SHOT Privacy Notice

Serious Hazards of Transfusion (SHOT) Privacy Notice

Version 4.0, 02/07/2019

Right to access and control how your data is used

Everyone has a right:

- to be informed about how your data is used. It is the intention of this document to give you an overview of how SHOT uses your data
- to request a copy of the information we may hold about you
- to update or amend the information we may hold about you if it is wrong
- to change your communication or marketing preferences at any time
- to erasure (also called the right to be forgotten). Applications to apply this right will be considered by SHOT on a case by case basis
- to restrict how your data is processed
- to raise a concern or complaint about the way in which your information is being used.

The Data Protection Officer

Our Data Protection Officer (DPO) is provided by NHS Blood and Transplant. The DPO for NHSBT is Katrina Smith, the Head of Information Governance, who is responsible for ensuring that all practices and processes within SHOT are designed to support people’s privacy and data rights and making sure data protection is represented at a board level.

You can contact the Data Protection Officer if you have any questions or concerns about your privacy rights within SHOT via: katrina.smith@nhsbt.nhs.uk.

What is the SHOT database?

The SHOT database is the haemovigilance database for adverse events and reactions in blood transfusion reported by healthcare organisations that are involved in the transfusion of blood and blood components in the United Kingdom. The information in the database will be used to identify risks and problems, from which SHOT produces recommendations to improve patient safety. The recommendations are published in the Annual SHOT Report which is then circulated to all the relevant organisations including hospitals, the four UK Blood Services, the Departments of Health in England, Wales, Scotland and Northern Ireland and other relevant professional bodies.
What is the legal basis for the SHOT database?

SHOT data is processed according to Article 6(e) and Article 9(h) under the General Data Protection Regulation (GDPR) which means that we can process this health care data for the performance of our official task in the public interest.

What information does the SHOT database contain?

SHOT has been collecting data on adverse events and reactions in blood transfusion since 1996 and since 2010 this has been supplied by reporting healthcare organisations via the SHOT database. The information includes restricted details about the patient, such as medical diagnosis and investigations performed, plus treatments given and outcomes of the adverse event. The information importantly also contains the patient’s date of birth and gender. These details can be essential for assessment of the incident. Transfusion requirements vary at different ages, some of which need to be very precise, so use of age alone may not be sufficiently accurate. There are also substantial differences between male and female patients in relation to transfusion. The Information Commissioner’s Office (ICO) has confirmed that they regard date of birth, gender and a procedure (incident) as sufficiently anonymous to maintain patient confidentiality.

To increase security of patient identification, a new policy regarding use of the date of birth was introduced in 2017:

- Only the age, calculated from the supplied date of birth, will be shared with SHOT experts as required for analysis of cases
- The date of birth will remain only accessible to authorised staff via the SHOT database
- Case studies used in the Annual SHOT Report and for educational purposes will no longer include an age of the patient and will be restricted to a decade, e.g. ‘in their 70s’.

Who manages the SHOT database?

The SHOT database is managed by the SHOT Steering Group (SG), which provide professional ownership and strategic direction, monitor the performance of SHOT and is accountable to the UK Forum (representing the four UK blood services) through the SHOT Medical Director for the use of resources and management of the budget. Membership of the Steering Group will consist of nominated representatives of the Medical Royal Colleges and other professional bodies.
What happens to the data and who can see it?

The data is collected by hospital staff treating and managing the patient, including doctors, nurses and laboratory staff. Once the records have been loaded to the SHOT Database they can be reviewed by authorised staff at the reporting hospital and by SHOT staff, using an approved user account with a secure password. This data does not include patient names or addresses. All SHOT staff are required to undertake regular mandatory annual Information Governance training.

Hospital staff enter the information directly into a secure Web-based database via the Medicines and Healthcare products Regulatory Agency (MHRA) database known as SABRE. Reporting of serious adverse events and reactions to the MHRA is mandated by law.

When the data have been checked and confirmed by the hospital reporters, the software engineers and data analysts at Dendrite Clinical Systems™ will download the data to a secure server in Dendrite’s offices (see Section on Dendrite security).

The information collected allows SHOT to analyse adverse events and reactions in blood transfusion and learn from these. SHOT produces an annual report with recommendations for improved practice. These annual reports do not contain the details of individual patients. Annual reports are available via the SHOT website www.shotuk.org. No data which could identify somebody will be shared with anyone, or used for purposes other than those required to perform the analysis. If the current arrangements for running this haemovigilance analysis through SHOT should end, the data will be deleted or securely transferred to a new provider.

SHOT Database Server

The server is hosted on the NHS network (N3) within a data centre in London, by Piksel. This is a tier four data centre which meets the highest levels of building security.

The service delivery and information security provided complies with ISO 20000 & ISO 9001 accreditation and the security management structure is aligned alongside ISO27001. The security arrangements are internally audited approximately every three months and externally audited every six months.

All servers have firewall and anti-virus software installed which is configured to use real-time scanning.
Backup Resilience

The data is securely backed-up each day. All backed up data stored is compressed, de-duplicated and encrypted within a secure off-site vault.

There are two backup vaults, the primary one is hosted locally and is then backed up to a secure secondary off-site vault hosted within a separate datacentre located at Heathrow.

Dendrite Security

Dendrite Clinical Systems™ is assessed against NHS Information Governance standards, which includes both physical and organisational security measures. Dendrite’s toolkit assessment score is available on the Data Security and Protection Toolkit (replaced the Information Governance Toolkit) website (https://www.dsptoolkit.nhs.uk/OrganisationSearch?searchValue=Dendrite).

The computer software program created by Dendrite, that holds the SHOT data, has been independently tested to ensure that it is not vulnerable to unauthorised access, or internal breaches of security.

Can I ask to see the data that the SHOT registry holds about me?

The anonymity associated with SHOT reporting means it would not be possible to identify data about an individual.

Further information

Queries should be directed to SHOT via shot@nhsbt.nhs.uk or 0161 423 4208.