



Information sharing protocol governing the exchange of data
for the Trauma and Injury Intelligence Group
Project in xxx



Liverpool John Moores University

Contents

1	Details
2	Data Controllers
3	Preface
4	Purpose of the Protocol
5	Background
6	Partners
7	Legal Framework
8	Data Sharing Protocols
8.1	Sharing
8.2	Acquisition
8.3	Data Flow
8.4	Data Quality
8.5	Storage
8.6	Dissemination
8.7	Access to Data
8.8	Retention
8.9	Confidentiality
8.10	Compliance
8.11	Staff Responsibility
9	Monitoring and Review
10	Further Information
11	Agreement
12	Signatories
13	Appendices
	Appendix 1 Data Dissemination Protocol
	Appendix 2 Amended Data Controllers Form

1. Details

Organisation Requesting Data:

TRAUMA AND INJURY INTELLIGENCE GROUP (TIIG)

Group Hosted / Managed by:

In Partnership With:

--	--

TIIG Executive Personnel: Data Procurement, Management, and Analysis:

Information Required

Anonymised Accident and Emergency Department data.

2. Data Controllers

3. Preface

This protocol sets out an agreement for the exchange and use of data between the Trauma and Injury Intelligence Group (TIIG), the providers of data to the TIIG and the long term facilitators, xxx. The protocol is designed as a generic form that reflects the needs of the provider, TIIG, and xxx, with particular respect to how data protection, patient confidentiality, and Caldicott Principles will be observed at all times.

4. Purpose of the Protocol

The remit of the TIIG xxx Project is to deliver data to inform the development and planning of prevention strategies, the targeting of operational programmes, and monitoring and evaluation in the field of intentional and unintentional injuries across xxx. By working towards this objective, the group hopes to deliver trauma and injury data from across xxx with a degree of consistency and comparability. In xxx, the TIIG reports to xxx PCTs. Intelligence collected will aid the identification of at risk groups and provide good evidence to develop policy, inform public health interventions and assist in monitoring the effectiveness of injury prevention campaigns.

5. Background

In 2007 a meeting was held with representatives from xxx PCT and TIIG to discuss the need and potential benefits of the establishment of an Injury Surveillance System (ISS) in the xxx area. As a result of this meeting, and subsequent discussions with public health practitioners from xxx, an agreement and funding was sought to set up an ISS in xxx which collects data specifically from local Accident and Emergency Departments (AEDs), modelled on the work of the TIIG in Merseyside.

6. Partners

The following partners are actively involved in the TIIG xxx Project:

- Xx
- Xx
- xx

7. Legal Framework

The following statutory instruments and legal principles provide the framework for the governance of data exchange between agencies:

- Section 115 of the Crime and Disorder Act 1998
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Local Government Act 2000
- The Freedom of Information Act 2000
- Crime and Disorder Regulations 2007
- Common Law Duty of Confidence
- Memorandum of Information

The Crime and Disorder Regulations 2007 place a duty on police forces, fire and rescue authorities, local authorities and primary care trusts to share depersonalized information held in electronic form.

8. Data Sharing Principles

8.1. Sharing

The AEDs specified in this document in accordance with their PCT agrees to provide TIIG with all data relating to AED attendances for intentional and unintentional incidents.

8.2. Acquisition

Non-personal identifiable data is to be transferred by email to a NHS secure line, on a monthly basis. Data must only be transferred electronically from an [nhs.net](https://nhs.uk) account to an [nhs.net](https://nhs.uk) account. TIIG do not feel that encryption is required for the transfer of data as patient identifiable data is not included, although they are willing to discuss this with the Caldicott Guardian of each supplier of data if required.

8.3. Data Flow

TIIG officers at the Centre for Public Health, Liverpool John Moores University will receive anonymised data directly from the AED. The data will be collated by TIIG officers and will be transferred to xxx PCT. The data will be transferred to the PCT by email through a NHS secure line. The data flow will take place on a monthly basis, a month in arrears.

Funding for the TIIG xxx Project Officer concludes on xxx. After this date it is anticipated that the mechanisms for data exchange set out in this protocol will continue. Data Providers agree to continue to share data with the TIIG, whilst TIIG will continue to distribute data to the relevant Data Controllers set out in this protocol. However, responsibility for data analyses for xxx partners will fall within the remit of the Information Department within xxx PCT. **The data flow systems in place will not change and the protocols stated in this document will continue to be binding.**

8.4. Data Quality

- i) Data Providers will ensure quality assurance checks are in place before any data are transferred. Data Controllers receiving shared information are responsible for applying relevant quality assurance before using the information they hold.
- ii) If information is found to be inaccurate, it is the responsibility of the Data Controller discovering the inaccuracy to notify the Data Provider and other Data Controllers directly. The Data Provider will ensure that the source data is corrected and will notify all other Data Controllers, who will be responsible for updating the information they hold.
- iii) As a result of any information being wrongly disclosed by another party through an act of neglect or omission Data Controllers will not be liable for any financial or other costs incurred.

8.5. Storage

Each agency is responsible for ensuring that all data received are stored in a secure and confidential manner. Partners must ensure that data are stored on secure computer networks, password protected and only accessible by the appointed Data Controllers. Any hard copies should be housed in a locked cabinet in an alarmed office.

8.6. Dissemination

Data will only be disseminated in line with the TIIG dissemination protocol (Appendix 1).

8.7. Access to data

Access to the full data sets will be restricted to the specified Data Controllers. Data Controllers will have access to all data collected for the purpose of the TIIG xxx Project to cover all cross border issues. Where requests for raw data are made by other agencies and partners, Data Controllers will seek authorisation to share the requested data directly from the Data Providers. This protects the integrity and confidentiality of the agreement and is in line with the Caldicott Principles.

8.8. Retention

Data will be stored indefinitely, but will be archived periodically and stored on CD-ROM. CD-ROMs will be stored in a locked cabinet within a locked and alarmed office; data will be archived for ten years.

8.9. Confidentiality

i) Although the agencies identified are partners of the group, all disaggregated data will be held exclusively by the signatory members and only aggregate data analysis outputs will be disseminated to other partners. Data Controllers will manage and analyse the data, and will only provide data to other partners in the form presented in the dissemination protocol (see Appendix 1), for the purposes of setting strategies, and bidding for, implementing, monitoring and evaluating interventions.

ii) The data provided will be selected so as to ensure patient anonymity. For example, age will be requested as a proxy for date of birth; a unique identifier will be generated other than the NHS number in order that auditing can take place whilst protecting anonymity. Although there will not be any patient identifiable data exchanged, it is necessary to confirm this and for all parties to sign the agreement and protocol outlined. This document sets out a list of standards under which the data will be procured, used and stored.

8.10 Compliance

Structures are in place within each organisation and partner to ensure that they act within the constraints of the law and are observant of their legal requirements, specifically relating to data sharing and confidentiality.

8.11 Staff Responsibilities

Data Controllers will ensure that they and all additional users of the data will be trained and made aware of their obligations and responsibilities regarding the sharing, storing and dissemination of data.

9. Monitoring and Review

This protocol will be monitored and reviewed annually by TIIG. If any operational problems or complaints arise, these may be reviewed and amended accordingly but within 3 years of the date of signing. The protocol should also be reviewed and amended in line with any changes in legislation.

10. Further Information

It is possible that personnel will change during the TIIG project's lifetime. In this circumstance, all partner agencies must complete the *Amended Data Controller* form (see Appendix 2). Upon completion, copies of the form must be circulated to all Data

Providers. Any new signatory will be bound by the principles of this agreement and must adhere to their responsibilities as set out in this protocol.

11. Agreement

The signatories signed over formally agree to the following:

- To subscribe to the principles contained within the protocol.
- To work to the procedures identified within the protocol.
- To fully implement the protocol within their own agency, ensuring all staff know of its existence and support their attendance at any training event provided.
- To supply information within the bounds of the protocol at no financial cost to any of the other signatory agencies.
- To ensure that any partner agencies (voluntary or otherwise) used by each agency work to the protocol when undertaking contracted activity.
- To contribute to the development of trust and confidence between the signatory agencies by working within the framework of the protocol for the purpose of enhancing community safety.

12. Signatories

Data Controllers

.....

Signatures on behalf of xxx Trust

<p>Caldicott Guardian Name..... Position..... Signature..... Date.....</p> <p>Information Manager Name..... Position..... Signature..... Date.....</p> <p>AED Representatives Name..... Position..... Signature..... Date.....</p> <p>Name..... Position..... Signature..... Date.....</p> <p>Name..... Position..... Signature..... Date.....</p>

13. Appendices

Appendix 1. Data Dissemination Protocol

TRAUMA AND INJURY INTELLIGENCE GROUP xxx PROJECT

DATA DISSEMINATION PROTOCOL

Purpose

This document outlines protocol guidelines for the dissemination of intelligence relating to data received for the purpose of the Trauma and Injury Intelligence Group (TIIG) xxx Project. It is designed to ensure the appropriate use of intelligence derived from the data collected.

For the purpose of this document 'TIIG Intelligence Disseminators' refers to the two key Data Controllers: xxx Primary Care Trusts, Public Health Intelligence Departments; and the TIIG.

Fundamental Dissemination Principles

TIIG Intelligence Disseminators for the purpose of the TIIG xxx Project must ensure the following principles are met when disseminating intelligence in all circumstances (excluding those identified below):

1. They must respect the Caldicott Principles when considering the use of patient information.
2. Data must be aggregated to ensure patient anonymity for example:
 - a. Where the collated values received are below five they must be suppressed to ensure patient anonymity.
 - b. The minimum time period for which aggregate data will be disseminated is one month. This will prevent the identification of 'unusual' cases or individuals in data sets covering extremely small periods (for example: could you tell me the number of patients attending hospital X with gun shot wounds in the week beginning X?).
 - c. Free text data displaying names of individual businesses and street names will be removed.
 - d. All postcode data will be aggregated to at least Lower Super Output Area level.
3. Everyone should be aware of their responsibilities to respect patient confidentiality.

Open Access Data Principles

Access to the full data sets will be restricted to the specified Data Controllers. Data Controllers will have access to all data collected for the purpose of the TIIG xxx Project to cover all cross border issues. Where requests for raw data are made by other agencies and partners, Data Controllers will seek authorisation to share the requested data directly from the Data Provider/s. This protects the integrity and confidentiality of the information sharing agreement and is in line with the Caldicott Principles.

Limited Access Data Principles

It may be necessary to provide disaggregated data in some circumstances. For example, where data is collected on assault or last drink location (e.g. pub / club name) of assault attendances to AED, such data is typically collected for the purposes of targeted policing or licensing enforcement. It is envisaged that this data will be shared with relevant agencies, for example local police, Crime and Disorder Reduction Partnerships and licensing departments. Such data must be restricted to partners involved in promoting community safety. Data Controllers sharing this data must ensure that:

- All partners accessing the data have been approved by the xxx PCT or a TIIG representative.
- They have received in writing a full justification for use of the data from all partners and details of how the data will be used.
- Data provided to the restricted access group remains anonymised; the patient identifier field will be removed to prevent the agency in question approaching the data provider directly for more information about a particular AED attendance.

This restricted access group will still be bound by the fundamental dissemination principles defined above as well as the following:

1. Data can only be used for the purpose of improving community safety.
2. Data shared to the restricted access group must not be disseminated any wider, in any format.

Restricted Access Data Principles

Data provided to all other partners, in any format, must ensure they meet the fundamental dissemination principles as outlined above.

Individual Partner Data Use and Responsibilities

PCT Public Health Intelligence Departments

It is envisaged that local PCTs will produce and disseminate intelligence reports on trauma and injury for the trust and other key partner agencies using data supplied through TIIG. These will provide evidence for public health policy, interventions and strategy throughout the trust area. Intelligence may be disseminated in a variety of formats and differing intervals. The PCT Public Health Intelligence Departments dissemination protocol provides comprehensive details of their dissemination procedure. Any xxx TIIG data received by PCT Public Health Intelligence Departments must be disseminated in line with the above fundamental dissemination principles and the Caldicott Principles. This document must be used in conjunction with the PCT Public Health Intelligence Department dissemination document.

TIIG

Xxx TIIG intelligence is to be combined with intelligence from other TIIG projects to provide a comprehensive injury surveillance system for the North West. Data for the whole group will be utilised to identify at risk groups and communities to aid the development of policy, public health interventions and assist in monitoring campaigns in the field of intentional and unintentional injury.

Any xxx TIIG data received by the central TIIG coordinators must be disseminated in line with the above fundamental dissemination principles and the Caldicott Principles.

Ad hoc Requests and Specialised Reporting

In addition to regular reporting it is acknowledged, due to the growth in evidence-based policy, that various agencies will require data. Examples of the utilisation include: bids for funding; monitoring progress on Key Performance Indicators; Health Improvement and Modernisation Plans (HIMP); and other health targets. In such circumstances TIIG Intelligence Disseminators may disseminate intelligence in line with the fundamental dissemination principles outlined above. Where raw data is requested, a justification for the data must be received and permission to share such data must be sought from the Data Provider/s before data can be disseminated. For audit purposes Data Controllers will keep records of all information disseminated. This should include the details of the organisation requesting the data, the type of data provided, their intended use and the type of audience the data will be further disseminated to.

Other Information

This protocol may be subject to change as decided by the TIIG xxx Project steering group. This document must be considered in conjunction with TIIG Intelligence Disseminators individual dissemination protocols.

Appendix 2

Amended Data Controller Form

This addendum provides for the addition or removal of Data Controllers for the purpose of this protocol. In the event of a change in Data Controller in the partner organisations, a copy of this form must be completed, signed and distributed to all signatory parties. This form will act as an appendage to the protocol document and act in conjunction with it.

Addition of Data Controller:

I am hereby added as a Data Controller for the purpose of the TIIG xxx Project. I am fully aware of my responsibilities in this protocol and agree to subscribe to the principles and procedures identified:

Name.....

Position.....

Email address.....Telephone.....

Signature.....Date.....

Removal of Data Controller:

The signatory below agrees to remove themselves from the position of Data Controller for the purpose of this protocol. The signatory will no longer have access to data collected for the purpose of TIIG Xxx Project but will continue to be bound by a duty of patient anonymity.

Name.....

Position.....

Email address.....Telephone.....

Signature.....Date.....