident in their use of systems, including a clear understanding of the limitations of these systems
- **IT, electronic systems and equipment 'fit for purpose'** – The design and configuration of IT, and other electronic systems, has to meet current requirements and be flexible enough to take account of developments in blood safety and changes in practice, whether they be anticipated or unexpected. Analysis of SHOT errors has shown weaknesses in some systems and this information should be taken into account for the benefit of all when upgrading existing or developing new systems. There is a challenge for software and equipment providers to listen to and work with the UK transfusion community so that together we can maximize the promise of IT and electronic systems for patient benefit. Using alerts, warnings and flags as an example – we need to learn from what works well, share good practice and standardise
- **Sharing information** – Communication is critical to good care in transfusion practice but lack of connectivity and interoperability between IT systems repeatedly fails to enhance the potential benefits of secure electronic transfer of information. Any manual steps required to transfer or transcribe information introduce a source of error and potential delay. There could be, and should be, IT solutions to make test results and other information available between hospitals, between hospital and reference laboratories and also across country boundaries. This would improve the care of complex and shared care patients, and also improve the experience of patients who have repeated samples because their care is delivered in more than one healthcare setting

In 2016 there were 297 reported incidents of errors related to IT systems. The cases included are drawn from the other chapters of this report as shown in Table 13.1 and these are categorised in Table 13.2 according to the errors and the reason for the error based on the reporter's classification and the author's interpretation of the report. The commentary relating to these cases is included in the relevant chapters.

Table 13.1: Source of cases containing errors related to information technology

Error	2016
Incorrect blood component transfused (IBCT-WCT)	29
Specific requirements not met (SRNM)	161
Right blood right patient (RBRP)	57
Avoidable, delayed and undertransfusion (ADU)	26
Handling and storage errors (HSE)	3
Total	**276**
Anti-D immunoglobulin (Ig) errors (Anti-D Ig)	21
Total including anti-D	**297**

In 2016, 57.9% (172/297) of the IT incidents originated in the transfusion laboratory and 42.1% (125/297) originated in the clinical area.

Excluding the anti-D Ig cases and where the relevant information was provided by the reporter, the majority of incidents related to transfusion in adults (230/262 87.8%) with 20 cases in children under 18 years and 12 cases in neonates or infants. The incident involved red cells in 210/273, 76.9%, platelets in 25/273, 9.2%, FFP/cryoprecipitate in 23/273, 8.4% and multiple components in 15/273, 5.5% of cases where the component was stated. Most incidents were said to take place in normal working hours 138/178, 77.5%, but there were many cases where a specific time was not recorded. Where the urgency of the transfusion was stated 149/257, 58.0%, were classified 'routine', 80/257, 31.1% 'urgent' and 28/257, 10.9% 'emergency' cases.

Deaths n=0

There were no transfusion-related deaths where IT systems contributed.

Major morbidity n=3

There were two cases with major morbidity due to alloimmunisation in women of childbearing potential. These both developed anti-K as a result of transfusion of K-positive red cells. A third case suffered serious haemolysis due to anti-S where IT systems contributed.

Minor or moderate morbidity n=6

There was an additional case of significant haemolysis in a solid organ transplant patient where IT systems contributed to moderate morbidity.

There were two cases classified as minor morbidity who were alloimmunised (anti-e and anti-c) but with no haemolytic transfusion reaction where incorrect use of IT systems contributed.

There were two delays where surgery was cancelled because blood components were not available (minor morbidity) and following another blood delay the patient died due to underlying injuries, not blood delay.

All the other cases did not result in any harm to the recipient of the components transfused.

IT flags, alerts and warnings

Once again nearly half of the errors (48.2%, 133/276) related to IT systems can be attributed to the failure in some way of laboratory information management systems (LIMS) and electronic blood management systems (EBMS) to prevent wrong blood and missed specific requirements including 'right blood, right patient errors' where there was a discrepancy in one of the core patient identifiers but blood was still issued, collected, checked at the bedside and administered.

Whilst robust clinical systems for identifying patients and communicating their age- gender- or disease-specific requirements to the transfusion laboratory cannot be replaced with IT systems, it is disappointing that the functionality of these systems has not been standardised so that clinical and laboratory users can have the confidence that ABO-incompatible red cell transfusion will be prevented and that complex and vulnerable patients can receive blood components of the exact specification they require.

An example in 2016 was the introduction of hepatitis E virus (HEV)-screened components for allogeneic haemopoietic stem cell transplant (HSCT) and solid organ transplant (SOT) patients. This was widely discussed and debated before implementation and yet, at the point of implementation, not all LIMS systems were able to provide this new alert with the result that there were 23 cases where failure to use the LIMS correctly to flag these patients was the predominant cause of failure to provide HEV-screened components (21/23).

In previous SHOT reports, and at the SHOT symposia, we have been encouraged to learn as much from **what goes right** as well as learning from the relatively small numbers of human and system failures reported to SHOT. In this spirit we should critically review the methods for existing flags, alerts and warnings used by the software in clinical and laboratory use in the UK and decide what works best in different situations. It should no longer be acceptable to tolerate workarounds and patches that can solve one problem only to create another unanticipated effect.

Recommendation

- Clinicians, laboratory scientists, information technology (IT) professionals and IT providers should work together to develop an industry standard for flags, alerts and warnings that prevent harm from wrong blood but still ensure timely and accurate availability of blood components for clinical use

Action: IT/software providers with UK Transfusion Laboratory Collaborative

IT vulnerability: Serious Trust/Health Board-wide IT incidents

In 2016 two large Trusts in England had serious problems with their IT systems.

Failure of the pathology IT system

At the first site the laboratory information system failed. This was supporting three different hospitals. The root cause of this was progressive failure of 3 hard drives where hardware warnings had not been acted on. The back-up processes had also not been robust leading to difficulty in restoration. The LIMS was not available for blood transfusion for a total of 8 days and in the interim arrangements were made with other hospital laboratories to perform the analyses and return the results. Elective surgery was cancelled. This downtime resulted in 27 SHOT-reportable incidents (25 SRNM, 1 HSE and 1 RBRP).

The second site identified an issue with malevolent intrusion which threatened all of the IT support.

Incident affecting two linked Trusts/Health Boards (T/HB-1 and T/HB-2)

T/HB-1 was subject to a type of malware attack known as ‘ransomware’. Manual systems were quickly put in place in order to continue some services. T/HB-1 is part of a networked organisation and is linked to a second Trust/Health Board (T/HB-2).

Throughout the incident the pathology laboratory information management system (LIMS) was not affected or switched off, because it uses a different IT language and was not considered at risk. Therefore, LIMS access for T/HB-1 was maintained throughout the incident, but staff at T/HB-2 took the decision to sever the IT links with T/HB-1 until they could be assured there was no risk to their systems from the ransomware.

As T/HB-1 pathology was fully functional, non-urgent work from T/HB-2 sites was transferred to T/HB-1 sites. For any transfusion work that could not be transferred, T/HB-1 staff were able to provide patient history to staff on T/HB-2 sites, because the LIMS had shared patient records across all sites.

The incident review demonstrated that not all sites had the required paper copies of documents critical to service provision in the event of IT failure. No site was without access to key information or documents during the incident, because these were available on other sites and shared either by fax or email.

No SHOT or MHRA-reportable incidents occurred during this IT downtime.

Learning points

- Trusts/Health Boards should evaluate what documentation might be required in the event of IT failure and ensure paper master copies are available wherever needed
- Trusts/Health Boards should test cyber security regularly, including network threat monitoring and have a cyber incident response contract in place for expert advice during an incident

Table 13.2: Summary of errors related to information technology

Error	Reports	Right BC	Wrong BC	Unit transfused when specific requirements not met						Wrong group HSCT/SOT	HSE	ADU
				Not irradiated	Not CMV	Not VIP	Not phenotyped	Not HLA-matched	Not HEV-			
Failure to consult or identify historical record	**36**	-	3	11	5	-	13	-	2	1	-	1
Failure to link, merge or reconcile computer records	**13**	6	-	1	-	-	4	-	-	-	-	2
Wrong record selected on LIMS or PAS	**9**	6	-	1	-	-	-	-	-	-	-	2
Warning flag in place but not heeded	**22**	-	5	5	-	1	3	-	2	4	-	2
Warning flag not updated or removed in error	**20**	-	1	11	-	-	4	-	4	-	-	-
Failure to use flags and/or logic rules	**91**	-	1	45	-	7	11	3	15	6	1	2
Computer or other IT systems failure	**7**	1	2	-	-	-	-	-	-	-	-	4
Errors related to computer system	**5**	-	-	-	-	-	-	-	-	-	-	5
Errors related to electronic blood management system	**8**	1	2	-	-	-	-	-	-	-	1	4
Other equipment failure	**7**	2	-	-	-	-	1	-	-	-	2	2
Incorrect result or data entered or accessed manually	**23**	18	2	-	-	-	2	-	-	-	-	1
Discrepancy between LIMS and PAS	**13**	12	-	-	-	-	-	-	-	-	-	1
Blood issued against wrong patient ID (sample or request form)	**11**	10	1	-	-	-	-	-	-	-	-	-
Electronic blood ordering/OBOS	**7**	-	1	-	-	5	-	1	-	-	-	-
Crossmatched blood labelled as uncrossmatched	**1**	1	-	-	-	-	-	-	-	-	-	-
Inappropriate EI (+17 counted in another category)	**3**	-	(1)	-	-	-	3 (13)	(1)	-	(1)	-	(1)
Totals	**276**	**57**	**18**	**74**	**5**	**13**	**41**	**4**	**23**	**11**	**4**	**26**

BC=blood component; CMV=cytomegalovirus; VIP=virally inactivated plasma; HLA=human leucocyte antigen; PAS=patient administration system; EI=electronic issue