# Information Sharing to Tackle Violence (ISTV)

# Initial Standard

# Implementation Guidance

**Version 2.1**

# 1 Contents

Amendment History:

| Version | Date | Amendment History |
|---|---|---|
| 0.1 | 10 Dec 2013 | Initial draft |
| 0.2 | 18 Dec 2013 | Second draft including alignment with IG view from Phil Walker. |
| 0.3 | 20 Dec 2013 | Third draft incorporating comments from JS and AB |
| 0.4 | 11 Feb 2014 | Updated following ISB appraisal |
| 0.5 | 14 Feb 2014 | Minor amendments following further comments from appraisers |
| 0.6 | 26 Feb 2014 | Requirements for information sharing agreements relaxed following representation from Home Office. |
| 0.7 | 11 Mar 2014 | Version for submission to ISB with amendments from quality assurance. |
| 0.8 | 20 Mar 2014 | Final version for submission to ISB following pre-board screening |
| 0.9 | 02 Apr 2014 | Post ISB conditional approval notice – changed to include statement regarding data protection (see section 6) |
| 1.0 | 03 April 2014 | Amended following SRO review |
| 2.0 | 10 June 2014 | Publication copy |
| 2.1 | 02 April 2019 | Revised to take account of the Data Protection Act 2018 (GDPR) |

Approvals:

| Name | Organisation | Version | Date |
|---|---|---|---|
| ISB | Information Standards Board | 0.9 | 04/04/14 |
| Amy Nicholas | Department of Health | 2.0 | 9/06/14 |
| Kathy Farndon | NHS England | 2.0 | 9/06/14 |
| Dawn Monaghan | NHS England | 2.1 | 02/04/19 |
| Mark England | NHS England | 2.1 | 02/04/19 |

Glossary of Terms:

| Term | Acronym | Definition |
|---|---|---|
| Association of Chief Police Officers | ACPO | Organisation representing UK chief police officers. |
| Accident and Emergency | A&E | One of four types of NHS department dealing with high priority unscheduled care |
| Community Safety Partnership | CSP | Body defined in the 1998 Crime and Disorder Act bringing together local 'competent authorities' such as police, fire, health and local authorities. |
| NHS Digital | NHSD | DHSC sponsored non-departmental public body with responsibility for NHS data collection including the processing of patient identifiable data |
| Information Governance | IG | The compliant and secure processing of personal or confidential patient information |
| Information Standards Management Service | ISMS | Secretariat and management service that supports the Information Standards Board |
| Information Sharing to Tackle Violence | ISTV | Process based on the 'Cardiff Model' of sharing a small de-identified dataset between A&E departments and CSPs to support community violence reduction |
| Police and Crime Commissioner | PCC | Locally elected representative with a lead on police and crime issues. |
| Patient Administration System | PAS | Hospital IT system used to manage patient care |

# 2 Contacts

| Sponsor | |
|---|---|
| Name | Dr Simon Eccles<br>Chief Clinical Information Officer for<br>Health and Care |
| Organisation | Department of Health and Social Care, NHS England, NHS Improvement |
| Implementation Manager | |
| Name | Mark England<br>Director of Strategy - Emergency and<br>Elective Care<br>Deputy National Director of Urgent and<br>Emergency Care |
| Organisation | NHS England and NHS Improvement |

**Acknowledgements**

The author acknowledges the generous assistance of a number of individuals and organisations without which this document and the associated specification and submission could not have been completed.

- Behnam Khazaeli, Gemma Thompson, Adam Lindridge, Moira Richardson: Gateshead Council
- Leslie Petrie, Heather Henderson, Michael Waterworth: Wythenshawe Hospital
- Royal Derby Hospital
- Lucy Jones, Jayne Burton, Jennifer Ashley, Debbie Eardley: Chesterfield Royal Hospital:
- Susan Taylor: Balance Northeast
- David Ottiwell: New Economy, Manchester
- Dr Adrian Boyle: College of Emergency Medicine
- Professor Jonathan Shepherd: Cardiff University
- The independent appraisers appointed by ISMS

# 3 Purpose

This document explains the actions required to implement the Information Sharing to Tackle Violence (ISTV) dataset. The guidance covers activities required of NHS Accident and Emergency (A&E) departments and Community Safety Partnerships (CSP) and the governance structures required to make the model of information sharing work effectively at a local level.

The guidance does not cover the use of the data by Community Safety Partnerships (CSP) in any detail as this is beyond the scope of the Information Standard itself.

## 3.1 Note on terminology

The term Community Safety Partnership (CSP) has been used throughout this document to refer to the agency receiving the data from A&E departments. This is the statutory mechanism identified in the Crime and Disorder Act responsible for coordinating community level responses to criminality[1]. They are sometimes referred to as Crime and Disorder Reduction Partnerships (CDRP) but the term CSP has been used throughout this document.

It is recognised that individual partnerships will operate in different ways and in practice, the organisation receiving and processing the data on behalf of the CSP will vary. In this context 'CSP' should be taken to mean whichever organisation takes the lead for receiving and processing ISTV data locally.

## 3.2 Related documents

| Ref # | Reference | Title |
|---|---|---|
| 1 | ISTV_Specification_v2.1 | ISTV Initial Standard: Specification |
| 2 | CR1344-18092014 | ISTV NHS Data Model and Dictionary Change Request |

[1] Under section 5-7 of the Crime and Disorder Act 1998.

# 4 Overview

The ISTV standard is relatively straightforward. The principal actors are:

- NHS A&E departments[2]
- Community Safety Partnerships (CSP)

Staff who book patients into the A&E department collect a small additional dataset on patients whose attendance has been caused by a violent incident.

The data comprises[3]:

- Time and date of the violent incident
- Time and date of attendance at the A&E departments (already collected as part of ISB 1588 [4])
- Specific location of the violent incident
- Primary means of assault (i.e. weapon or body part used)

A&E staff must be able to identify patients who have been assaulted and collect the additional data accurately.

The data is then compiled and passed to the CSP on a monthly basis[5] for further analysis.

The users of the data are analysts in local government or the police. The data forms one component of the information they gather to inform violence reduction measures agreed by the CSP.

[2] The Standard is mandatory for Type 1 A&E Departments in England and optional for all other Types
[3] Full details of the dataset are provided in the ISTV Specification and the associated NHS Data Model and Dictionary entry.
[4] ISB 1588 Accident and Emergency Clinical Quality Indicators.
http://www.isb.nhs.uk/library/standard/251 [accessed 16/12/2013]
[5] Monthly submissions are recommended, but the frequency can be increased if this is agreed locally.

# 5 Organisation guidance

## 5.1 Local governance

The implementation of this standard requires effective collaboration between the A&E department and the CSP. They need to establish a shared vision, working relationship and routine communication and governance arrangements as a prerequisite for data collection and flow.

It is recommended that:

- A nominated consultant for the A&E department must routinely attend the CSP body with executive responsibility for violence reduction;
- ISTV data sharing is a standard agenda item at meetings of the CSP body with executive responsibility for violence reduction;
- The identity of the data controller for the CSP is established as a prerequisite to data sharing;
- Where ISTV data sharing has not yet been established, a joint implementation plan is developed and agreed by both A&E department clinical and managerial leadership and the CSP, including project management leads from each side;
- An information sharing agreement is put in place between the NHS Trust that operates the A&E department and the CSP which sets out:

- The purpose for which the data is to be used;
- The roles and responsibilities of individuals and organisations involved;
- Prohibition of re-identification;
- Prohibition of further disclosure of the data;
- Technical and organisational security arrangements including the protection in place for data transfer;
- Arrangements for storage and disposal of the data;
- Training arrangements for staff receiving the data;
- Penalties for breach of the protocol
- The process for periodic review of the data by the Trust Caldicott Guardian to ensure that the data is properly de-identified.

Where data in addition to the minimum dataset is shared with the CSP, an information sharing agreement or protocol should be considered to be mandatory.

## 5.2 A&E departments and host NHS Trusts

### 5.2.1 Departments that are already sharing ISTV data

A&E departments that are already collecting and sharing ISTV data with one or more local CSP will need to carry out an impact assessment of their existing practice against the Information Standard documentation, including this document.

Where variation from the practice described in the standard documentation is identified, the A&E department should develop a conformance plan to ensure they comply with the standard.

It is recommended that the CSP is notified at the earliest possible opportunity of changes to existing practice and that they are included in the planning of any conformance activity.

It is particularly recommended that A&E departments review their training schedules to ensure that ISTV data collection and data quality issues are covered regularly, and that Caldicott Guardians work proactively with A&E department staff to ensure that IG issues are covered thoroughly.

### 5.2.2 Departments that are not yet sharing ISTV data

A&E departments not sharing will need to establish the data collection mechanisms the process for transferring the data to the CSP.

The options for data collection are either to build the functionality into the Patient Administration System (PAS), or to collect and collate the data manually. The former is the preferred method as it is more robust and sustainable in the long-term and will save staff time and effort.

The process for implementing the data collection is:

- Establish formal governance and communications channels between A&E and CSP, including where necessary, the establishment of a written information sharing protocol as set out in section 5.2;

- Secure approval for the data collection from A&E department leadership, both clinical and managerial;
- Secure the approval of the Trust Caldicott Guardian / privacy / IG lead;
- Institute changes to the PAS system, or develop a manual process to collect the data;
- Gain agreement on data extraction timetable, data format and transfer mechanism with CSP;
    - The recommendation is for monthly reporting; it can be more frequent, but must not be less frequent;
    - Data should be extracted, anonymised and sent to the CSP as soon as possible at the end of a reporting period (i.e. 2-5 working days)
- Carry out training for data collection staff covering:
    - Purpose of the data collection and benefits;
    - Importance of ensuring the data is de-identified;
    - Importance of accurate descriptions, except where private addresses are the location;
    - Rules for communal residences, ways of assessing sizes (i.e. what type of site is likely to have greater or fewer than 2000 residents)[6] and the importance of erring on the side of caution;
    - Rules for data collection, data quality and general IG issues;
    - Mechanisms to collect the data;
- Carry out training for data extraction / transfer staff covering:
    - Purpose of the data collection and benefits;
    - Importance of ensuring the data is de-identified;
    - ICO anonymisation code of practice;
    - Agreed data extraction processes and timescales, as specified in the information sharing protocol;
    - Caldicott Guardian audit process.
- Piloting – limited duration live running to test out the process and review any problems, including review with the CSP of the data extracted;
- Live rollout.

When the standard is implemented, the A&E department also needs to agree the process for refresher training on ISTV data collection to account for staff turnover. Training on ISTV issues must be incorporated into the routine staff training schedule to ensure that it is firmly embedded into practice.

It is recommended that all ISTV training (i.e. for both setup and refresher training) include the active participation of the CSP, particularly to ensure that A&E staff understand the use the data will be put to and the requirements for data quality. This will also help cement the shared vision and open communication between both sides.

It is recommended that the A&E department assigns a member of staff to act as a ‘Cardiff Model Champion’ on an on-going basis. During the implementation phase, this individual will form the link with the violence reduction nurse network being put in place by NHS England to support implementation[7].

[6] A&E departments should consider developing a list of possible sites of violence with over 2000 residents that can be used as a quick reference guide for staff.
[7] See the ISTV Implementation Plan

This needs to be a person with credibility within the department who can champion the ISTV data collection work amongst colleagues, act as a source of expertise on the process and provide a single point of contact for ISTV issues.

A&E departments that are not yet collecting and sharing ISTV data should consider contacting neighbouring A&E units that have already implemented the process so they can share knowledge and experience. This can be particularly useful where departments use the same IT system.

## 5.3 Community safety partnerships

The Department of Health and Social Care (DHSC) has published formal guidance for CSPs in how to engage with the NHS[8].

The CSP must ensure that there is appropriate representation from A&E departments on their governance bodies, and that an information sharing protocol is agreed as outlined in section 5.2.

In addition to the overall governance and communications arrangements, the CSP need to agree the transfer mechanism[9] from the A&E department for the data and the timetable.

They will also need to establish:

- The mechanism for processing the data when it is received to turn it into useful intelligence. This might include augmenting the data from other sources (e.g. assigning postcodes or coordinates to the locations identified), mapping the data and carrying out other analysis to understand trends and patterns of violence
- The process for feeding the intelligence into the development of violence reduction measures.

The CSP has a responsibility to limit the range of information it requests from the A&E department to the minimum required, and to use of the data to the purpose for which it has been provided – to support community safety and violence reduction activities.

The CSP also has a responsibility to ensure that their staff are trained in data protection and information governance issues with respect to the processing of NHS data. This should cover:

- Basic knowledge of the Data Protection Act 2018 (GDPR) including the data protection principles;
- Caldicott principles and the role of Caldicott Guardians in the NHS
- Uses of ISTV data as documented in the information sharing protocol agreed with the A&E department (outlined under section 5.2)

[8] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/212949/CSP-Guidance-September-Final.pdf
[9] Which must conform to the process requirements in the ISTV Specification.

- Information Commissioner's Office anonymisation code of practice[10].

The most common strategies developed from current implementations of ISTV data sharing are:

- Targeted policing: aligning the deployment of police units with the time and location of violence hotspots to;
- Targeting 'problem' licensed premises;
- Informing licensing applications and appeals;
- Development of strategies aimed at specific weapon types (e.g. enforced use of plastic glasses, reductions in bottle availability, knife amnesties);
- Informing other public health and social strategies such as drug and alcohol services.

The role of Police and Crime Commissioners (PCC) in local CSPs, is not yet clear and is likely to vary. However, it should be assumed that even where PCCs do not take an active role in CSPs, they will need to understand the role of ISTV data sharing and be briefed on progress in community violence reduction.

[10] ICO. Anonymisation: managing data protection risk code of practice. November, 2012. http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf

# 6 Information governance

## 6.1 The basis of information sharing

The commitment in the Coalition Government Agreement provides a strong mandate for NHS organisations to share the ISTV dataset with CSPs. However, there is an implicit assumption that those organisations will share information in a safe and legal manner. This means the data collection and sharing process must comply with:

- Data Protection Act 2018 (GDPR)[11]
- NHS Confidentiality Code of Practice[12]

Additionally, NHS organisations share data in accordance with the Caldicott Principles.

In order to be shared with CSPs, the ISTV dataset must be anonymised in accordance with the ICO Anonymisation Code of Practice (https://ico.org.uk/media/1061/anonymisation-code.pdf). Caldicott Guardians and IG leads for CSPs should be familiar with the ICO code of practice and able to provide advice to staff locally. Provided that the data you supply to CSPs meets these requirements it will comply with data protection and confidentiality requirements.

## 6.2 Risks and safeguards

There are some essential safeguards that need to be put in place to ensure the data remains anonymous and cannot be combined with other public datasets to identify an individual.

Risk arises from three factors:

- Need for an element of free text entry
- When the violent incident occurred in a private address such as the home of the victim or perpetrator;
- When additional data beyond the minimum dataset is included in the collection.

[11] HM Government. Data Protection Act 1998. http://www.legislation.gov.uk/ukpga/1998/29/contents [accessed 10/01/2014]
[12] Department of Health. Confidentiality: NHS Code of Practice. 2003. https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice [accessed 10/02/2014]

The rules on handling private addresses is set out in the section on Data Quality, but the underlying principle is that location information on private addresses should NOT be shared and the generic description HOME OR PRIVATE ADDRESS must be used instead.

The general risk arising from free text entry should be mitigated through rigorous training of data collection staff to ensure they understand the purpose of the data collection and the reason the data must be properly de-identified. The de-identification of the data should be assured by the audit arrangements put in place by the Caldicott Guardian.

The augmentation of the minimum dataset with additional information is **not necessary** to achieve the benefits reported in Cardiff and elsewhere. It is recommended that local A&E departments and CSP prioritise establishing the minimum dataset collection and the process for the CSP to transform it into useful intelligence in the first instance.

Although not recommended, the intention is not to stifle local innovation and the potential for the controlled development of the dataset.

Additional information should only be collected on the following basis:

- Where additional data is collected and shared, an information sharing agreement or protocol should be considered to be mandatory;
- The A&E department and CSP involved MUST notify the ISTV Programme Board of the details of the data collection and gain its approval;
- It MUST be approved by the Trust Caldicott Guardian and subject to the same audit mechanisms as the ISTV data collection;
- If at all possible it should be separated from the ISTV data collection and flow and subject to specific IG controls appropriate for the type of data being collected;
- It MUST be legal – i.e. not include any clinical or patient identifiable data;
- It MUST NOT compromise the de-identification of the dataset;
- It MUST be for a clearly defined purpose, preferably supported by some research evidence;
- It MUST be subject to evaluation to determine the effectiveness of the collection;
- If evaluation determines that the collection is not effective, it must be ceased immediately;
- The results of any evaluation MUST be reported back to the ISTV Programme Board so that it can take an informed decision on whether work should be commissioned to include the additional collection in the ISTV standard;
- Approval MUST be secured from the relevant research ethics committee.

## 6.3 Responsible data processing

The guidance from the Information Commissioner's Office is very clear that the data must be handled responsibly both by the A&E department collecting it, and the CSP. In practice, this means:

- A&E departments collecting, storing and transferring the data safely and in line with NHS information governance rules;
- CSPs processing, storing and using the data responsibly and only for the purpose for which it is intended: the development of community violence reduction measures.
- Should any personal data be transferred then the data controller must be conformant with the Data Protection Act 2018 (GDPR).

# 7 Data quality

For the data to be of use to the CSP is must be as accurate and complete as possible. This includes:

- **Coverage**: all violent incidents that result in an A&E attendance must be identified and recorded by the A&E department
- **Accuracy**: the minimum dataset must be recorded for as many attendances as possible, (accepting limitations such as patient's refusal or inability to cooperate), and the data must include enough information to be useful to the CSP but not so much that it creates a risk of individuals being identified

## 7.1 What is enough information?

The purpose of the data collection is to identify 'hotspots' of violence so that these can be addressed systematically by the authorities. This might include changing policing patterns or increasing the number of youth workers in a particular locality.

So the most important features of the data are:

- It must identify the location of the violence as accurately as possible, except when it occurred at a private address where this might compromise anonymity.
- It must identify the approximate time the incident happened
- It must identify the nature and severity of the violence using the primary type of weapon as a proxy (e.g. firearms, knives, knuckle dusters etc are generally more serious than feet and fists)

'Enough' information is likely to include a clear description of the location, for example:

The name of any licensed premises associated with the violence (e.g. THE RED LION IN MARKET SQUARE ANYTOWN; STUDIO NIGHTCLUB, ANYTOWN)

Street or urban descriptions enabling the mapping of the incident (ANYTOWN MARKET SQUARE; ANYTOWN RAILWAY STATION; SMITH STREET UNDERPASS; ANYTOWN BUS STATION; JUNCTION OF NEW ROAD AND LOW LANE IN CEDARS ESTATE, ANYTOWN)

Generic descriptions of location should be avoided, so the following are NOT appropriate:

- IN THE STREET
- ANYTOWN
- ROAD JUNCTION

- TAXI RANK (without identifying which taxi rank)
- STATION (without identifying which bus/rail station)

## 7.2 When does enough become too much?

The risk of compromising the identity of an individual arises when the violence occurs in a private address, either the home of the victim, the assailant or an associated individual (e.g. relative or friend).

If the address or full postcode of the assault is included in the data, it would be possible to use this in combination with data from other sources (such as the electoral register) to narrow the search down to an individual or a small number of people.

For this reason, the following Information Governance (IG) rules should be applied:

- When the violence occurs in a private address such as a house, flat, or maisonette only the generic description HOME OR PRIVATE ADDRESS should be shared;
- Where a licensed premises is also the residence of the patient (i.e. for example where a landlord or member of their family has been assaulted) the name of the licensed premises should be included in the data, but there is no reason to include the fact that the subject of the violence is a resident in the free text entry;
- All hotels should be treated in the same way as licensed premises (which many of them are) and named in the data;
- Where the violence occurs in a small (fewer than 2000 people) communal residence such as a care home, shared house or hostel, then the rules for private addresses must be applied.

Where the violence occurs in a large (greater than 2000 people) communal residence, such as large university halls of residence, large flats complex, military base, hospital etc, then it is acceptable to give the highest level of name to the location (ANYTOWN UNIVERSITY HALLS; ANYTOWN GENERAL HOSPITAL NURSES ACCOMODATION) and to include the postcode sector if this is available (first part of the postcode and first digit of the second part).

The recording of the fact the violence occurred in a home environment is in itself important as it allows the NHS to identify people injured in incidents of domestic violence, thereby ensuring they are risk assessed and supported appropriately. It is also an indicator of general violence in a home setting and can be used as a proxy for domestic violence for some purposes.

## 7.3 Securing data quality

The quality of the data is entirely dependent on A&E staff understanding the reason for the data collection, how the data is used and how it will help to reduce violence, i.e. how they are contributing to reducing violence in their community. This message should be reinforced in routine training.

There are three related strands of activity to securing data quality:

- **Engagement**: routine engagement and good communications between the A&E department and CSP staff;
- **Training**: training of A&E staff to ensure they understand how to collect the data and why it is important, repeated periodically to reinforce messages and account for staff turnover
- **Feedback**: feedback to A&E staff on what how the data is being used, for example by sending monthly crime reports, and particularly by reporting any successes that are directly attributable to the data provision.

# 8 Technical guidance

Suppliers should use the ISTV Specification document and the NHS Data Model and Dictionary Service (DMDS)[15] entry as the basis for any changes they make to their system to implement the standard.

How the collection of the data items is handled in system user interfaces must follow the system requirements in the Specification document, but otherwise is at the discretion of the system operators and their suppliers. The following is intended as guidance only:

- The lists contained in the ISTV Specification document should be used as the basis for drop down / selection lists in the user interface;
- Supplementary information on screen or visual or audible cues can be used to promote appropriate data entry for free text fields;
- Although the file type of the data extract can be agreed locally between the A&E department and CSP, it is recommended that a common format is used such as CSV or Excel file;
- An XML schema for the dataset and supporting documentation is also available as part of the NHS Data Model and Dictionary specification.

The transfer of files from A&E department to CSP should be carried out using a secure mechanism. For example, secure email, either between two NHSmail accounts or between NHSmail and Government Connect Secure Extranet (GCSx) accounts is acceptable, using generic mailboxes rather than personal accounts.

It is also recommended that files are encrypted to NHS Digital approved standards[16] to ensure the data is protected if it is sent accidentally to an incorrect, non-secure email address.

Encrypted files should not be zipped (e.g. compressed into a .zip type file) using the compression software built into Microsoft Windows as this does not support file encryption.

Other forms of compression such as WinRAR, WinZip, P7Z may be used if supported by both sending and receiving organisations. However, the dataset is unlikely to be large enough to warrant compression.

Where files are encrypted the passphrase MUST be sent in a separate email.

[15] CR1344 ISTV NHS Data Model and Dictionary Service Change Request.
[16] http://systems.hscic.gov.uk/infogov/security/infrasec/gpg [accessed 10/02/2014]

# 9 Further reading

## 9.1 General

Department of Health. Information Sharing to Tackle Violence: guidance for community safety partnerships on engaging with the NHS. DH, 2012. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/212949/CSP-Guidance-September-Final.pdf

College of Emergency Medicine. Guideline for information sharing to reduce community violence. The College of Emergency Medicine. CEM, 2009.

http://www.collemergencymed.ac.uk/code/document.asp?ID=4881

Information Commissioner's Office. http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

Health and Social Care Information Centre (HSCIC) good practice guidance: http://systems.hscic.gov.uk/infogov/security/infrasec/gpg

Department of Health. NHS Confidentiality Code of Practice. https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

## 9.2 Published research

Curtis F, et al. Costs and benefits of anonymised information sharing and use in health service, police and local government partnership for preventing violence related injury. BMJ 2011;342.

Shepherd J. Violence: the relation between seriousness of injury and outcome in the criminal justice system. Journal of Accident Emergency Medicine, 1997.

Shepherd J, et al. Effectiveness of anonymised information sharing and use in health service, police and local government partnership for preventing violence related injury. BMJ, 2011.

Shepherd J. Preventing violence – caring for victims. Surgeon 5; 2, 2007.

Warburton AL and Shepherd JP. Tackling alcohol related violence in city centres: effect of emergency medicine and police intervention. Emergency Medicine Journal, 2006;23.