Home Office

Publishing Incident Recording System data on the fire and rescue service at an incident level:

Project overview

Produced by the Fire Statistics team
FireStatistics@homeoffice.gsi.gov.uk
First published: 27 April 2017
Updated: 21 September 2017

1 Background

1.1 This document provides an overview of the work undertaken to make publicly available incident level data of incidents attended by fire and rescue services (FRS) and how the Home Office reached decisions about publication.

1.2 This document explains the process that the Home Office has taken to ensure that the risk of identifying individuals and releasing personal or sensitive data is minimised by using reasonable precautions.

1.3 The Incident Recording System (IRS) collects detailed information on every incident attended by fire and rescue services. In addition to fire incidents it contains records of false alarms, and non-fire incidents which cover a wide range of activity including flooding, lift releases and, increasingly, co-responding to medical incidents. There are nearly 200 questions within the IRS. Whilst no individual incident would require each to be completed, in general the more serious the incident the more questions that are asked. The system is maintained by the Home Office and information is entered by FRSs, using information collected by automatic systems and those present at the time of the incident. FRSs add incidents on a daily basis.

1.4 The Home Office currently publish four annual reports, and supporting data tables, based on IRS data-
a) Fire and rescue incident statistics – National statistics on fires, casualties, false alarms and non-fire incidents attended by the fire and rescue services in England. Published quarterly.
b) Detailed analysis of fires attended - Greater detail on incidents attended, including the causes of fires, the use of smoke alarms, the seasonality and timing of fires.
c) Detailed analysis of non-fire incidents - Greater detail on non-fire incidents attended.
d) Fire incidents response times. Trends in average response times in England at national level.

1.5 Whilst the publications provide a good overview of the main trends in incidents and related outcomes, it is not feasible to publish in this way the huge volume of information captured by the Home Office through the IRS. To address this, and as part of the Government's transparency agenda, the Home Office considered ways to publish more detailed IRS data. It is not possible to make everything in the IRS publicly available due to privacy considerations which are summarised in Sections 4 and 5.

1.6 The publication of incident level data is intended to have the following benefits-
a) Improve the ability of the fire sector and others to do more detailed analyses.
b) Improve the transparency of the sector's information.
c) Give the sector a resource to answer Freedom of Information and other requests in a quick, efficient and consistent manner by referring to these datasets.
d) Enhance the quality of the data held, benefitting the Home Office, FRSs and external users.

2. Personal Data in the IRS

2.1 In considering the types and levels of data to include in the incident level data releases, we have taken into account the possibility of the disclosure of personal information as defined by the Data Protection Act 1998, which is "…data which relate to a living individual who can be identified from those data or those data and other information which is in the possession of, or is likely to come into the possession of, the data controller …". Under the Data Protection Act 1998 there are seven kinds of information which constitute sensitive personal data, of which the most relevant to the IRS are information relating to the racial or ethnic origin of a person, the physical or mental health or condition of a person, the commission or alleged commission of an offence by a person and any criminal proceedings in respect of a person.

2.2 The IRS contains a range of personal data such as name and age of those rescued or injured in fires. It also contains data which could become personal if combined with the responses to other questions or other information in the public domain. For example, combining geographical area and the type of building with the nature of an injury could produce a unique combination from which it could be possible to identify a living individual, and so would constitute personal data. We have considered that a huge amount of information could be linked, for example, council tax records and FRS published information. In addition some information, although not strictly personal data, could be distressing for friends and family if released into the public domain, for example details of those fatally injured in fires (which also could be used to deduce the personal information of friends and family). The proposed approach to publishing these data from the IRS has been designed to mitigate this risk.

3 Data Controller

3.1 In general, a data controller is a person (see below) who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. In relation to IRS incident data, the data controller is a person who makes significant decisions in relation to the information, for example regarding publication, as distinct from more technical tasks like retrieval or erasure of data.

3.2 A data controller must be a "person" recognised in law, that is to say individuals, organisations and other corporate and unincorporated bodies of persons. Data controllers will usually be organisations, but can be individuals. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

3.3 To decide who the data controller was for the IRS incident level information the examples on the Information Commissioner's website were extremely useful, with one relevant example being:

"A government department sets up a database of information about every child in the country. It does this in partnership with local councils. Each council provides personal data about children in its area, and is responsible for the accuracy of the data it provides. It may also access personal data provided by other councils (and must comply with the data protection principles when using that data). The government department and the councils are data controllers in common in relation to the personal data on the database".

3.4 The Home Office believes that this example is very similar to the IRS, where FRSs collect data and are responsible for the quality of the data. They then provide these data to the Home Office through the IRS, which is maintained by the Home Office. The Home Office is responsible for the guidance provided to FRSs on inputting information into the IRS, which attempts as much as possible to ensure the comparability of the data across FRSs.

3.5 The Home Office has concluded that both the Home Office (of all data) and FRSs themselves (of their own data) are data controllers in this instance.

4 Assessing privacy risk

4.1 The Privacy Impact Assessment (PIA) screening questions[1] are a list of questions to consider at the beginning of any project involving personal data. They shaped the project and informed the decision that a full Privacy Impact Assessment is not necessary.

Table A: Privacy Impact Assessment Screening Questionnaire

	Question	Yes	No	N/A
Q1	Will the policy involve the collection of new information about individuals?		√	
Q2	Will the project compel individuals to provide information about themselves?		√	
Q3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		√	
Q4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	√		
Q5	Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		√	
Q6	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		√	
Q7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.		√	
Q8	Will the project require you to contact individuals in ways which they may find intrusive?		√	

4.2 Table A above provides an example of how the IRS data has been assessed on the basis of the PIA screening. It is anticipated that the majority of the data released in this project will follow this example. On this basis it has been decided that a PIA is not required and this document instead sets out the approach to suitably anonymise the data, however it may be the case that future releases will require a PIA.

4.3. Broadly, the approach to publishing incident level FRS data has been to avoid publishing personal data, because people involved in incidents attended by FRSs do not give explicit consent for their sensitive personal data to be used. Without consent the justification required for publishing personal data is greater.

[1] See Annex One in the Information Commissioner's Conducting Privacy Impact Assessments Code of Practice here https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

4.4 A key consideration of the development phase of this project was how to increase data availability whilst being mindful of the potential sensitive nature of the data. Following discussions with data experts, and with due regard to the Data Protection Act 1998, it was decided that the most appropriate way to open up more of the data was to publish standalone datasets that address particular topics or themes. These datasets would not be linkable to each other, meaning sensitive information cannot be matched.

4.5 Given this approach, the remaining major risk was “deductive disclosure” (otherwise known as the “jigsaw effect” or “mosaic effect”), where the identification of an individual's identity is possible through identifying respondents with unique characteristics. This risk has been minimised by anonymising the data.

5 Data anonymisation

5.1 As well as releasing data in thematic unlinked datasets, the following steps have been taken to achieve data anonymisation. It should be noted that these steps are common to many of the datasets, but some individual datasets may require additional measures to protect the identification of individuals. These will be documented in guidance that will accompany each release.

- Some variables have been grouped to reduce the risk of 'deductive disclosure'. For example, an incident with more than 100 officers in attendance would be rare, if not unique, if published with the precise number of officers present.

- Some variables, for example "Suicide/attempted: setting fire to self", have been subsumed into other categories because of the distress they could cause by being published.

- The FRSs of Isles of Scilly and Cornwall have been merged because the Isles of Scilly FRS has so few incidents that these could easily be identified and matched to other sources of sensitive personal data.

- Due to the small number of fatalities, these individuals are easily identifiable risking deductive disclosure. A marker to show if an incident has resulted in a fatality or casualty has been included which greatly reduces this risk while serving a public need.

- Each incident has a unique identifier used by the FRS concerned, these have not been published because of deductive disclosure concerns.

5.2 At this early stage of publication we have been prudent with the release of data variables in order to prevent a privacy issue with forthcoming datasets. This situation will be under constant review and so in later iterations datasets may have data variables added.

6 Quality of IRS data

6.1 The IRS is a continually updated database, with FRSs adding incidents on a daily basis. There is, however, variation in how long an incident takes between being closed on site and being entered and confirmed on the IRS. This can be for a variety of reasons, including the size of the incident, meaning information from many people is required. The intensity of quality assurance, and in some cases information from a coroner's report, may be required to finalise an incident report. Because of this, the incident level data published may not match that held locally by FRSs.

6.2 The data in the IRS are the responsibility of, and quality assured by, FRSs. The Home Office and FRSs work together on improving the quality of the data. Although it should be noted that the IRS was not designed to publish data at incident level, and so the datasets being released may unearth a very small number of previously unidentified inconsistencies. We are aware of three issues that have circumvented quality assurance checks currently:

- A small proportion of incidents in the IRS have been recorded with 0 officers attending, despite the definition of an incident being that an FRS attended. In these cases we believe the information has simply not been entered and therefore these incidents are marked as having a "not known" number of officers and vehicles attended.

- Similarly, a small proportion of incidents in the IRS have blank answers for certain data variables. These have been marked as having a "not known" for that particular data variable answer, sometimes "not known" is subsumed into "other".

- A small proportion of incidents in the IRS have been recorded as "deliberate" in one question but "accidental" in another question. We have marked these consistently with the cause/motive stated, as this appears to be the more straightforward question and the majority of these incidents state a cause of "other".

We have started monitoring these three issues with FRSs to reduce inconsistencies in future years. Addressing these issues will improve the quality of this data for the Home Office, FRSs and external users.